Ultra Cloud Core 5G Session Management Function, Release 2024.01 - Configuration and Administration Guide

First Published: 2024-01-31

Last Modified: 2024-03-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

About this Guide lix

Conventions Used lix

CHAPTER 1

5G Architecture 1

Feature Summary and Revision History 1

Summary Data 1

Revision History 1

Overview 2

Control Plane Network Functions 2

User Plane Network Function 3

Subscriber Microservices Infrastructure Architecture 3

Control Plane Network Function Architecture 5

CHAPTER 2

5G SMF Overview 9

Feature Summary and Revision History 9

Summary Data 9

Revision History 9

Product Description 10

Converged Core Overview 11

Interservice Pod Communication 11

Feature Description 11

How it Works 12

Feature Configuration 13

OAM Support 13

Use Cases and Features 13

Base SMF Configuration 13

4G Session Support 14
5G Session Support 14
Access and Mobility Support 15
Charging Integration 15
Cloud Native Infrastructure 15
Converged Core Network 16
IMS Support 16
IPAM Support 17
Lawful Intercept 17
MVNO Support 17
NF Management 18
OAM Support 18
Policy Integration 18
RADIUS Support 19
Redundancy Support 19
Roaming Support 19
SMF Inline Services 20
SMF Specification Compliance 20
Subscription Management 20
UPF Integration 20
Wi-Fi Support 20
Deployment Architecture and Interfaces 21
SMF Architecture 21
SMF Deployment 21
Converged Core Architecture 22
Converged Core Deployment 23
Supported Interfaces 23
Life Cycle of Data Packet 24
Session Affinity 30
License Information 31
Standards Compliance 31

CHAPTER 3 **Deploying and Configuring SMF through Ops Center 33**
Feature Summary and Revision History 33

Summary Data 33
Revision History 33
Feature Description 34
SMF Ops Center 34
Prerequisites 35
Deploying and Accessing SMF 35
Deploying SMF 35
Accessing the SMF Ops Center 36
SMF Service Configuration 36
Mapping Pods with Node Labels 36
Loading Day 1 Configuration 37

CHAPTER 4 Smart Licensing 39
Feature Summary and Revision History 39
Summary Data 39
Revision History 39
Feature Description 39
Cisco Software Central 40
Smart Accounts and Virtual Accounts 40
Requesting a Cisco Smart Account 40
SMF Smart Licensing 41
Software Tags and Entitlement Tags 41
Configuring Smart Licensing 42
Users with Access to CSC 42
Users without Access to CSC 47
Monitoring and Troubleshooting Smart Software Licensing 52

CHAPTER 5 SMF Rolling Software Update 55
Feature Summary and Revision History 55
Summary Data 55
Revision History 55
Feature Description 56
Updating SMF 56
Rolling Software Update Using SMI Cluster Manager 57

Prerequisites 58
Triggering the Rolling Software Upgrade 62
Monitoring the Upgrade 63
Viewing the Pod Details 64

CHAPTER 6 AN-initiated Session Modification and Release 67
Feature Summary and Revision History 67
Summary Data 67
Revision History 67
Feature Description 67
How it Works 68

CHAPTER 7 Cisco Common Data Layer 75
Feature Summary and Revision History 75
Summary Data 75
Revision History 75
Feature Description 76
Architecture 76
How it Works 77
Call Flows 77
CDL Endpoint Failure Call Flow 77
Limitations 78
Configuring the CDL Through SMF Ops Center 79
Configuring the CDL Session Database and Defining the Base Configuration 79
Configuring the Zookeeper in CDL 80
Sample Configuration 81
Configuring Event Trace Data 81
Verifying Event Trace Data 81

CHAPTER 8 Content Filtering and X-Header Enrichment 83
Feature Summary and Revision History 83
Summary Data 83
Revision History 83
Feature Description 83

Content Filtering 84
Feature Description 84
Configuring Content Filtering 84
Configuring Content Filtering under Active Charging Service 84
Configuring Content Filtering under Rulebase 84
Configuring Content Filtering under APN 85
Content Filtering Policy ID on N7 Interface 85
X-Header Insertion 85
Supported X-Header Information 85

CHAPTER 9 **Diameter Endpoint 87**
Feature Summary and Revision History 87
Summary Data 87
Revision History 88
Feature Description 88
Supported Interfaces 89
Diameter Endpoint Instance 89
Diameter Client Profile 89
Diameter Endpoint Profile 89
Disconnect Peer Request Management 90
Feature Description 90
DWR and DWA Handling 91
Feature Description 91
How it Works 91
Architecture 92
How it Works 93
Standards Compliance 93
Limitations 93
Configuring Diameter Endpoint 93
Configuring Diameter Endpoint Instances 93
Configuration Example 94
Configuration Verification 94
Configuring Diameter Client Profile 95
Configuration Example 95

Configuration Verification 96
Configuring Diameter Profile Endpoint on the Gx and Gy Interfaces 96
Configuration Example 99
Configuration Verification 100
Configuring Busy Time for DPR 102
Configuring Do Not Talk Time for DPR 102
Configuring Drain Time for DPR 103
Configuring Reboot Time for DPR 103
Dynamic Configuration Change 104
Feature Description 104
How it Works 104
Destination Host AVP for CCR and Retried Messages 105
Feature Description 105
Configuring Destination Host AVP 105
Configuration Example 106
Peer Management 106
Feature Description 106
Route Flags 107
Route Status 107
Considerations for Peer Management 108
Route Selection 108
Route Sort Order 109
Host Selection 109
Feature Description 109
How it Works 109
Configuring Host Selection through Diameter Endpoint 110
Route Failure 111
Feature Description 111
Configuring Route Failure 111
Bounded Peer 112
Feature Description 112
How it Works 112
Failure Handling 113
Feature Description 113

How it Works 113
Configuring Failure Handling 114
Configuring Failure Handling Profile 114
Configuration Example 116
Configuration Verification 117
OAM Support 118
Bulk Statistics Support 118
Troubleshooting Information 127
Monitor Protocol and Monitor Subscriber 127
Feature Description 127
How it Works 127
Configuring the Monitor Subscriber and Monitor Protocol Support 128
Debugging Data Collection 129

CHAPTER 10 DSCP Marking 131
Feature Summary and Revision History 131
Summary Data 131
Revision History 131
Feature Description 131
DSCP Marking for Data Packets 132
Feature Description 132
How the DSCP Marking Works for Data Packets 132
Configuring 5QI-QoS Mapping 132
Verifying DSCP Configuration for UP Packets 134
DSCP Marking for Control Plane Signaling 134
Feature Description 134
How the DSCP Marking Works for Control Signaling 134
Limitations 135
Configuring DSCP Marking for Control Plane Signaling 136
Configuring DSCP Marking per Endpoint 136
Configuring DSCP Marking per Interface 136
Verifying DSCP Configuration for CP Signaling Messages 137
OAM Support for DSCP Marking 137
Monitoring Support 137

CHAPTER 11 **Dynamic Routing by Using BGP** 139

Feature Summary and Revision History 139

Summary Data 139

Revision History 139

Feature Description 140

How it Works 140

External Network Failure 142

Geo Switchover 142

Internal Network Failure 143

Local Switchover 143

Recovery and Failback 143

Call Flows 144

Publish Route for Incoming Traffic in an Active-Standby Mode 144

Single Protocol Pod Failure Call Flow 145

Learn Route for Outgoing Traffic Call Flow 146

Configuring Dynamic Routing Using BGP 147

Monitoring and Troubleshooting 150

CHAPTER 12 **Emergency SoS Support** 155

Feature Summary and Revision History 155

Summary Data 155

Revision History 155

SoS Emergency Service Fallback to LTE 156

Feature Description 156

How it Works 156

Call Flows 156

Configuring Emergency SoS Support 158

Configuring Local Authorization 158

Configuring Secondary Authentication 159

Configuring Charging Failure Handling 159

Emergency Services Support 160

Feature Description 160

How it Works 160

Configuring Emergency Service Support 162
Configuring Default Flow Only Timer in DNN Profile 162
Configuring Emergency DNN 163
Verifying Emergency DNN 163
OAM Support for Emergency Services 164
Bulk Statistics Support 164

CHAPTER 13 EPS Interworking 165
Feature Summary and Revision History 165
Summary Data 165
Revision History 166
Feature Description 167
Architecture 168
How it Works 170
Standards Compliance 171
Support for UE Initial Attach 172
Feature Description 172
How it Works 172
Call Flows 172
Configuring UE Initial Attach 178
Define FQDN in SMF Profile Configuration 178
Configure S5 Binding Address 178
Configuring GTP Endpoint Parameters 179
Configuring APN-AMBR in CSR 179
Configuring PCRF, PCF, and OCS Interfaces 179
Verifying the UE Initial Attach Configuration 180
OAM Support 181
Show Command Support 181
Detach Procedure for EPS on SMF 182
Feature Description 182
How it Works 183
Dedicated Bearer Activation and Deactivation 191
Feature Description 191
How it Works 191

EPS Fallback 198
Feature Description 198
How it Works 198
EPS Fallback Trigger Cause Configuration 200
Indirect Data Forwarding Tunnel (IDFT) Timer Support 201
Feature Description 201
How it Works 201
Call Flows 201
Configuring the IDFT Timer 205
EPS Fallback Guard Timer Support 206
Feature Description 206
How It Works 206
Standards Compliance 208
Configuring the EPS Fallback Guard Timer 208
Generating EPS Fallback Report 209
Feature Description 209
How It Works 209
Call Flows 209
Bearer Modification for EPS Session on SMF 212
Feature Description 212
How it Works 212
Standards Compliance 227
Session Management Procedures for EPS and 5GC Interworking 227
Feature Description 227
How it Works 229
Call Flows 229
Standards Compliance 250
Generating EPS PDN Connection Parameters from 5G PDU Session Parameters 250
5G to EPS Handover Using N26 Interface 251
Feature Description 251
How it Works 251
Standards Compliance 253
Create Dedicated Bearer Delay and Retry Support 254
Feature Description 254

How It Works 254
Call Flows 254
Configuring Create Dedicated Bearer Delay and Retry Support 256
Handling Dedicated Bearer Procedure Failures Caused by Timer Expiry 257
Feature Description 257
How it Works 257
Call Flows 258
Configuring Dedicated Bearer Procedure Failure Handling Feature 263
Configuring Procedure SLA Timer 263
Verifying Dedicated Bearer Procedure Failure Handling Feature 263
OAM Support for Dedicated Bearer Procedure Failure Handling Feature 264
Bulk Statistics Support 264
Troubleshooting Information 264
Handling GTP-U Error Indication for 4G Sessions 265
Feature Description 265
Standards Compliance 265
How it Works 265
GTP-U Error Handling Procedure 265
GTP-U Error Indication with Diameter Interfaces 267
GTP Path Failure Handling, Restoration, and Recovery 267
Feature Description 267
Call Flows 268
GTP-C Path Management 269
GTP-C Echo Request Handling 270
GTP-C Restoration on PGW-C/SMF 270
Memory and Performance Impact 271
Configuring Echo at GTP Endpoint 271
Sample Configuration 271
Show Command 272
Bulk Statistics 272
Limitations 273
Configuration Support for Rejecting 4G-only Devices 273
Change Notification Request Handling 274
Feature Description 274

Change Notification with ULI Change 274
Change Notification with No Change in ULI 275
Call Flows 276
Change Notification with ULI Change 276
Change Notification with No Change in ULI 278
Dynamic Configuration Change Support 279
Feature Description 279
How it Works 279
Access Profile 279
Semantic and Syntactic Error Handling for 4G and 5G 281
Feature Description 281
Cause Handling 282
Configuration for Semantic and Syntactic Error Handling 284
Configuration Example 285
Bulk Statistics Support 286

CHAPTER 14 **Event Detail Records** 287
Feature Summary and Revision History 287
Summary Data 287
Revision History 288
Feature Description 288
EDR Transaction File 290
Procedure-level EDR Generation 293
EDR Transaction Collision 339
EDR Attributes 340
Limitations 348
Configuring EDRs 349
Configure EDR Reporting 349
Configure EDR Files for Generation 350
Configure EDR Parameters 350
Verifying EDR Transactions 353
OAM Support for EDR Logging 353
Bulk Statistics Support 354

CHAPTER 15 **Failure Handling Support** 355

Feature Summary and Revision History 355
Summary Data 355
Revision History 355
Feature Description 356
Access and Mobility Management Function Failure Handling 356
Feature Description 356
How it Works 357
Configuring Retransmission for Request Messages 357
Configuration Example 358
Charging Function Failure Handling 359
Feature Description 359
How it Works 360
Handling a CHF Server Failure 360
Relaying to an Offline CHF Server 360
HTTP Cause Code Mapping with Failure Actions 361
Application Error Code-based Failure Handling 361
Rating Group-level Failure Handling 361
Call Flows 362
SMF Behaviour for Failure Actions 365
Standards Compliance 366
Limitations 366
Configuring CHF Failure Handling 366
Configuring Failure Handling Profile 367
Configuring Offline Server Client and Offline Failure Handling Profile 367
Configuring Action for Rating Group-level and Application-level Errors 368
Network Repository Function Failure Handling 369
Feature Description 369
How it Works 369
Call Flow 370
Configuring NRF Failure Handling 372
Configuring the Failure Handling Template 372
Configuring Failure Handling Actions 374

Configuring NRF Failover Option 377
Configuring Failure Handling in Network Element Profile 378
Configuration Example 379
Verifying the NRF Failure Handling 380
NF Management Failure Handling 380
NF Discovery Failure Handling 381
Policy Control Function Failure Handling 382
Feature Description 382
How it Works 382
Configuring the PCF Failure Handling Feature 384
Configuring the PCF Failure Handling Profile 384
Configuring the Association of Failure Handling Profile 385
Configuring Secondary and Tertiary IP Addresses 385
OAM Support for PCF Failure Handling 386
Bulk Statistics Support 386
Unified Data Management Failure Handling 387
Feature Description 387
How it Works 388
Configuring UDM Failure Handling Feature 390
Configuring UDM Failure Handling Profile 390
Configuring Association of FH profile 390
Configuring Secondary and Tertiary IP Addresses 391
Configuring Response Timeout Parameter 392
Statistics 392
OAM Support for UDM Failure Handling Feature 392
Bulk Statistics Support 392
User Plane Function Failure Handling 393
Feature Description 393
Configuring the UPF Failure Handling Feature 394
Configuring UPF Failure Handling Profile 395
Configuring the Failure Profile Association 397
OAM Support 397
Statistics Support 398

CHAPTER 16 **Flow Failure Handling for Access and Mobility Procedures** 399

Feature Summary and Revision History 399

Summary Data 399

Revision History 399

Feature Description 400

How it Works 400

Call Flows 400

QoS Flow Failure Handling During Xn Handover 400

QoS Flow Failure Handling During N2 Handover 402

QoS Flow Failure Handling During N26 4G to 5G Handover 404

QoS Flow Failures for Service Request Procedures 407

PDU UE Synchronization Procedure 408

Handling Failed QoS Flow Identifier During PDU Setup Procedure 411

Handling Failed QoS Flow Identifier During PDU Session Modification 412

Flow Failure Management Call Flows 415

Standards Compliance 419

CHAPTER 17 **GTPP Endpoint** 421

Feature Summary and Revision History 421

Summary Data 421

Revision History 421

Feature Description 422

Charging Related Transfers 422

CDR Transport through GTPP 422

Path Protocol 423

GTPP Message Types 423

Endpoint GTP Prime 424

GTPP Resiliency 424

CDR Archiving 424

CDR File Storage 424

Information Elements Support 425

Standards Compliance 425

Limitations 426

Configuring the GTPP Profile 426
Verifying GTPP Profiles 428
Configuring the GTPP Endpoint 429
Verifying GTPP Endpoints 430
Verifying GTP Prime Configuration 430

CHAPTER 18 **Handover Procedures** 431
Feature Summary and Revision History 431
Summary Data 431
Revision History 431
Feature Description 432
4G to 5G Data Session Handover 432
Feature Description 432
How it Works 433
Architecture 434
Call Flows 434
Standards Compliance 446
Limitations 446
CHF and PCF Integration for Access and Mobility Procedures 447
Feature Description 447
How it Works 448
Call Flows 448
Standards Compliance 457
Inter gNodeB Handover 457
Feature Description 457
How it Works 457
Call Flows 457
Limitations 470
OAM Support 470
Statistics Support 470
Wi-Fi Handover 470
Feature Description 470
Architecture 471
Standards Compliance 474

How it Works 474
EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow 474
Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow 477
Non-3GPP Untrusted Wi-Fi to 5GS Handover with EPS Fallback Call Flow 480
Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow 487
5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow 491
Non 3GPP Untrusted LTE to WiFi Handover 494
IE Support for GTPC 496
Wi-Fi to 5G Handover with Alternate RAT Tunnel Creation Call Flow 497
5G to Wi-Fi Handover with Alternate RAT Tunnel Creation Call Flow 498
Configuring Wi-Fi Handovers 499
Configuring Compliance Profile 499
Configuring Calls with Handover Indication 500

CHAPTER 19 **IMS PDU Sessions for Voice 501**
Feature Summary and Revision History 501
Summary Data 501
Revision History 501
Feature Description 502
Voice Over LTE Support 502
Feature Description 502
How it Works 502
VoLTE and Emergency Call Prioritization Configuration 512
Standards Compliance 513
Limitations 513
NPLI Support for VoLTE and VoNR 513
Feature Description 513
Architecture 514
Call Flows 514
Standards Compliance 514
VoWi-Fi Support 515
Feature Description 515
Architecture 515
How it Works 515

Call Flows 515
Standards Compliance 521
Limitations 521
Voice over New Radio 521
Feature Description 521
Standards Compliance 521
Address Resolution Using DNS Proxy 522
Feature Description 522
Configuring the DNS Proxy for Address Resolution 522
Randomization of P-CSCF Addresses from DNS 524
DNS Test Query 525
Address Resolution Using Local Configuration 527
P-CSCF Address Selection Mechanism 527
Configure the P-CSCF Servers for Address Resolution 527
VoNR MO and MT Call Support 530
Feature Description 530
VoNR Paging Policy Differentiation 539
Feature Description 539
Configuring the VoNR Paging Profile Differentiation 542

CHAPTER 20 **Interfaces Support** 545
Feature Summary and Revision History 545
Summary Data 545
Revision History 546
Feature Description 548
3GPP Specification Compliance for SMF Interfaces 549
Feature Description 549
URI Version Selection Logic 550
Standards Compliance 550
Configuring 3GPP Specification Compliance for Interfaces 552
Configuration Verification 554
Supported SMF Interfaces 555
GTP Interface 555
GTP Cause Code Handling 555

GTPv2 IE and Cause Codes 562
Gx Interface 565
Feature Description 565
How it Works 565
Gx Initial Attach and Detach Support 566
Origin Host and Origin Realm for Gx 569
Dynamic and Predefined Rule Support 570
Gy Interface 571
Gy Usage Reporting 571
Gy Failure Handling 579
Gy MSCC Level Failure Result Codes 586
Gy Quota Validity Time (QVT) and Quota Holding Time (QHT) 590
Gy Tarrif Time Support 592
Origin Host and Origin Realm for Gy 593
Pending Traffic Treatment over Diameter Interfaces 594
Routing Data Support 594
Gz Interface 595
PDN Attach and Detach with Gz Interface 595
Gz Usage Reporting 604
Handling Modify Bearer Request Triggers 619
Gz Default Bearer Modification 631
Handling Periodic Report of Secondary RAT Usage 642
Support for EGCDR Final Record Closing Cause 648
Suppress CDR with Zero Volume 649
N1/NAS Interface 650
NAS Messages Compliance with Invalid Protocol Data Handling 650
5GSM Cause Code Handling 652
N2/NGAP Interface 657
N2 Cause and Diagnostic IE Support 657
N4 Interface 668
N4 Over IPSec 668
User Plane Integrity Protection 673
N7 Interface 680
Error Handling with HTTP Error Codes 680

Configuration-based Control of PCF Messages 685
N10 Interface 687
Configuration-based Control of UDM Messages 688
3GPP Release 16-Compliant N10 Attributes 690
S-NSSAI Validation Against the UDM Subscription S-NSSAI 690
N11 Interface 692
ProblemDetails JSON Object 693
Cause Information Elements 702
N16 Interface 711
ProblemDetails JSON Object 711
N40 Interface 717
Nnrf Interface 717
Configuration-based Control of NRF Messages 717
RADIUS Interface 719
S2b Interface 719
S5 Interface 720
SBA Interface 720
HTTP/2 with TLS 720
SCP Interface 724
Indirect Communication for NFs through SCP Model D 725
Configuring Interfaces 732
Configuration Example 734
Configuration Verification 735
OAM Support 736
Bulk Statistics Support 736

CHAPTER 21 **IP Address Management** 737
Feature Summary and Revision History 737
Summary Data 737
Revision History 738
Feature Description 739
How it Works 740
IPAM Integration in SMF 740
Feature Description 740

Architecture 741
IPAM Integration 741
Components 741
How it Works 741
Call Flows 741
Configuring IPAM 743
Configuring IPv4 Address Ranges 744
Configuring IPv6 Address Ranges 745
Configuring IPv6 Prefix Ranges 745
Configuring IPv4 Address and Prefix Ranges with Next Hop Forwarding Address 746
Configuring IPv6 Address Ranges with Next Hop Forwarding Address 747
Configuring SMF Tags 749
Configuring IPv4 Address Range Threshold 750
Configuring IPv6 Address Range Threshold 751
Configuring IPv6 Prefix Range Threshold 751
Configuring IPv4 Address Range Split 752
Configuring IPv6 Address and Prefix Address Range Split 753
Configuring Global Threshold 754
Configuring IPAM Source 755
Verifying the IPAM Integration Configuration 755
Verifying the Details of a Data Plane 755
Verifying the Threshold for Data Plane 755
Verifying the IPv4 Address Range Assigned to a Data Plane 756
Verifying the IPv6 Address Range Assigned to a Data Plane 756
Configuring IP Pool Selection Method 757
Configuring UPF Group Profile for IP Pool Selection 757
Configuring Slice Group List for IP Pool Selection 758
Static IP Support 759
Feature Description 759
How it Works 760
Call Flows 762
Adding a DNN 763
Adding a Static IP Address Range 764
Adding a Static IP Pool 764

Adding the UPF 765
Deleting the UPF 765
Deleting a Static IP Address Range 765
Deleting a Static IP Pool 766
Removing Sx Association with an Offline UPF 766
Sx Path Failure on UPF 766
Limitations 766
Configuring Static IP Support 767
Statistics Support 767
Dual-stack Static IP Support Through IPAM 768
Feature Description 768
How it Works 768
Limitations 769
Configuring Dual-stack Static IP 769
Configuring IPAM No-Split 769
IPAM Offline Mode Support 769
Feature Description 769
How it Works 769
Configuring the IPAM Offline Mode 770
Configuring Pool to Offline Mode 770
Setting IPv4 Address Range to Offline Mode 770
Setting IPv6 Prefix Ranges to Offline Mode 771
IPAM Redundancy Support Per UPF 771
Feature Description 771
How it Works 772
IPAM Quarantine Timer 772
Feature Description 772
Configuring IPAM Quarantine Timer 773
Configuring IPAM Quarantine Timer 773
IP Address Validation with CDL Configuration 773
System Diagnostics IP Validation 773
Statistics 774
IPAM Data Reconciliation 775
Feature Description 775

Triggering IPAM Reconciliation 775
Triggering IPAM Reconciliation at Instance Level 775
Triggering IPAM Reconciliation at Pool Level 775
Triggering IPAM Reconciliation at Chunk Level 775
IPAM Periodic Reconciliation 775
Limitations 776
Feature Configuration 776
Configuration Example 777
Configuring IPAM Quarantine Qsize 777
Configuring IPAM Quarantine Queue Size 777
Overlapping IP Address Pools 778
Feature Description 778
Configuring Overlapping IP Address Pools 778
Auto-Reclamation of Under-Utilized IP Chunks 779
Feature Description 779
Limitations 779
Configuring Instant Reclamation Process for Under-Utilized IP Chunks 780
Configuration Example 780
Configuring Periodic Reclamation Process for Under-Utilized IP Chunks 780
Configuration Example 781
Configuration Verification 781
OAM Support 781
Bulk Statistics 782
Unique IP Pools for UPFs 782
Feature Description 782
Configuring SMF for Unique IP Pools 782
Configuring Tags Based on Location DNN 782
Enabling UPF Fallback 783
Configuration Example 783
Reconciliation of IP Chunks between SMF and UPF 786
Feature Description 786
How It Works 786
Configuration to Enable or Disable Reconciliation of IP Chunks 787
Configuration Example 787

OAM Support 787
Bulk Statistics 787
IP Chunk Throttling 788
Feature Description 788
How It Works 788
Limitations 788
Configuring Maximum Supported Session for UPF on SMF 789
Configuration Example 789
Configuring Maximum Sessions Supported Per vDNN Per UPF 789
Configuration Example 790
OAM Support 791
Metrics 791
Route Aggregation to Handle Switch Limit 791
Feature Description 791
How It Works 791
Migration of Old Pools Without Chunk-Group into Pools with Chunk-Group 792
Limitations 793
Configuring IPv4 Address Range to Define Chunk Group Size 793
Configuration Example 794
Configuration Verification 795
Configuring IPv6 Prefix Range to Define Chunk Group 795
Configuration Example 795
Configuring IPv6 Address Range to Define Chunk Group 796
Configuration Example 796
Configuration Verification for IPv6 Prefix Range and Address Range 796
Pre-Allocation of IP Chunks Based on Maximum Session Size 797
Configuration Example 798
OAM Support 798
Metrics 798
NAT Support 799
Feature Description 799
How it Works 800
Call Flows 800
PFCP IEs for NAT Binding Procedure 805

Handling Network Address Translation Binding Record at SMF 807
Radius AVPs for NAT Binding Procedure 807
Limitations 808
Configuring NAT Binding Update 808
OAM Support 808
Bulk Statistics 808
Troubleshooting Information 809
Range of IPv6 Allocated to UPF 809
Range of IPv4 Allocated to UPF 809
IP Pool Mapping Error Logs 810
Releasing N4 Resources or Association 811
Feature Description 811
How It Works 811
Configuration for Releasing N4 Resources or Associations 811
OAM Support 812
Identification of Corrupted IP Chunks 813
Feature Description 813
How It Works 813
OAM Support 813

CHAPTER 22 **IPv6 PDU Sessions** 815
Feature Summary and Revision History 815
Summary Data 815
Revision History 815
Feature Description 816
Unsolicited Router Advertisement 816
Solicited Router Advertisement 816
Configuring Router Solicit and Router Advertisement 817
Configuring Router Advertisement Parameters 817
Configuring Virtual MAC Address 818
Associating the ICMPv6 Profile with SMF Service Profile 819

CHAPTER 23 **MBR Short Circuit Optimization** 821
Feature Summary and Revision History 821

Summary Data 821
Revision History 821
Feature Description 821
How it Works 822
Limitations 822
MBR Short Circuit Optimization Support 823
Statistics 823

CHAPTER 24 Mesh Connectivity to All UPFs 825
Feature Summary and Revision History 825
Summary Data 825
Revision History 825
Feature Description 825

CHAPTER 25 MTU Support in PCO 827
Feature Summary and Revision History 827
Summary Data 827
Revision History 827
Feature Description 827
Configuring IPv4 Link MTU 828
Configuration Verification 828

CHAPTER 26 DNN Support 831
Feature Summary and Revision History 831
Summary Data 831
Revision History 831
Feature Description 832
How It Works 833
Limitations 834
Configuring Virtual DNN 834
Configuring Subscriber Policy 834
Configuration Verification 836
Configuring Operator Policy and Associating a DNN Policy 836
Configuring a DNN Policy 837

Configuring a Virtual DNN under a DNN Profile 837
Associating Subscriber Policy under the SMF Service 838
Network Function Selection based on SMF Instances 839
Feature Description 839
Configuring SMF Instances 840
Switching DNN Profile to Offline Mode During Dynamic Config Update 841
Feature Description 841
How it Works 841
DNN Policy 841
DNN Profile 841
Subscriber Policy 842
Limitations 843
Configuring the Offline DNN Profile 843
Switching the DNN Profile to Offline Mode 843
Verifying the DNN Profile Offline Mode Configuration 843
OAM Support for DNN Profile Offline Mode Setting 844
Bulk Statistics Support 844
DNN Inheritance 844
Feature Description 844
How it Works 844
Configuring DNN Inheritance 848
IP Pool Allocation per DNN 849
Feature Description 849
How it Works 849
Configuring IP Pool Allocation 850
Allocating the IP Pool per DNN 851
Verifying IP Pool Allocation Configuration 851
IP Pool Allocation per Slice and DNN 851
Feature Description 851
How it Works 852
Limitations 852
Feature Configuration 852
Configuring Allowed NSSAI Values 852
Configuring Slice-based IP Pool Allocation 853

CHAPTER 27 **Multiple PLMN Support** 855

Feature Summary and Revision History 855

Summary Data 855

Revision History 855

Feature Description 856

How it Works 856

Configuring Multiple PLMNs 856

Configuration-based Peer NF Selection 856

Configuring PLMN ID 857

Configuring Non-standard PLMN List 857

Verifying Non-standard PLMN List 857

Configuring Primary PLMN 858

Configuring PLMN in NRF Discovery 858

Configuring Serving PLMN MNC list 858

Configuring Roamer in Operator Policy 859

OAM Support for Multiple PLMNs 859

Bulk Statistics Support 859

CHAPTER 28 **N3IWF for Non-3GPP Access** 861

Feature Description 861

Architecture 862

How it Works 862

Call Flows 862

Standard Compliance 863

OAM Support 864

CHAPTER 29 **Network-initiated Session Modification Procedures** 865

Feature Summary and Revision History 865

Summary Data 865

Revision History 865

Feature Description 866

How it Works 866

Call Flows 866

Network-initiated Modification Call Flow for Active User Plane and UE in CM-Connected State 866
Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State 868
Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State 868
Standards Compliance 870
OAM Support 870
Bulk Statistics Support 870

CHAPTER 30 New Radio Dual Connectivity 871
Feature Summary and Revision History 871
Summary Data 871
Revision History 871
Feature Description 871
How it Works 872
Call Flows 872

CHAPTER 31 NF Discovery and Management 877
Feature Summary and Revision History 877
Summary Data 877
Revision History 877
Feature Description 878
NF Management 878
Feature Description 878
Registration 879
Configuring NRF Endpoints Profile Parameters for NF Management 879
SMF Deregistration with NRF 881
Feature Description 881
How it Works 882
NF Heartbeat 884
Feature Description 884
How it Works 885
Configuring NRF Heartbeat Interval 886
NRF Support for SMF Subscription and Notification 886

Feature Description 886
How it Works 888
Configuring NRF for Subscription and Notification 892
NF Profile Update 893
Feature Description 893
How it Works 893
NF Discovery 896
Feature Description 896
How it Works 897
Call Flows 897
Standards Compliance 899
Limitations 899
Configuring NRF for Discovery 899
Registering NRF 899
Discovering NRF 900
Configuring NF Client Profile 900
Associating a Discovery Group with NF Type 902
Configuring NF Endpoint Profile Parameters in NRF Discovery Group 902
Configuring Locality for NF Types 904
Configuring Locality for SMF 905
Configuring NF Profiles for a DNN 905
Defining Locality within NF Profile 906
Configuring NF Endpoint Profile Parameters in NF Client Profile 907
NRF Selection per Peer NF Type 909
Feature Description 909
Configuring the NRF Selection per Peer NF Type 910
Caching for Discovered NF Profiles 913
Feature Description 913
How it Works 913
NF Discovery Cache Invalidation 914
Static Configuration for Peer NF Management 915
Fallback to Static IP Address Support 915
Feature Description 915
How it Works 915

Configuring Fallback to Static IP Address 917
NRF Failure Handling 920
Feature Description 920

CHAPTER 32 Overload Management 921
Feature Summary and Revision History 921
Summary Data 921
Revision History 921
Feature Description 922
SBA Interface Overload Control 922
Feature Description 922
How it Works 922
Message Priority 923
Overload Protection at Endpoint 923
Configuring Overload Protection 923
Configuring Overload Protection at Endpoint Level 923
Configuring Overload Protection at Client Level 924
Verifying the Overload Protection Configuration 925
Configuring the Message Priority 925
Monitoring and Troubleshooting 926
Statistics 926
GTP-C Load and Overload Control 927
Feature Description 927
GTP-C Load Control 928
GTP-C Overload Control 928
Message Throttling 929
Overloaded Peer Detection 929
How it Works 930
Standards Compliance 932
Limitations 932
Configuring GTP-C Load and Overload Control Feature 932
Create Load Profile 933
Create Exclude Profile 934
Create Overload Profile 935

Associate Load and Overload Profiles 938
OAM Support for GTP-C Load and Overload Control 939
Bulk Statistics Support 939
Node Overload 940

CHAPTER 33 **Performance Optimization Support 943**
Feature Summary and Revision History 943
Summary Data 943
Revision History 944
Feature Description 945
Batch ID Allocation, Release, and Reconciliation Support 945
Feature Description 945
How it Works 946
Feature Configuration 947
OAM Support 947
Cache Pod Optimization 948
Feature Description 948
CDL Flush Interval and Session Expiration Tuning Configuration 948
Feature Description 948
Feature Configuration 948
Domain-based User Authorization Using Ops Center 949
Feature Description 949
How it Works 949
Feature Configuration 950
Configuration Example 951
Configuration Verification 951
Edge Echo Implementation 952
Feature Description 952
How it Works 952
OAM Support 953
Bulk Statistics Support 953
Encoder and Decoder Optimization for GTPC Endpoint Pod 953
Feature Description 953
Feature Configuration 954

ETCD Peer Optimization Support 954
Feature Description 954
How it Works 954
Roaming Peer Optimization 955
Feature Description 955
How It Works 955
Roaming Peer Detection Based on Interface 955
Roaming Peer Detection by Application 955
Peer Optimization 955
Limitations 956
Feature Configuration 956
Configuration Example 957
Configuration Verification 957
ETCD Traffic Optimization 957
Feature Description 957
How It Works 958
ETCD Client Fallback 958
Feature Description 958
ETCD Client Load Balancer 959
ETCD Client Retry Mechanism 959
Flag DB Database Updates 959
Feature Description 959
Handling PDU Session Modifications based on RRC Inactive Cause Codes 960
Feature Description 960
How it Works 960
Call Flows 961
Feature Configuration 966
Configuration Example 967
Configuration Verification 967
Pod Failure Detection using K8 Liveness Probe 967
Resiliency Handling 968
Feature Description 968
How it Works 968
Feature Configuration 969

Configuration Example 970
Configuration Verification 971
OAM Support 971
Bulk Statistics Support 971
Monitoring Support 972

CHAPTER 34 **Pods and Services Reference** 973
Feature Summary and Revision History 973
Summary Data 973
Revision History 973
Feature Description 974
Pods 975
Replicas 976
UDP Proxy Pod 977
Feature Description 977
Node Monitoring Pod 978
Configure Node Monitoring Pod 978
Services 979
Open Ports and Services 981
Associating Pods to the Nodes 983
Viewing the Pod Details and Status 983
States 984
GTPC Protocol Endpoint Merge with UDP Proxy Bypass 985
Feature Description 985
UDP Proxy Functionality Merge into Protocol Micro-services 985
Feature Description 985
How it Works 986

CHAPTER 35 **Policy and User Plane Management** 989
Feature Summary and Revision History 989
Summary Data 989
Revision History 990
Feature Description 991
QoS Management on SMF 992

Feature Description 992
Use Cases 992
Subscribed QoS 995
QoS Negotiation 995
QoS Flow Management 996
QoS Communication on 3GPP Interfaces 998
QoS Modification 999
Qos Capability Support for PCF and SMF Interaction 999
Bit Rate Mapping Support 1000
Feature Description 1000
How it Works 1001
Standards Compliance 1001
Configuring Bit Rate Mapping 1002
Verifying the Feature Configuration 1002
Bitrate Mapping across Diameter Interfaces 1002
Configuring Bit Rate Mapping with Diameter Interfaces 1003
Handling of Authorized QoS for Default Bearer 1003
Feature Description 1003
How it Works 1004
Default-Bearer QoS Handling for 4G and WiFi Sessions 1004
Default-Bearer QoS Handling for 5G Sessions 1004
Default-Bearer QoS Handling During WiFi Handovers 1005
Default-Bearer QoS Modification During Failure Handling 1005
Limitations 1006
Authorized QoS Handling OAM Support 1006
Statistics Support 1006
GBR Bearer Creation Based on Local Policy 1006
Feature Description 1006
How It Works 1006
Creating Default Non-GBR Bearer and Dedicated GBR Bearer Without PCF 1007
5G Attach with Dedicated GBR Bearer Creation 1007
4G Attach with Dedicated GBR Bearer Creation 1010
Limitations 1011
Configuration for Creating Default Non-GBR Bearer and Dedicated GBR Bearer without PCF 1011

Configuration for Associating QoS Profile and Event Management Policy to the DNN Profile 1011
Configuration for Adding Event Management Policy 1012
Configuration for Adding Rule Definition Policies 1012
Configuration for Adding Action Definition Policies 1013
Configuration Example 1013
OAM Support 1015
Metrics 1015
SMF-triggered Metadata for EDR Generation on UPF 1015
Dynamic Configuration Update 1015
Feature Description 1015
How it Works 1016
Configuring Dynamic Configuration Change Support 1017
Verifying Dynamic Configuration Change Support Configuration 1017
Dynamic PCC Rules Enforcement 1018
Feature Description 1018
Supported Features Negotiation 1018
Provisioning and Management of Session AMBR and Default QoS 1019
Provisioning of Policy Revalidation Time 1020
Provisioning and Management of Additional QoS Flows 1020
QoS Enforcement 1022
Policy Control Request Triggers 1022
Gating Control 1024
How it Works 1024
Standards Compliance 1026
Limitations 1027
Configuring the Dynamic PCC Rules Enforcement Feature 1027
Creating QoS Profile 1027
Configuring QoS Parameters 1027
Defining QoS Profile in DNN Profile Configuration 1028
Verifying the Dynamic PCC Rules Enforcement Feature Configuration 1028
Controlling PCF and SMF Interaction 1029
Handling Traffic Flow for Dedicated UE Services 1031
Feature Description 1031
How It Works 1031

N7 Optimization 1033
Feature Description 1033
How it Works 1033
Configuring N7 Optimization 1037
OAM Support 1038
Dynamic QoS Flow-based Application Detection and Control 1039
Feature Description 1039
How it Works 1039
Interface Details 1039
Limitations 1040
Static PCC Rules Support 1041
Feature Description 1041
Relationships 1041
How it Works 1041
Pre-processing During Configuration 1042
During PDU Session Creation 1042
During PDU Session Modification 1043
Configuring the Static PCC Rules 1044
Configuring Charging Action 1044
Configuring Packet Filter 1046
Configuring ACS Ruledef 1047
Configuring ACS Group of Ruledefs 1048
Configuring Rulebase and Predefined Rule Prefix 1049
Configuring ACS Rulebase in APN Configuration Mode 1049
Configuring URR ID 1050
Configuring GTPP Group 1050
Configuring APN 1050
Associating GTPP Group with APN 1051
Configuring ACS Rulebase in ACS Configuration Mode 1051
Defining UPF APN Profile in DNN Profile Configuration 1053
Configuring QoS Parameters 1053
Verifying the Static PCC Rules Support Feature Configuration 1054
Predefined PCC Rules 1056
Feature Description 1056

Predefined Rules vs Static Rules 1056
Combined Application of Static, Predefined, and Dynamic Rules 1056
Bearer QCI Support 1057
Feature Description 1057
Non-standard QCI Support for Dynamic PCC and Session Rules 1059
Feature Description 1059
How it Works 1060
Limitations 1060
OAM Support 1060
Statistics Support 1060
Troubleshooting Information 1061
Support for Configuring the Bandwidth ID 1061
Feature Description 1061
Limitations 1061
Configuring Bandwidth ID 1061
Verifying Bandwidth ID Configuration 1062
Generating UE Camping Report for PCF 1063
Feature Description 1063
UPF Node Selection 1063
UPF Selection Based on Query Parameters 1064
Feature Description 1064
How it Works 1065
Configuring the UPF Selection Feature 1068
UPF Selection OA&M Support 1078
IP Threshold-based UPF Selection 1079
Feature Description 1079
How it Works 1079
OAM Support for IP Threshold-based UPF Selection 1080
Co-located UPF Selection During Initial EPS Attach 1081
Feature Description 1081
How it Works 1081
Configuring Node ID 1082
Statistics Support 1082
Co-located UPF Selection During Handover 1083

Feature Description 1083
Configuring Parameters for Co-located UPF Selection 1083
Support for UPF Node Reports and Proprietary Session Reports 1084
Feature Description 1084
How it Works 1085
PFCP Node Report Handling 1085
PFCP Session Report Handling 1085
Collision Handling 1085
Resiliency Handling 1085
Standards Compliance 1086
Limitations 1086
OAM Support 1086
Monitoring Support 1086
Show Command Support 1087
Statistics Support 1088
Outer Header Format 1090
Feature Configuration for Outer Header IE 1091
Usage Monitoring over PCF 1092
Feature Description 1092
How it Works 1092
Usage Reporting 1092
Usage Monitoring Data Modification 1093
Error Handling 1094
Call Flows 1094
Standards Compliance 1096
Limitations 1096
Configuring Usage Monitoring Key for Pre-defined Rules 1096
Configuration Verification 1097
OAM Support 1097
Usage Monitoring Statistics 1097
QoS Group of Ruledefs Support over N7 1098
Feature Description 1098
How it Works 1098
QGR Processing Flow 1099

QGR Parameters 1099
Data Path Enforcement 1104
Call Flows 1105
Limitations 1108

CHAPTER 36 **RADIUS Authentication and Accounting 1109**
Feature Summary and Revision History 1109
Summary Data 1109
Revision History 1109
Feature Description 1110
RADIUS Authentication 1112
Throughput Limiting 1112
RADIUS Accounting 1113
Handling RADIUS Disconnect Request Messages 1114
Architecture 1115
RADIUS Client Integration in SMF 1115
How it Works 1116
RADIUS Interaction for Authentication 1116
RADIUS Authentication Attributes 1119
Call Flows 1121
RADIUS Interaction for Accounting 1122
RADIUS Accounting Attributes 1123
Call Flows 1126
Processing of Usage Reporting Rules 1128
Dynamic Configuration Update 1128
RADIUS Attribute Definition 1129
Standards Compliance 1138
Limitations and Restrictions 1138
Configuring the RADIUS Client 1138
Configuring RADIUS Server 1139
Verifying the RADIUS Configuration 1140
Configuring RADIUS Server Selection Logic 1140
Configuring RADIUS Attributes 1141
Enabling RADIUS Authentication Allow Parameter 1142

Configuring Consecutive Failure 1142
Configuring Internal Virtual IP for Protocol Endpoint 1143
Configuring RADIUS Detect Dead Server 1144
Configuring RADIUS Dead Time 1144
Configuring RADIUS Dictionary 1145
Configuring RADIUS Retries 1145
Configuring Max Transmissions 1146
Configuring RADIUS Timeout 1147
Configuring RADIUS Pod 1147
Configuring RADIUS NAS-IP 1148
Configuring Secondary Authentication Method 1150
Verifying the RADIUS Authentication Configuration 1150
Configuring PAP, CHAP, or MSCHAP-based Authentication 1151
Defining Priority for Authentication Algorithm 1151
Configuring Host Password 1151
Enabling RADIUS Accounting 1152
Defining RADIUS Server Group in DNN Profile 1153
Configuring RADIUS Accounting Options 1153
Configuring RADIUS Accounting Server Group 1154
Verifying the RADIUS Accounting Configuration 1154
Configuring the Session Disconnect Feature 1155
Configuring the Dynamic Authorization Service 1155
Configuring the CoA-NAS Interface 1156
RADIUS Client OA&M Support 1157
Statistics Support 1157
Troubleshooting Information 1163
RADIUS Bulk Statistics 1163
Subscriber Details for RADIUS-specific Information 1175
RADIUS Endpoint Authentication and Accounting Statistics 1175
RADIUS Endpoint Disconnect Message and CoA Statistics 1176
External Inbound and Outbound Connections 1177
Internal and External Connections 1177
Status of Pods 1177
Configuration Errors 1177

show alerts 1177
RADIUS Alerts 1179
RADIUS EP Down Alert 1179
RADIUS Accounting Establishment Failure Threshold Alert 1180
RADIUS Accounting Release Failure Threshold Alert 1180
RADIUS Authentication Failure Threshold Alert 1180
RADIUS Disconnect Message Failure Threshold Alert 1181
RADIUS Server RTT Alert 1181
RADIUS Accounting Start Initial Message Failure Threshold Alert 1181
RADIUS Accounting Interim/Update Message Failure Threshold Alert 1181
RADIUS Accounting Stop/Terminate Message Failure Threshold Alert 1182
RADIUS Authentication Type Message Failure Threshold Alert 1182
Grafana Charts 1182
Error Logs 1183
RADIUS Authentication 1183
RADIUS Accounting 1184
Idle Timeout-based Release 1185
Disconnect Message 1185
RADIUS Test CLI support 1186
Testing a RADIUS Accounting Server 1186
Testing a RADIUS Authentication Server 1187

CHAPTER 37 **Redundancy Support** 1189
Feature Summary and Revision History 1189
Summary Data 1189
Revision History 1190
Feature Description 1190
Types of Redundancies Supported 1190
High Availability Support 1191
Feature Description 1191
High Availability of UDP Proxy 1191
High Availability of Node Manager 1191
High Availability Inside Rack 1192
Architecture 1192

SMF Pod and VM Deployment Layout 1192
How It Works 1193
Configuring Pod-level Labelling and Replicas 1194
Configuration Example 1194
Configuration Verification 1195
Traffic Monitoring on L2 VIP for Active Instance 1195
Feature Description 1195
How It Works 1196
Configuring HA and GR Scenarios 1196
OAM Support 1197
Inter-Rack Redundancy Support 1198
Feature Description 1198
How It Works 1198
Overview 1198
Inter-Rack Redundancy Triggers 1200
Rack NF Roles 1200
General Guidelines 1201
Instance Awareness 1202
Configuring Inter-Rack Redundancy Instance 1202
Configuring Endpoint Instance Awareness 1203
Configuring Profile SMF Instance Awareness 1204
Dynamic Routing 1204
Configuring Dynamic Routing Using BGP 1207
Configuring BGP Speaker 1210
IPAM 1211
Configuring IPAM 1212
Geo Replication 1213
Configuring ETCD/Cachepod Replication 1214
Geo Monitoring 1214
Pod Monitoring 1215
Remote Cluster Monitoring 1215
Traffic Monitoring 1216
Geo Redundancy Strengthening 1216
How It Works 1217

OAM Support 1217
BFD Monitoring 1218
CDL GR Deployment 1221
Prerequisites for CDL GR 1221
CDL Instance Awareness and Replication 1221
Lawful Intercept 1225
RADIUS Configuration 1226
Software Upgrade on GR Pairs 1227
GR CLI 1231
Geo Replication Pull Data 1231
Geo Reset Role 1231
Geo Switch Role 1232
Troubleshooting 1232
show/clear Commands 1232
Monitor Subscriber 1243
Monitor Protocol 1244
Geographic Redundancy OAM Support 1245
Health Check 1245
Recovery Procedure 1249
Key Performance Indicators (KPIs) 1251
Bulk Statistics 1256
Alerts 1259
Inter-site Geographic Redundancy 1265
Feature Description 1265
Architecture 1265
Prerequisites 1265
General Guidelines 1266
How It Works 1266
BGP Route Advertisement 1266
Configuration for Inter-site Deployment 1269
L3 Routing of Pods 1270
Inter-site Redundancy Scenarios 1271
Split Brain 1272
KPI 1273

CHAPTER 38 **Roaming Support** 1281

Feature Summary and Revision History 1281

Summary Data 1281

Revision History 1282

Feature Description 1282

Local Breakout Roaming Support 1283

Feature Description 1283

Architecture 1283

Home Routed Roaming Support 1291

Feature Description 1291

Architecture 1291

How it Works 1296

vSMF Create Session Procedure 1296

hSMF Create Session Procedure 1299

vSMF Modify Session Procedure 1300

hSMF Modify Session Procedure 1302

vSMF Release Session Procedure 1303

hSMF Release Session Procedure 1304

vSMF Clear Subscriber Release Session Procedure 1305

EPS to 5G Handover Using N26 Interface 1306

5GS to EPS Handover for Single Registration Mode with N26 Interface 1309

EPS to 5G Handover Without Using N26 Interface 1311

5G to EPS Handover Without Using N26 Interface 1313

Standards Compliance 1314

Limitations 1315

Charging Support for HR Roaming 1315

Configure Charging for HR Roaming 1318

Default DNN Support in HR Roaming 1319

IPv6 RS/RA Support in HR Roaming 1320

SEPP Support 1320

Feature Description 1320

How it Works 1320

Configuring the SEPP 1324

OAM Support 1327
N3 and N9 User Plane Separation 1328
Homer Calls with N3 and N9 Separation 1331
Dedicated Bearer Call Flow 1331
Roamer Calls with N3 and N9 Separation 1331
Allowed PLMN List Support 1332
Inter-plmn Roaming Mobility Support 1332
Limitations and Restrictions 1333
Standards Compliance 1334
How it Works 1334
Call Flows 1334
Configuring the Inter PLMN Handover 1340
Sending DTSSA and ACSCR 1341
OAM Support 1342
Bulk Statistics Support 1342
Roaming Status on N4 Interface 1342
Troubleshooting Information 1343
Subscriber Details for Roaming-specific Information 1343
Subscriber Details for Roaming-specific Information for hSMF 1343
Subscriber Session Details for Roaming-specific Information for hSMF 1351
Subscriber Details for Roaming-specific Information for vSMF 1353
Subscriber Session Details for Roaming-specific Information for vSMF 1357
Roamer UE Alerts 1358
In-roamer UE Failure Threshold Alert 1358
Out-roamer UE Failure Threshold Alert 1359
Roamer UE Bulk Statistics 1359
Roaming Error Logs 1360

CHAPTER 39 **Session and Service Continuity Mode** 1363
Feature Summary and Revision History 1363
Summary Data 1363
Revision History 1363
Feature Description 1363
SSC Mode Selection 1364

Priority for Choosing SSC Mode 1364
SSC Mode Selection Method 1364
Configuring SSC Mode 1365

CHAPTER 40 **Session Timers** 1367
Feature Summary and Revision History 1367
Summary Data 1367
Revision History 1367
Feature Description 1368
3GPP-Compliant Timers 1369
GTP and N11 Timers 1369
Feature Description 1369
How it Works 1369
Standards Compliance 1369
Configuring the N11 and GTP Timers 1369
Back-off Timer Support 1371
Feature Description 1371
How it Works 1371
Standards Compliance 1377
Configuring Back-off Timer 1378
Non-3GPP Compliant Timers 1380
Feature Description 1380
Configuring Non-3GPP Session Timers 1381
Configuration Example 1382
Configuration Verification 1382

CHAPTER 41 **SMF Capabilities to Support 4G and 5G Devices** 1383
Feature Summary and Revision History 1383
Summary Data 1383
Revision History 1383
Feature Description 1384
How it Works 1386
Standards Compliance 1386
Limitations 1386

Configuring Parameters to Support 4G and 5G Devices 1387
Configuring the NSSAI 1387
Enabling DCNR in DNN Profile 1388
Configuring UPF Selection 1388
Configuring Secondary RAT Usage Report 1389
Configuring Presence Reporting 1390
Configuration Verification 1390
OAM Support 1391
Statistics Support 1391
Bulk Statistics 1392
Troubleshooting Information 1393
Subscriber Details with DCNR and Presence Reporting Enabled 1394
Option-3x: DCNR Enabled UE Alerts 1395
DCNR UE Attach Failure Threshold Alert 1395
DCNR UE Attach Failure Threshold Alert with Presence Reporting 1395
DCNR UE Bulk Statistics 1396
Option-3x Device Specific Error Logs 1396

CHAPTER 42 **SMF Serviceability** 1399
Feature Summary and Revision History 1399
Summary Data 1399
Revision History 1400
Feature Description 1400
Relationships 1400
How it Works 1401
Call Failure Logs 1405
Configuring the Call Failure Logs 1406
Configuration Example 1406
Configuration Verification 1406
Procedure Failure Logs 1406
Configuring the Procedure Failure Logs 1407
Configuration Example 1408
Configuration Verification 1408
Generic Procedure Failure Logs 1409

Configuring the Generic Procedure Failure Logs 1409
Configuration Example 1410
Configuration Verification 1410
Additional Call Flow Failure Logs 1410
Configuring the Additional Call Flow Failure Logs 1411
Configuration Example 1412
Configuration Verification 1412
Event Trace Logs 1413
Configuring the Event Trace Logs 1416
Configuration Example 1416
Configuration Verification 1416
Call Flow Statistics Logs 1417
Configuring the Call Flow Statistics Logs 1418
Configuration Example 1418
Configuration Verification 1418
Core Dump Utility Logs 1418
Configuring the Core Dump Utility Logs 1419
Configuration Example 1419
Configuration Verification 1419
Monitor Subscriber (MonSub) Logs 1420
Configuring the Monitor Subscriber Logs 1422
Configuration Example 1423
Configuration Verification 1423
N40 Additional Logs and Statistics 1424
Configuring the N40 Additional Logs and Statistics 1424
Configuration Example 1425
Configuration Verification 1425
N7 Additional Logs and Statistics 1425
Configuring the N7 Additional Logs and Statistics 1426
Configuration Example 1426
Configuration Verification 1426

CHAPTER 43 **Subscriber Charging** 1427
Feature Summary and Revision History 1427

Summary Data 1427
Revision History 1427
Feature Description 1428
Converged Charging 1430
Chargeable Events 1430
Charging Identifier 1430
Charging Information 1431
How it Works 1431
Charging Session 1431
Offline Charging and Online Charging 1432
CHF Selection 1435
Charging Activities at SMF 1435
Static and Predefined Rules for Charging 1443
Modification Scenarios in Charging 1444
URR Linking 1445
Local Configuration 1445
Zero Usage Report Suppression 1446
Call Flows 1447
Limitations 1449
Standards Compliance 1449
3GPP June 2019 Compliance for Charging Interface 1449
Configuring SMF Charging 1450
DNN Profile Configuration 1450
Charging Characteristics Profile Configuration 1450
Charging Characteristics ID Configuration 1450
Charging Profile Configuration 1451
Mapping of Charging Scenario on Various Interfaces 1455
Feature Description 1455
How it Works 1455
Limitations 1461
Standards Compliance 1461
Failure Handling Scenarios 1461
Application Error and Result Code Handling 1462
N40 Application Error Codes 1462

Gy Application Error Codes 1463
RG-level Result Codes 1466
Handling Charging Disable Functionality 1467
Charging Server Reconciliation 1468
Dynamic Update of Charging Configurations 1468
Feature Description 1468
How it Works 1469
ACS Profile 1469
Charging Profile 1472

CHAPTER 44 TAI Selection from AMF 1477
Feature Summary and Revision History 1477
Summary Data 1477
Revision History 1477
Feature Description 1477
How it Works 1478
Configuring TAI Selection Feature 1480
Configuring TAI Group List 1480
Verifying TAI Group List 1480
Configuring TAI Group 1481
Configuring TAC List 1481
Configuring TAC Range List 1481
Verifying the TAI Group Configuration 1482
Configuring Priority 1482
Verifying the Priority Configuration 1482

CHAPTER 45 UDM Integration 1485
Feature Summary and Revision History 1485
Summary Data 1485
Revision History 1485
Feature Description 1486
How it Works 1486
Configuring UDM 1486
Configuring Options for Controlling SDM Messages 1486

Configuring RAT Type 1486
Configuring Session Type 1487
Configuration to Disable Optional IEs 1488
N10 Fail Open on Converged Core 1489
Feature Description 1489
Configuration-based Control of Subscription Messages 1490
Feature Description 1490
How it Works 1490
Standards Compliance 1491
Call Flows 1491
OAM Support for the Unsubscribe-To-Notifications Messages 1491
Statistics Support 1492
Configuration-based Control of UDM Registration Messages 1492
Feature Description 1492
How it Works 1493
Configuring Control for UDM Registration Messages 1493

CHAPTER 46 **UP Session Activation and Deactivation Service Request Procedures** 1495
Feature Summary and Revision History 1495
Summary Data 1495
Revision History 1495
Feature Description 1496
UE-initiated Service Request Procedure 1496
Feature Description 1496
How it Works 1497
Deactivation of the User Plane Connection of a PDU Session 1497
Activation of the User Plane Connection of a PDU Session 1498
Network-initiated Service Request Procedure 1500
Feature Description 1500
How it Works 1501
Call Flows 1501
Standards Compliance 1512
Limitations 1512
Configuring N3 Tunnel Profile 1512

Always-On PDU Session Support 1512
Feature Description 1512
How it Works 1512
Call Flows 1512
Configuring Always-On PDU Session Support 1516
Verifying Always-On PDU Session Support 1517
Always-On PDU Session OAM Support 1518
Bulk Statistics Support 1519
DLDR Handling for N3 Connection Reactivation 1519
Feature Description 1519
How it Works 1520
Configuring N3 Connection Reactivation 1520

CHAPTER 47 UPF Path Management and Restoration 1521
Feature Summary and Revision History 1521
Summary Data 1521
Revision History 1521
Feature Description 1522
Standards Compliance 1522
How it Works 1522
Configuration Support for the UPF Path Management and Restoration 1523
Configuring the Heartbeat at the Interface Level 1523
Verifying the Heartbeat Configuration for the SMF 1524
Configuring the Heartbeat at the UPF Group Level 1524
Verifying the Heartbeat Configuration for the UPF Group Level 1525
Associating UPF Group to Individual UPF Network Configuration 1525
Verifying the Association of the UPF Group with the Individual UPF 1526
Configuring the Sx/N4 Path Failure Detection Policy 1526
Verifying the Sx/N4 Path Failure Detection Policy 1527
OAM Support 1527
Bulk Statistics 1527

CHAPTER 48 Virtual Routing and Forwarding 1529
Feature Summary and Revision History 1529

Summary Data 1529
Revision History 1529
Feature Description 1530
How it Works 1530
VRF Creation 1530
VRF Modification 1531
VRF Deletion 1531
Limitations 1531
Configuring Virtual Routing and Forwarding 1532
VRF Configuration 1532
Configuration Example 1532
Endpoint Configuration 1532
Configuration Example 1533
VRF Configuration in RADIUS Profile 1533
VRF Association for BGP Peering 1534
Configuration Example 1535
Configuration Verification 1535
OAM Support 1536
Bulk Statistics Support 1536

CHAPTER 49 **Wireless Priority Services** 1539
Feature Summary and Revision History 1539
Summary Data 1539
Revision History 1540
Feature Description 1540
Use Cases 1541
Multimedia Priority Services 1541
DSCP Marking for N3, S5-U, or S2-B over PFCP 1546
WPS Profile Support 1546
SBI Message Priority Mechanism 1546
How it Works 1548
Standards Compliance 1548
5QI Mapping Support 1549
Feature Description 1549

QCI Modification for Dynamic Rules 1549
Collision Between Original QCI and Remapped QCI 1549
Configuring Wireless Priority Services 1550
Configuring the WPS Profile 1550
Associating WPS Profile under DNN Profile 1551
Configuration Verification 1552
Remapping Nonstandard QCI to Standard QCI 1552
Configuring Message Priority Profiles 1554
Associating Message Priority Profiles 1554
Configuring SMF to Exclude WPS Sessions from Overload Throttling 1557
Configuring Overload Exclusion at an Endpoint Level 1557
WPS OAM Support 1559

CHAPTER 50 **Troubleshooting Information** 1561
Feature Summary and Revision History 1561
Summary Data 1561
Revision History 1561
Description 1563
Using CLI Data 1563
Show and Clear Commands 1563
show Commands 1563
clear Commands 1586
Monitor Subscriber and Monitor Protocol 1590
Feature Description 1590
Configuring the Monitor Subscriber and Monitor Protocol Feature 1590
UPF Monitor Subscriber from SMF 1592
Feature Description 1592
Configuring UPF Monitor Subscriber from SMF 1593
Alerts 1594
Feature Description 1594
How it Works 1594
Configuring Alert Rules 1594
Viewing Alert Logger 1596
Call Flow Procedure Alerts 1597

Interface Specific Alerts 1602
IP Pool 1607
Message Level Alerts 1608
Policy Rule Alerts 1614
SMF Overload/Congestion 1615
SMF Sessions 1616
Metrics 1617
Feature Description 1617
How it Works 1618
Configuring Metrics Collection 1618
Configuration Example 1619
Configuration Verification 1620
Bulk Statistics and Key Performance Indicators 1621
Feature Description 1621
Logs 1621
Feature Description 1621
Download OAM and EDR Monitor Pod Files 1622
How it Works 1622
Configuring the Logs 1623
Enabling or Disabling the Transaction Messages 1623
Configuring the Logging Levels 1625
Configuring Persistent Transaction Logs 1626
Dispatcher 1627
Feature Description 1627
Configuring Dispatcher for S11 Interface 1627
Configuration Example 1628
OAM Support 1628
Metrics 1628

CHAPTER 51 **Sample SMF Configuration** 1631
Sample Configuration 1631

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This preface describes the *5G Session Management Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco Session Management Function (SMF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

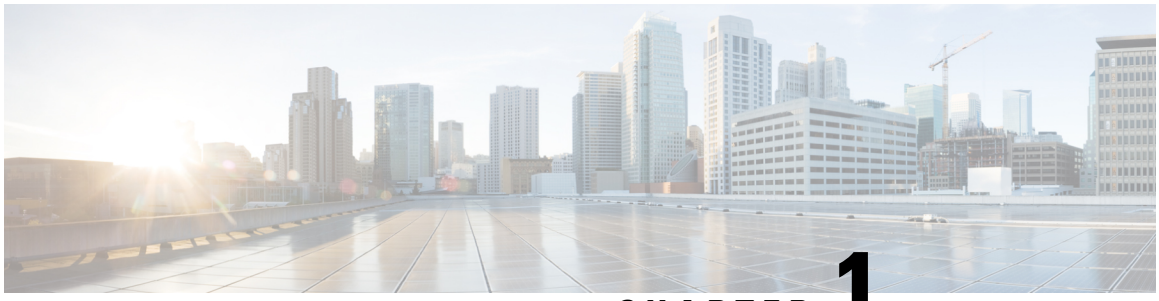
• Conventions Used, on page lix

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**



CHAPTER 1

5G Architecture

- Feature Summary and Revision History, on page 1
- Overview, on page 2
- Subscriber Microservices Infrastructure Architecture, on page 3
- Control Plane Network Function Architecture, on page 5

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	• PCF • SMF • UPF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Overview

The Ultra Cloud Core is Cisco's solution supporting 3GPP's standards for 5G new radio (NR) standalone (SA) mode. These standards define various network functions (NFs) based on the separation of control plane (CP) and user plane (UP) (for example CUPS) functionality for increased network performance and capabilities.

Control Plane Network Functions

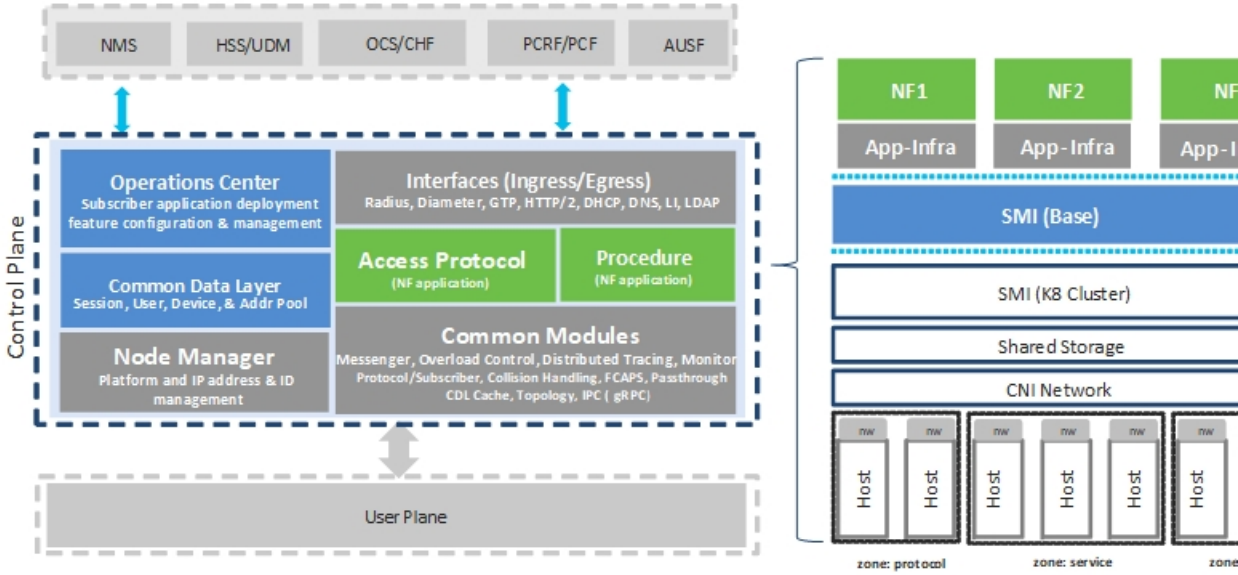
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture that is designed around the following tenants:

- Cloud-scale—Fully virtualized for simplicity, speed, and flexibility.
- Automation and orchestration—Optimized operations, service creation, and infrastructure.
- Security—Multiple layers of security across the deployment stack from the infrastructure through the NF applications.
- API exposure—Open and extensive for greater visibility, control, and service enablement.
- Access agnostic—Support for heterogeneous network types (for example 5G, 4G, 3G, Wi-Fi, and so on).

These control plane NFs are each designed as containerized applications (for example microservices) for deployment through the Subscriber Microservices Infrastructure (SMI).

The SMI defines the common application layers for functional aspects of the NF such as life-cycle management (LCM), operations and management (OAM), and packaging.

Figure 1: Ultra Cloud Core CP Architectural Components



User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function (UPF). Unlike the CP-related NFs, the 5G UPF leverages the same Vector Packet Processing (VPP) technology currently in use by the user plane component within Cisco 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultrafast packet forwarding.
- Extensive integrated IP Services such as Subscriber Firewall, Tethering, Deep-Packet Inspection (DPI), Internet Content Adaption Protocol (ICAP), Application Detection and Control (ADC), and header enrichment (HE).
- Integrated third-party applications for traffic and TCP optimization.

Subscriber Microservices Infrastructure Architecture

The Ultra Cloud Core (UCC) Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life-cycle operations for microservices-based applications.

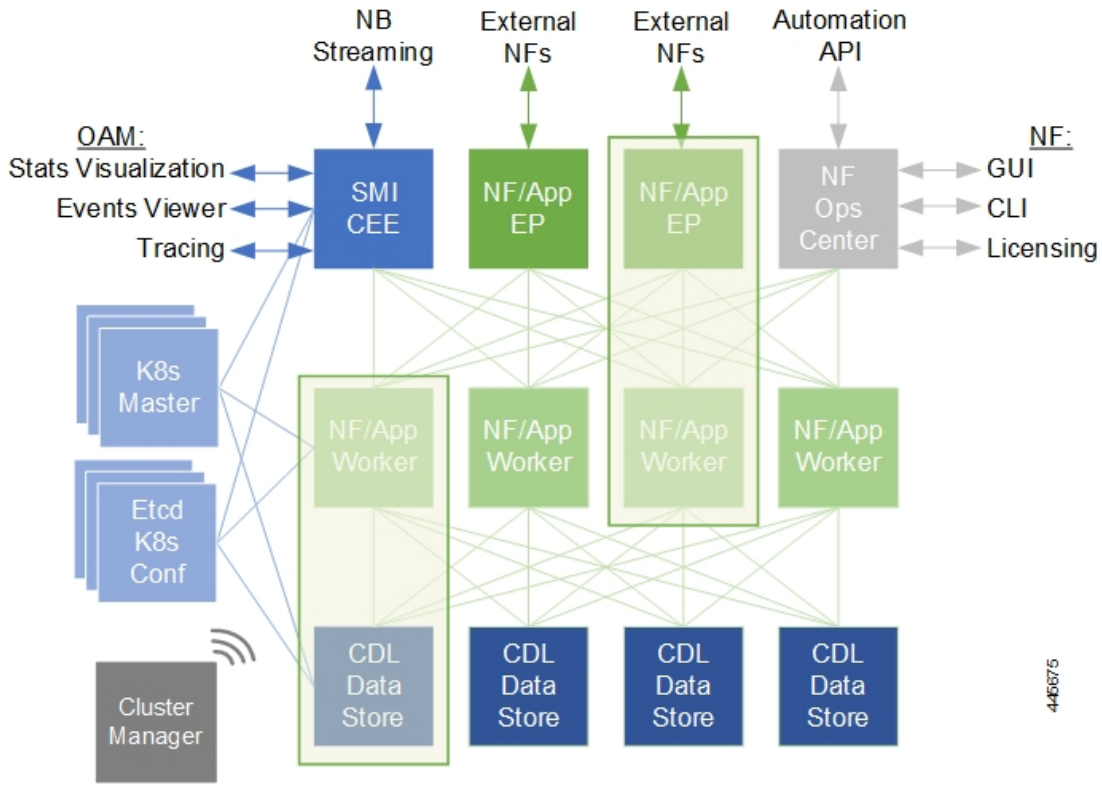
The SMI stack consists of the following:

- SMI Cluster Manager—Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.

- Kubernetes Management—Includes the K8s primary and etcd functions, which provide LCM for the NF applications that are deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE)—Provides common utilities and OAM functionalities for Cisco Cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Also, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL)—Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers high availability in local or geo-redundant deployments.
- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, extra security, and the ability to deploy new code and new configurations in low risk manner.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- NF or Application Worker Nodes—The containers that comprise an NF application pod.
- NF or Application Endpoints (EPs)—The NFs or applications and their interfaces to other entities on the network
- Application Programming Interfaces (APIs)—Provides various APIs for deployment, configuration, and management automation.

The following figure depicts how these components interconnect to comprise a microservice-based NF or application.

Figure 2: SMI Components



For more information on SMI components, see Ultra Cloud Core Subscriber Microservices Infrastructure and the related-documentation at *Deployment Guide* > *Overview* chapter.

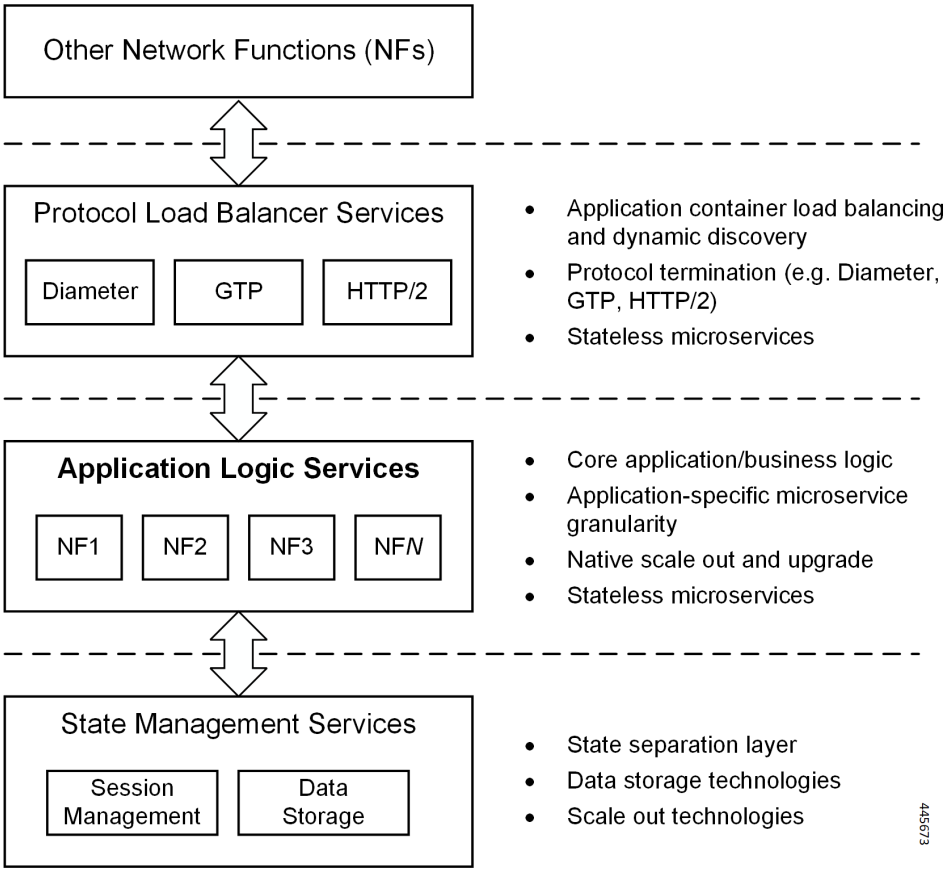
Control Plane Network Function Architecture

Control plane (CP) NFs are designed around a three-tiered architecture that take advantage of the stateful or stateless capabilities that are afforded within cloud native environments.

The architectural tiers are as follows:

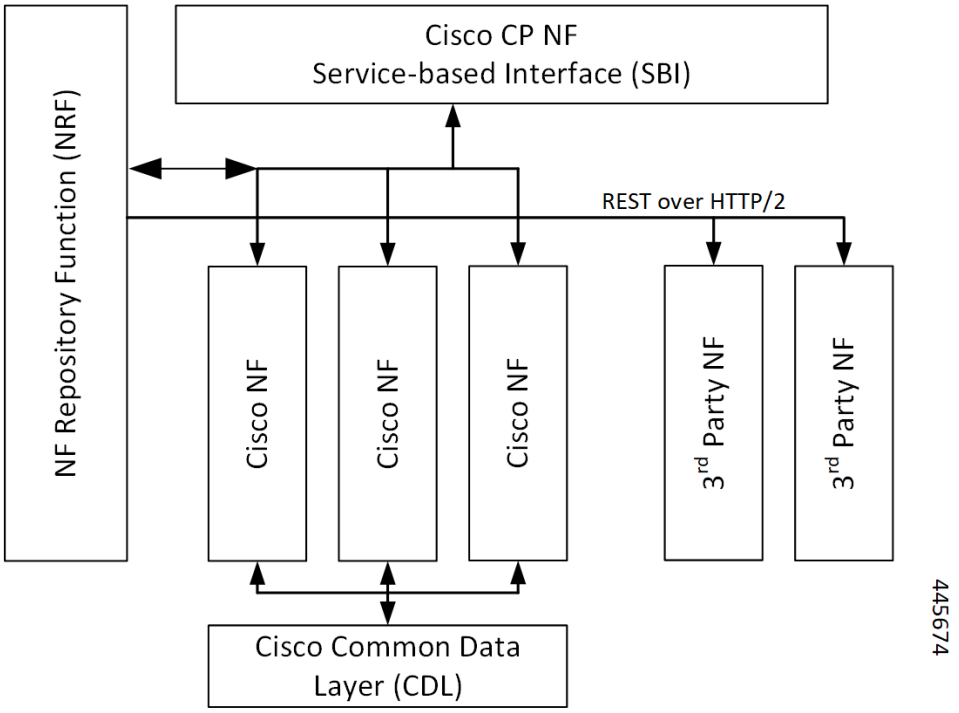
- Protocol Load Balancer Services—These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and termination. These include traditional 3GPP protocols and new protocols that are introduced with 5G.
- Applications Services—Responsible for implementing the core application or business logic, these are the stateless services that render the actual application based on the received information. This layer may contain varying degrees of microservice granularity. Application services are stateless.
- State management services—Enable stateless application services by providing a common data layer (CDL) to store or cache state information (for example session and subscriber data). This layer supports various data storage technologies from in-memory caches to full-fledge databases.

Figure 3: Control Plan Network Function Tiered Architecture

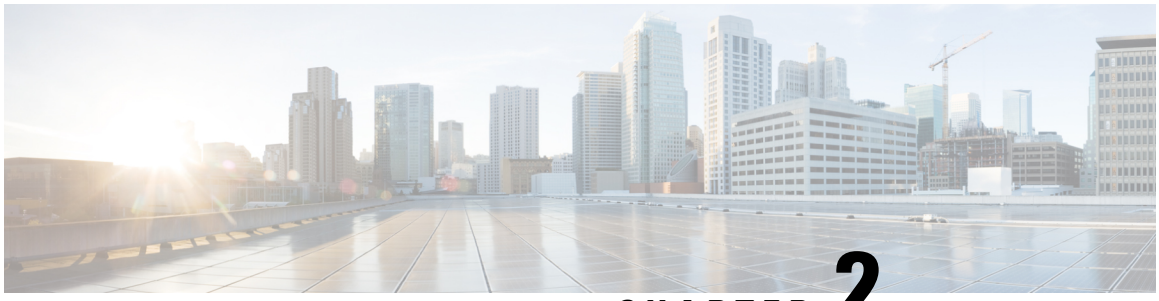


The three-tiered architecture on which Cisco CP NFs are designed fully support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



For more information on the Cisco network functions, see their corresponding network function documentation.



CHAPTER 2

5G SMF Overview

- Feature Summary and Revision History, on page 9
- Product Description, on page 10
- Converged Core Overview, on page 11
- Use Cases and Features, on page 13
- Deployment Architecture and Interfaces, on page 21
- Life Cycle of Data Packet, on page 24
- Session Affinity, on page 30
- License Information, on page 31
- Standards Compliance, on page 31

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 4: Revision History

Revision Details	Release
The converged core support for combined SMF + cnSGWc is added in this release.	2021.01.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Product Description

The Cisco Session Management Function (SMF) is one of the Control Plane Network Functions (NF) of the 5G core network (5GC). The SMF is responsible for the session management with the supported individual functions on a per-session basis.

A single instance of SMF can support some or all the functionality of the SMF. As specified in *3GPP TS 23.501*, the SMF supports the following functionality:

- Handles session management. For example, session establishment, modification and release, including the tunnel between the User Plane Function (UPF) and the access network (AN).
- Handles user element (UE) IP address allocation and management, which includes an optional authorization.
- Performs Dynamic Host Configuration Protocol for IPv4 (DHCPv4) and DHCPv6 functions, both as server and client.
- Performs Address Resolution Protocol (ARP) proxying and IPv6 Neighbor Solicitation Proxying functionality for the Ethernet PDUs. The SMF responds to the ARP and the IPv6 Neighbor Solicitation Request by providing the MAC address. This address corresponds to the IP address that exists in the request.
- Selects and controls the UPF for the Ethernet PDU sessions. The UP function includes controlling the UPF to proxy ARP or IPv6 Neighbor Discovery, and forwarding all ARP or IPv6 Neighbor Solicitation traffic to the SMF.
- Configures Traffic Steering at the UPF to route traffic to the corresponding Data Network (DN).
- Terminates interfaces toward the Policy Control Function (PCF).
- Handles the Lawful Intercept (LI) for Session Manager (SM) events and interface to the LI system.
- Controls and synchronizes the charging data collection at the UPF.
- Terminates the SM parts of Non-Access-Stratum (NAS) messages.
- Routes packets and ensures the delivery of information through the Downlink Data Notification (DDN).
- Initiates the AN-specific SM information that is sent through the Access and Mobility Management Function (AMF) to AN over the N2 interface.
- Determines the session and service continuity (SSC) mode of a session.
- Provides the following roaming functionality:
  - Manages the local enforcement to apply Quality of Service (QoS) SLAs (VPLMN).
  - Collects charging data and supports the charging interfaces.
  - Supports communication with the external DN. The communication is for the transport of signaling for the PDU session authorization or authentication by an external DN.

The SMF also provides support for an enterprise mobile virtual network operator (MVNO) model, which enables a mobile network operator (MNO) to perform secondary authentication for the leased MVNO subscribers. Additionally, the SMF supports other MVNO features, but is not limited to, RADIUS Client, vDNN, and so on.

Converged Core Overview

The converged core solution provides an advanced, cloud-native, converged control plane with the capability to support 4G and 5G devices, and use cases.

Important This release supports only the cloud-native integrated S-GW and SMF instance with S5C and cnSGW-C functionalities.

The converged core solution removes the operational complexity by providing a unified core network to handle all types of subscribers and use cases.

The operator has the following benefits:

- Improves the overall network efficiency by reducing signaling between cnSGW-C and SMF while handling a 4G subscriber or handoff from 5G to 4G coverage area.
- Reduces latency introduced due to the extra hop SGW-U for a subscriber in 4G coverage area, by collapsing the data path in the Converged UPF, thus improving the overall user experience.
- Provides ability to use a unified subscriber policy and billing infrastructure using SBA interfaces for 4G and 5G devices.

The solution supports the following converged control plane and user plane functions:

- Converged Control Plane Functions
  - Integrates S-GW and SMF network functions as a single deployment, under a single Kubernetes namespace, to support 4G and 5G devices from E-UTRAN/NR (converged core gateway)
  - Supports logical network functions (data)
- Converged User Plane Functions
  - Integrates UPF and SGW-U functionalities as a single network function
  - Provides simultaneous support for N4 and Sxa interfaces
  - Terminates multiple control planes in a single deployment

Interservice Pod Communication

Feature Description

When the cnSGW service and SMF service selected for a subscriber are on the same cluster and same rack, the messages exchanged between the two services flow through the gtpc-ep pod.

If a collocated session is identified and **enable-gtpc-bypass** CLI command is configured under GTP endpoint, then the SMF and cnSGW-C directly communicate with each other without exchanging the messages through the gtpc-ep pod. This approach reduces the latency and the processing load on the gtpc-ep. For details on the command, see the Feature Configuration, on page 13 section.

The SMF service directly communicates with cnSGW service for processing the following requests:

- Create Bearer Request
- Update Bearer Request (UBR) (expect Modify Bearer Command (MBC) triggered UBR)
- Delete Bearer Request (DBR) (expect Delete Bearer Command (DBC) triggered DBR)

The cnSGW service directly communicates with SMF service for processing the following requests:

- Create Session Request
- Modify Bearer Request
- Delete Session Request

If the subscriber session is not collocated, the inbound and outbound messages from SMF or cnSGW-C continue to be exchanged through the gtpc-ep pod.

For this feature support on cnSGW, see the *UCC 5G cnSGWc Configuration and Administration Guide*.

How it Works

This section describes how this feature works.

Perform the following steps to implement this feature.

1. Identify the deployment type of SMF and cnSGW-C.

   To identify the deployment type, the SMF or cnSGW-C compares the target GTPC peer IP address of the message with the locally configured IP address of S5e or S5 interface for the concerned GR instance. The SMF or cnSGW-C marks the subscriber session as collocated service based on the comparison result.

2. Identify the target service pod

   SMF uses session affinity in cnSGW namespace based on TEID, which is derived from Common ID to appropriately route the message towards cnSGW service pod instance.

3. Route the messages to the appropriate peers based on the identified deployment type and target service pod.

   Interservice pod communication uses the existing framework along with protocol buffer to carry the signaling message content.

   The interservice communication between SMF and cnSGW-C happens with the following exceptions:

   - GTPC messages cannot be captured using the packet sniffer tool and **monitor subscriber** command.
   - Path management is not performed for collocated GTPC peers.
   - GTPC message level metrics (at GTPC endpoint) will not be pegged for interservice GTPC messages as GTPC endpoint is bypassed for such messages.
   - Existing interservice metrics will be pegged for interservice messages.

- UBR and DBR initiated on Command Messages follow the existing message flow path. That is, the SMF sends the command messages to cnSGW service through gtpc-ep pod.

Feature Configuration

To enable GTPC bypass between cnSGW and SMF service, use the following sample configuration:

```
config
  instance instance-id gr_instance_id
    endpoint gtp
      enable-gtpc-bypass { false | true }
      end
```

NOTES:

- **endpoint gtp**: Enter the GTP endpoint configuration.
- **enable-gtpc-bypass { false | true }**: Specify the option to enable or disable the GTPC bypass between cnSGW and SMF service.

  When set to true, the GTPC bypass is enabled between SMF and cnSGW. That is, SMF and cnSGW directly communicate without involving the gtpc-ep pod. By default, it is false.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics is updated to support this feature.

- smf_service_stats: This statistics includes gtpc_bypass label to track the GTPC bypass messages.

For more information on bulk statistics support, see the *UCC 5G SMF Metrics Reference*.

Use Cases and Features

This section describes the use cases that SMF supports.

Base SMF Configuration

The SMF base configuration provides a detailed view of the configurations that are required for making the SMF operational. This includes setting up the infrastructure to deploy the SMF, deploying the SMF through SMI, and configuring the Ops Center for exploiting the SMF capabilities over time.

For more information on SMI, see the *Ultra Cloud Core SMI Cluster Deployer Operations Guide*.

The following feature is related to this use case:

- Deploying and Configuring SMF through Ops Center, on page 33

4G Session Support

For UEs, the SMF supports both 5G and 4G NAS to connect to both 4G and 5G core networks. The SMF includes the EPS interworking support and acts as a PGW-C+SMF. The interfaces, such as the Gx, Gy, or Gz, which are used for a 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the Npcf and Nchf.

The SMF supports interworking with EPS by using the N26 interface (which is an inter-CN interface between the MME and the 5GS AMF) to enable interworking between the Evolved Packet Core (EPC) and the NG core networks. Support of the N26 interface in the network is optional for interworking. The N26 interface supports a subset of the functionalities over S10 interface to enable interworking. The UE uses the EPC NAS or 5GC NAS procedures that are based on the core network. The SMF supports QoS flow failures for access and mobility procedures.

The following features are related to this use case:

- 4G to 5G Data Session Handover, on page 432
- EPS Interworking, on page 165
- Flow Failure Handling for Access and Mobility Procedures, on page 399
- SMF Capabilities to Support 4G and 5G Devices, on page 1383
- Session Timers, on page 1367

5G Session Support

The Session and Service Continuity (SSC) support in 5G system architecture addresses the continuous requirements of different applications and services for a User Equipment (UE). The 5G system supports the SSC modes such that the network maintains the connectivity service to the UE. The SMF manages the UE IP address and ID allocation for establishing sessions. The SMF also maintains session connectivity on interfaces, such as N40, N4, N7, and N10, to facilitate charging.

The SMF uses the Xn interface to handover a UE from a source NG-RAN to the target NG-RAN when the AMF is unchanged, and without relocating the UPF. The SMF includes the N3 tunnel profile configuration to enable the notifications on the Control Plane (CP) and enable buffering on the UPF. The SMF supports activation and deactivation of the User Plane (UP) connection of a PDU session. The SMF also includes the DNS proxy feature to configure proxy servers for resolving the host names and their IP addresses.

The following features are related to this use case:

- Inter gNodeB Handover, on page 457
- IP Pool Allocation per DNN, on page 849
- UP Session Activation and Deactivation Service Request Procedures, on page 1495
- Session and Service Continuity Mode, on page 1363
- Static IP Support, on page 759
- TAI Selection from AMF, on page 1477

Access and Mobility Support

The SMF supports the access and mobility through session management procedures for PDU session establishment, modification, and release. The SMF supports N2-based handovers for intra-SMF or inter-AMF when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases. With the multi-DNN support, SMF has multiple PDN connections for providing various services including Internet and Voice over New Radio (VoNR) services. The SMF supports network-initiated messages when a UE is either in the CM-Idle state or in the CM-Connected state.

Access and mobility support includes the intra-5G handover use case, which has the following handover support:

- Xn Handover
- Intra-AMF N2 Handover
- Inter-AMF N2 Handover

The following features are related to this use case:

- 5GSM Cause Code Handling, on page 652
- AN-initiated Session Modification and Release, on page 67
- CHF and PCF Integration for Access and Mobility Procedures, on page 447
- Inter gNodeB Handover, on page 457
- MTU Support in PCO, on page 827
- DNN Support, on page 831
- Network-initiated Session Modification Procedures, on page 865
- Policy and User Plane Management, on page 989
- UDM Integration, on page 1485
- Voice over New Radio, on page 521

Charging Integration

The SMF supports converged charging and uses the Nchf or N40 interface to generate charging events. The SMF supports offline failover for charging when a charging (CHF) server fails. Based on the charging data information that SMF receives, it provides reporting level support for online and offline charging.

The following feature is related to this use case:

- Subscriber Charging, on page 1427

Cloud Native Infrastructure

The SMF services includes the configuration to process PDU Session Management API calls. The IP Address Management (IPAM) technique is integrated with the SMF in the Application Services layer for tracking and managing the IP address space of a network. The SMF uses the Operations Center interface, which is a system-level infrastructure, to initiate the deployment of micro-services, to push application specific

configuration to one or more micro-services, and to run application-specific commands to invoke APIs in application-specific pods.

The following feature is related to this use case:

- Overload Management, on page 921

Converged Core Network

The SMF supports standalone deployment or an integrated deployment with cnSGWc for serving 4G and 5G subscribers. Converged Control Plane function comprises a combination of 4G and 5G control plane instances, that is, SMF and cnSGWc.

With converged core deployment, for the same PDN session, the S-GW and SMF select the same UPF instance so that the data path is optimized. The converged core architecture reduces the operational cost and the complexity of maintaining multiple different networks, leverages new interfaces and business avenues.

The converged core deployment involves changing some basic configurations of SMF, pod layout, and optimizing performance with call processing.

The following features are related to this use case:

- Alerts, on page 1594
- Content Filtering and X-Header Enrichment, on page 83
- Deploying and Configuring SMF through Ops Center, on page 33
- Dynamic Routing by Using BGP, on page 139
- EPS Interworking, on page 165
  - GTP Path Failure Handling, Restoration, and Recovery, on page 267
  - Support for UE Initial Attach , on page 172
- Monitor Subscriber and Monitor Protocol, on page 1590
- Pods and Services Reference, on page 973
- Policy and User Plane Management, on page 989
  - Support for UPF Node Reports and Proprietary Session Reports, on page 1084
  - Static PCC Rules Support, on page 1041
- Metrics, on page 1617
- UPF Path Management and Restoration, on page 1521
- Wireless Priority Services, on page 1539

IMS Support

The IP Multimedia Subsystem (IMS) connects to the LTE network and 5G core (through UPF node) for delivering voice services such as Voice over LTE (VoLTE) and Voice over New Radio (VoNR).

The following features are related to this use case:

- Voice Over LTE Support, on page 502
- Voice over New Radio, on page 521
- NPLI Support for VoLTE and VoNR, on page 513

IPAM Support

IP Address Management (IPAM) is a technique for tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. The IPAM provides all the functionalities necessary for working with the cloud-native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the Session Management Function (SMF), Policy Control Function (PCF), and so on.

The following feature is related to this use case:

- IP Address Management, on page 737

Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept and control data messages of targeted mobile users. The SMF that handles the Control Plane actions for the PDU sessions includes an IRI-POI that has the LI capability to generate the related xIRI.

For more details, contact your Cisco account representative.

MVNO Support

The SMF provides support for an enterprise MVNO model. A mobile network operator can perform secondary authentication for the leased MVNO subscribers and also support any additional features related to the AAA server. The SMF uses the RADIUS protocol for such secondary authentication purposes.

The following features are related to this use case:

- DNN Support
  - DNN Case Insensitive Support
- Policy and User Plane Management
  - Increase Max Groups Per Bandwidth Policy
- RADIUS Authentication and Accounting
  - Handling RADIUS Disconnect and CoA Requests
  - RADIUS Access Management
  - RADIUS Accounting
  - RADIUS PAP/CHAP/MSCHAP Support

- RADIUS NAS-IP Support

NF Management

Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters.

The following features are related to this use case:

- NF Discovery and Management, on page 877
- Failure Handling Support, on page 355

OAM Support

This use case covers all the Operation, Administration, and Maintenance (OAM) functions of the SMF.

The following features are related to this use case:

- Alerts, on page 1594
- Bulk Statistics and Key Performance Indicators , on page 1621
- Deploying and Configuring SMF through Ops Center, on page 33
- Logs, on page 1621
- Metrics, on page 1617
- Monitor Subscriber and Monitor Protocol, on page 1590
- Pods and Services Reference, on page 973
- Smart Licensing, on page 39
- SMF Rolling Software Update, on page 55

Policy Integration

The SMF communicates with the Unified Data Management (UDM) and Policy Control Function (PCF) to perform the following:

- Procure the subscribed and authorized QoS parameters for the Guaranteed Bit Rate (GBR) and non-GBR flows
- Pass the relevant information to the UE (NAS), gNB (NGAP), and UPF (PFCP)

This ensures that all nodes on the network provide the desired QoS to the PDU session.

The SMF uses the service-based N7 interface with the PCF to retrieve the session management policy information corresponding to the PDU session of the UE. The SMF selects the PCF during the PDU Session Establishment procedure. It also acts as a consumer of the PCF-provided session management policy service.

The following features are related to this use case:

- DSCP Marking, on page 131
- Policy and User Plane Management, on page 989
- Wireless Priority Services, on page 1539

RADIUS Support

In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI) during authentication and the key agreement between the UE and the network. In addition, the serving network can perform a secondary authentication for data networks outside the mobile operator domain.

The following feature is related to this use case:

- RADIUS Authentication and Accounting, on page 1109

Redundancy Support

The SMF deployment in K8 cluster plays a vital role to support High Availability (HA) and Geographic Redundancy (GR). The redundancy support ensures stateful session continuity among the clusters during the rack or cluster failures.

The SMF achieves HA through redundant set-up of each cluster component such that any single point of failure is avoided.

The GR provides rack-level redundancy to replicate data between two separate K8 clusters across racks so that, on rack or cluster failure, traffic can switch to a remote rack to process the traffic. Rack or cluster failure can be due to power failure, multi-compute failures, network failure, multi-pod failure, BFD link failure, and so on.

The following features are related to this use case:

- High Availability Support, on page 1191
- Inter-Rack Redundancy Support, on page 1198
- Mesh Connectivity to All UPFs, on page 825

Roaming Support

Mobile network operators make roaming partnerships to provide services to the subscribers seamlessly in geographies beyond their network reach. PLMNs define the operator network boundaries. HPLMN is the Subscriber’s home network and VPLMN is the visited network from where the service is rendered.

The following features are related to this use case:

- Roaming Support, on page 1281
- Multiple PLMN Support, on page 855

SMF Inline Services

The SMF uses the Inline Services feature such as the Enhanced Charging Service (ECS) that enables operators to reduce billing-related costs and gives the ability to offer tiered, detailed, and itemized billing to their subscribers. Using shallow and deep packet inspection (DPI), the ECS [also known as Active Charging Service (ACS)] allows operators to charge subscribers based on the actual usage, number of bytes, premium services, location, and so on. The ECS also generates charging records for postpaid and prepaid billing systems.

The following features are related to this use case:

- Content Filtering and X-Header Enrichment, on page 83
- Event Detail Records, on page 287
- Policy and User Plane Management, on page 989

SMF Specification Compliance

The SMF supports different 3GPP specification versions for the SMF interfaces. It processes the messages from the interfaces as per the compliance profile configured for the corresponding services.

The following feature is related to this use case:

- Interfaces Support, on page 545

Subscription Management

The SMF handles the user subscription management over the N10 interface.

The following feature is related to this use case:

- UDM Integration, on page 1485

UPF Integration

The SMF uses the available StarOS-based UPF node to meet the non-standard requirements on the UPF node to interwork with this UPF. To comply with the IPv6 Stateless Auto-configuration, the SMF supports ICMPv6 Router Solicit and Advertisement.

The following features are related to this use case:

- Policy and User Plane Management, on page 989
- IPv6 PDU Sessions, on page 815
- UPF Path Management and Restoration, on page 1521

Wi-Fi Support

The SMF supports Voice over Wi-Fi (VoWiFi). The VoWiFi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

The following features are related to this use case:

- VoWi-Fi Support, on page 515
- Wi-Fi Handover, on page 470

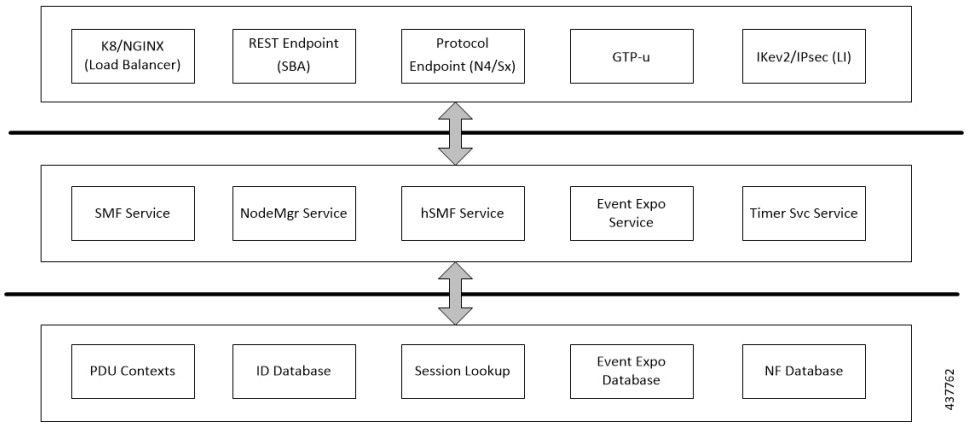
Deployment Architecture and Interfaces

The Cisco SMF is a part of the 5G core network functions portfolio with a common mobile core platform architecture. The core network functions include Access and Mobility Management Function (AMF), Network Repository Function (NRF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), and User Plane Function (UPF).

SMF Architecture

The SMF network function consists of loosely coupled microservices together. The microservice decomposition is based on a three-layered architecture as illustrated in the following figure.

Figure 5: SMF 3-Layered Micro Services Architecture



Following are the three layers of the SMF architecture:

- Layer 1—Protocol and Load Balancer services (Stateless)
- Layer 2—Application services (Stateless)
- Layer 3—Database services (Stateful)

SMF Deployment

The 5G Mobility NFs deployment supports the following modes:

- Standalone mode: In this mode, each NF together with the required microservices is deployed in a separate name space in Kubernetes.
- Converged mode: In this mode, several NFs are deployed together in a single name space and micro-service common to NFs render the service to all the deployed NFs.

Converged Core Architecture

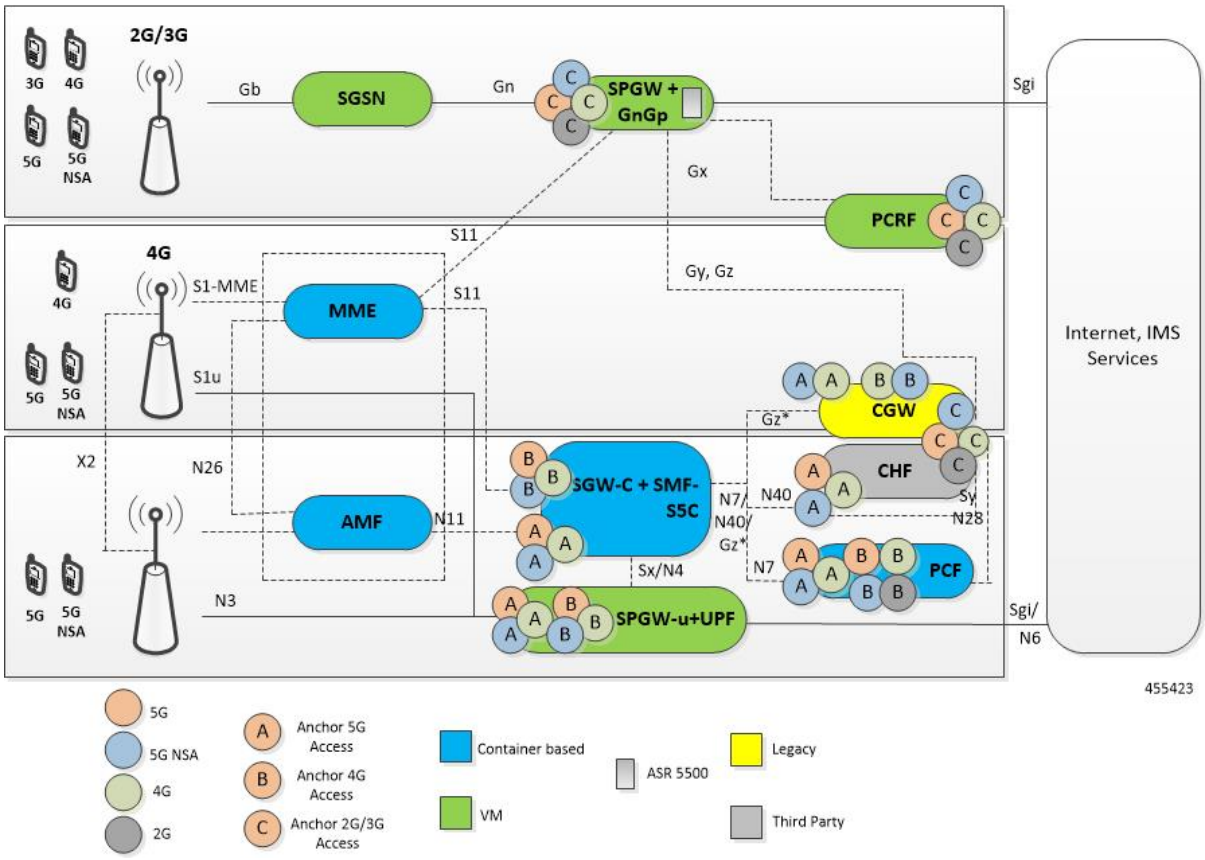
The converged core solution provides a single unified platform which is based on SMI architecture. The supporting architecture integrates the cloud-native S-GW and SMF deployment with 5GC and cnSGW-C functionalities. The solution uses 3GPP-defined SBA interfaces for policy and charging functions.

In the converged core architecture, the 4G and 5G capable UEs are anchored on the same control plane instance. The control plane instance provides the SMF, 5GC, and cnSGW-C functionalities.

The handoffs between 4G and 5G access types are seamless for 5G capable devices. The handoffs from LTE to UTRAN (bi-directional communication between 4G/5G and 3G/2G) are not seamless for 4G capable devices.

The following figure illustrates the supported network architecture.

Figure 6: Converged Core Architecture



The UPF deployed as a part of this solution is a VPC-SI VM. The UPF deployment is VM-based, and supports:

- SGW-U, PGW-U, and UPF functionalities in the same instance, and exposes the Sxa, Sxb, Sxab, or N4 interface towards the control plane.
- Multiple CP instances (up to 4) simultaneously.

Converged Core Deployment

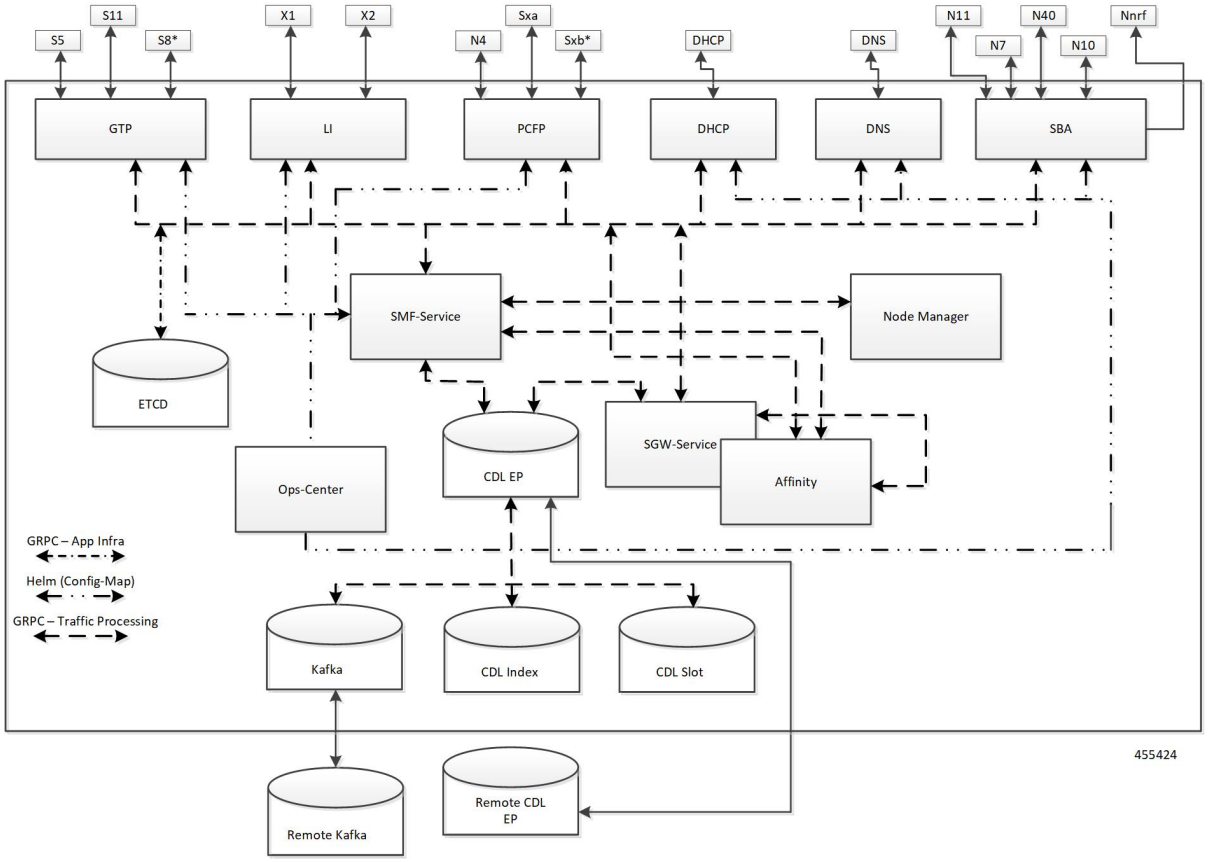
The converged core deployment is based on the converged control plane and unified user plane infrastructure for all use cases.

In the converged core deployment, all 4G and 5G-capable UEs are anchored on the 5G core (SMF) with SBA interfaces towards PCF.

The converged core deployment has a converged Ops Center that allows the configuration of cnSGW-C and SMF services along with other microservices. A single product helm chart is used to install components.

The following figure illustrates the Kubernetes deployment for the converged S-GW and SMF network function.

Figure 7: Kubernetes Deployment



The protocol layer services are shared across SMF and S-GW. The GTP endpoint terminates the S11 interface and S5/S8 interface. Similarly, the PFCP (protocol) endpoint terminates the N4 and Sxa interfaces.

The SMF and S-GW services are deployed as distinct pods and the session processing is segregated. Both the service pods use CDL for storing subscriber sessions.

Supported Interfaces

This section describes the interfaces supported between the SMF and other network functions in the 5GC.

- Diameter—Interface that provides framework for services that require Access, Authorization, and Accounting (AAA) or Policy support across IP-based networks.
- GTP—Uses the N9 interface as the reference point between two core UPFs.
- Gx—Interface between SMF and PCRF.
- Gy—Interface between SMF CTF and OCS Charging Data Function (CDF).
- N1/NAS—Reference point between the UE and AMF.
- N2/NGAP—Reference point between the RAN and AMF.
- N4—Reference point between the SMF and UPF.
- N7—Reference point between the SMF and PCF.
- N10—Reference point between the UDM and SMF.
- N11—Reference point between the AMF and SMF.
- N40—Reference point between the SMF and CHF.
- Nnrf—Interface displayed by NRF on 3GPP 5G system architecture.
- RADIUS—Interface that manages network access.
- S2b—Interface between the PGW-C and ePDG.
- S5—Interface between the PGW-C and S-GW.
- SBA—Interface for NFs to communicate with each other.

For details on the supported interfaces, see the Interfaces Support, on page 545 chapter.

Life Cycle of Data Packet

The following call flow depicts the life cycle of a data packet traversing through various pods of the SMF for a successful PDU session establishment.

The SMF application includes the following pods:

- REST-EP
- Cache
- Service
- Nodemgr
- Protocol
- UDP-Proxy
- CDL

Figure 8: 4G Session Procedure - Complete ByPass(PFCP and GTP)

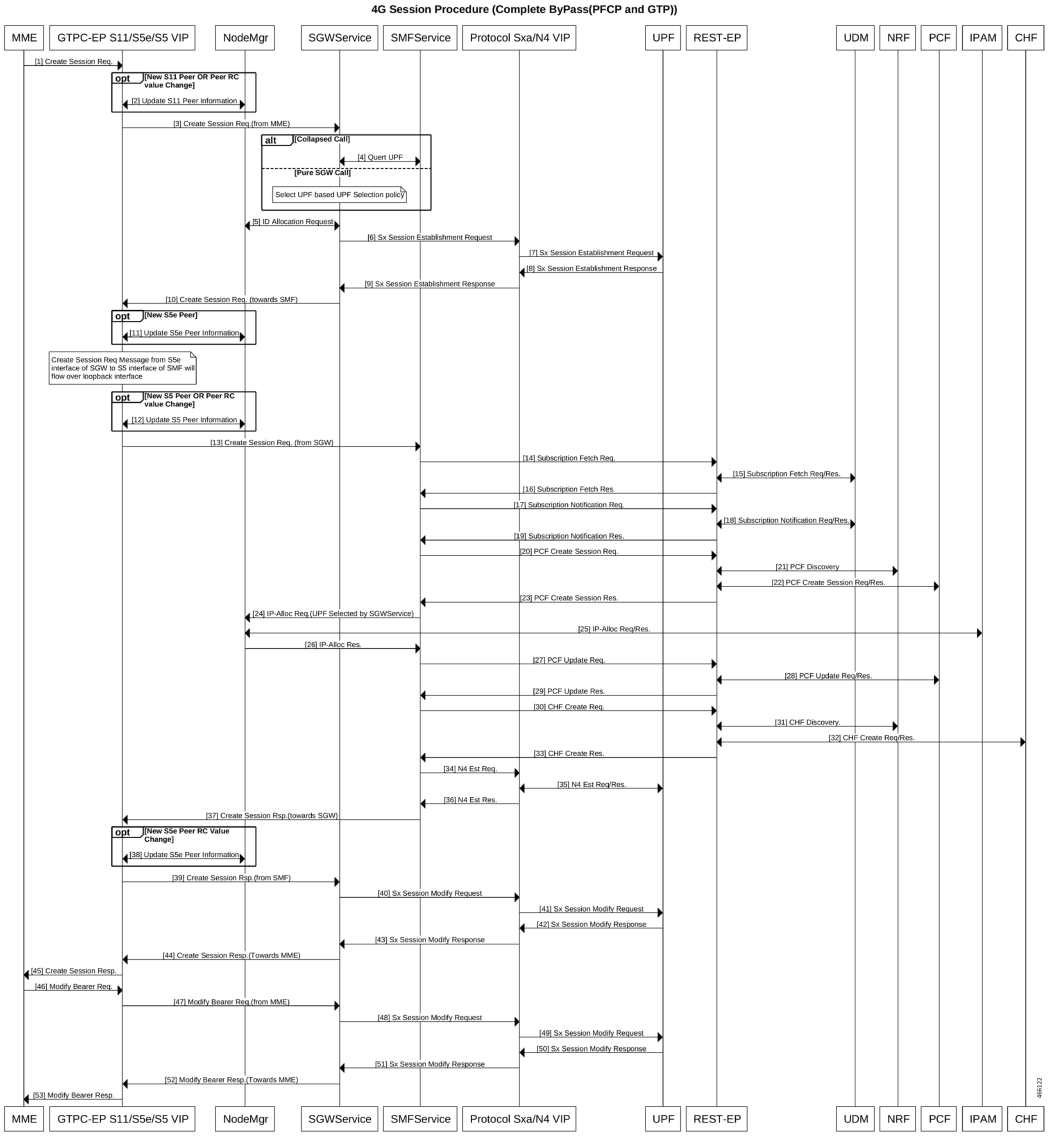


Figure 9: 4G Session Procedure with UDP Proxy for PFCP and GTP

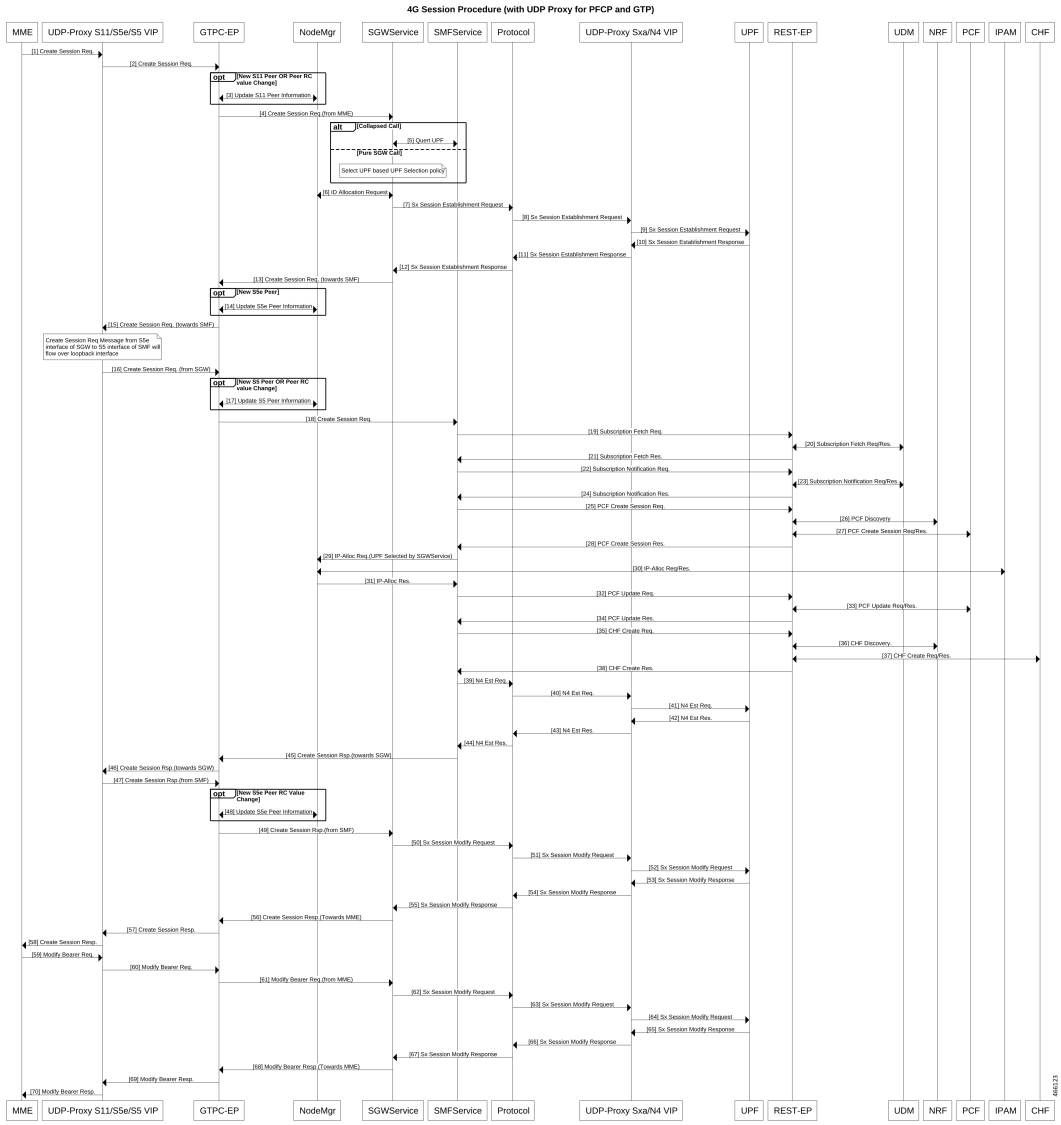


Figure 10: End-to-End PDU Session Establishment Call Flow for Data Packets

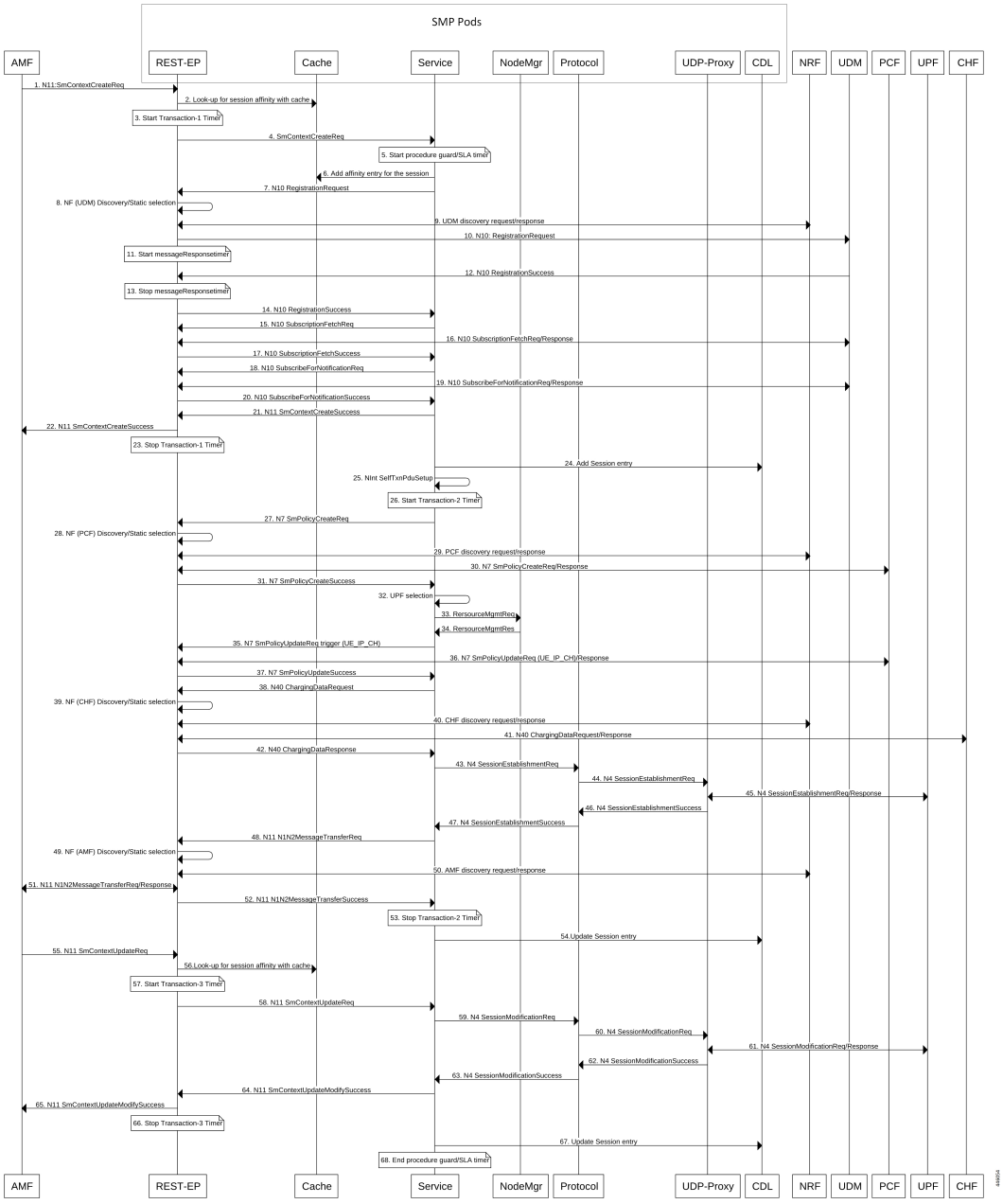


Table 5: End-to-End PDU Session Establishment Call Flow Description

Step	Description
1	The AMF sends N11:SMContextCreateRequest to the SMF, which terminates on the VIP-IP/external IP of REST-EP pod.

Step	Description
2	The REST-EP pod performs look-up for session affinity with cache pod. The SMF does not have the entry for the user session. The cache output does not result in any SMF-service affinity for the user session. Kubernetes service/ISTIO load balancer selects one SMF-service pod from multiple SMF-service pods that are configured.
3	The REST-EP starts the timer associated with transaction-1. The PDU session establishment procedure involves using three transactions which are started at different stages of the call flow. The default transaction timer on SMF is 10 seconds. The transaction timers are configurable through Service Level Agreement (SLA) feature.
4	The REST-EP forwards the N11:SMContextCreateRequest to the selected SMF-service.
5	The SMF-service starts procedure timer (guard timer/SLA timer). The SLA timers are configurable.
6	The SMF-service adds affinity entry with cache pod for the session. The SMF continues to use the same selected SMF-service in the subsequent stages of the call flow until the cache is expired.
7	The SMF-service instructs the REST-EP pod to trigger N10: Registration Request.
8	The REST-EP decides whether to perform NF discovery or static NF selection of UDM based on the configuration.
9	The REST-EP encodes and sends UDM discovery request to the NRF and receives a successful response with the list of UDMs.
10	The REST-EP encodes and sends N10:RegistrationRequest to the selected UDM.
11	The REST-EP starts messageResponseTimer. The default value of the configurable messageResponseTimeout is 2 seconds. The messageResponseTimer is applicable for all outbound HTTP2 messages initiated by SMF. They are not explicitly called out in the subsequent stages of the call flow.
12	The REST-EP receives successful N10:RegistrationResponse from the UDM.
13	The REST-EP stops messageResponseTimer.
14	The REST-EP forwards the N10:RegistrationResponse to the SMF-service.
15	The SMF-service instructs the REST-EP pod to trigger N10:SubscriptionFetchRequest.
16	The REST-EP encodes and sends N10: SubscriptionFetchRequest to the UDM. The REST-EP receives a response from the UDM.
17	The REST-EP forwards the N10:SubscriptionFetchResponse to the SMF-service.
18	The SMF-service instructs the REST-EP pod to trigger N10:SubscribeNotificationRequest.
19	The REST-EP encodes and sends N10:SubscribeNotificationRequest to UDM. The REST-EP receives a response from the UDM.
20	The REST-EP forwards the N10:SubscribeNotificationRequest to the SMF-service.
21	The SMF-service sends N11:SMContextCreateResponse to the REST-EP.
22	The REST-EP forwards the N11:SMContextCreateResponse to the AMF.

Step	Description
23	The REST-EP stops the transaction-1 timer started in step 3.
24	The SMF-service adds the session entry information in the CDL.
25	The SMF-service starts an internal transaction by sending NIntSelfTxnPduSetup message.
26	The SMF-service starts the timer associated with transaction-2.
27	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyCreateReq.
28	The REST-EP decides whether to perform NF discovery or static NF selection of PCF based on the configuration.
29	The REST-EP encodes and sends the PCF discovery request to the NRF and receives a successful response with the list of PCFs.
30	The REST-EP encodes and sends N7:SMPolicyCreateReq to the selected PCF. The REST-EP receives a response from the PCF.
31	The REST-EP forwards N7:SmPolicyCreateSuccess to the SMF-service.
32	The SMF-service performs the UPF selection.
33	The SMF-service sends ResourceMgmtReq to IPAM module of Nodemgr to request the IP address for the UE.
34	The SMF-service receives ResourceMgmtResp from the IPAM module of the Nodemgr with the IP address to the UE.
35	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyUpdateReq with trigger "UE_IP_CH".
36	The REST-EP encodes and sends N7:SMPolicyUpdateReq with UE_IP_CH trigger to the selected PCF. The REST-EP receives a response from the PCF.
37	The REST-EP sends N7:SMPolicyUpdateSuccess to the SMF-service.
38	The SMF-service instructs the REST-EP pod to trigger N40:ChargingDataRequest.
39	The REST-EP decides whether to perform the NF discovery or static NF selection of CHF based on the configuration.
40	The REST-EP encodes and sends the CHF discovery request to the NRF. The REST-EP receives a successful response with the list of CHFs.
41	The REST-EP encodes and sends N40:ChargingDataRequest to the selected CHF. The REST-EP receives a response from the CHF.
42	The REST-EP forwards N40:ChargingDataResponse to the SMF-service.
43	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionEstablishmentRequest.
44	The SMF-Protocol encodes and sends the N4:SessionEstablishmentRequest to the UDP-Proxy pod.
45	The UDP-Proxy pod sends the N4:SessionEstablishmentRequest to the UPF. The UDP-Proxy receives a response from the UPF.
46	The UDP-Proxy forwards the N4:SessionEstablishmentResponse to the SMF-Protocol pod.
47	The SMF-protocol forwards the N4:SessionEstablishmentResponse to the SMF-service.

Step	Description
48	The SMF-service instructs the REST-EP to trigger N11:N1N2MessageTransferReq.
49	The REST-EP decides whether to perform NF discovery or static NF selection of AMF based on the configuration.
50	The REST-EP encodes and sends the AMF discovery request to the NRF. The REST-EP receives a successful response with the list of AMFs.
51	The REST-EP encodes and sends N11:N1N2MessageTransferReq to the selected AMF. The REST-EP receives a successful response from the AMF.
52	The REST-EP forwards the N11:N1N2MessageTransferSuccess to the SMF-service.
53	The REST-EP stops the transaction-2 timer started in step 26.
54	The SMF-service updates the session entry in the CDL.
55	The REST-EP receives N11:SMContextUpdate from the AMF.
56	The REST-EP looks-up for session affinity in the cache pod and identifies the SMF-service handling the session.
57	The REST-EP starts the timer associated with transaction-3.
58	The REST-EP forwards the N11:SMContextUpdate to the SMF-service pod learnt in step 56.
59	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionModificationRequest.
60	The SMF-Protocol encodes and sends the N4:SessionModificationRequest to the UDP-Proxy pod.
61	The UDP-Proxy pod sends the N4:SessionModificationRequest to the UPF. The UDP-Proxy receives a response from the UPF.
62	The UDP-Proxy forwards the N4:SessionModificationResponse to the SMF-Protocol pod.
63	The SMF-protocol forwards the N4:SessionModificationResponse to the SMF-service.
64	The SMF-service forwards the N11:SMContextUpdateSuccess to the REST-EP.
65	The REST-EP forwards the N11:SMContextUpdateSuccess to the AMF.
66	The REST-EP stops the transaction-3 timer started in step 57.
67	The SMF-service updates the session entry in the CDL.
68	The SMF-service stops the procedure timer (guard timer/SLA timer).

Session Affinity

The SMF supports session affinity to facilitate stateless architecture.

When a session management procedure is ongoing for a subscriber session in some SMF service instance and another event from the network comes for the same subscriber in the meantime. Then, the SMF protocol layer micro-services, such as "smf-rest-ep" and "smf-protocol" direct these events towards the concerned SMF service instance. This ensures that all network events pertaining to an ongoing procedure of a subscriber session are handled by the same SMF service instance until the completion of the procedure.

Upon completion of the procedure, the subscriber session information is updated in the database and the session affinity towards the SMF service instance is removed. Subsequent network events can be handled by any of the available SMF service instances, by fetching the relevant subscriber session information from the database.

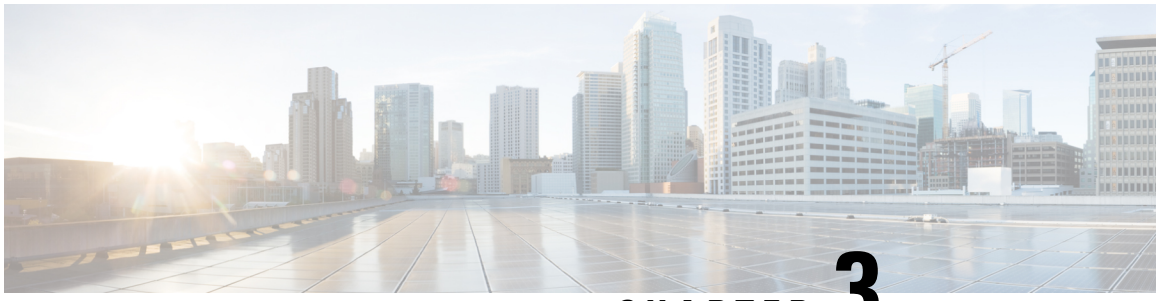
License Information

The SMF supports Cisco Smart Licensing. For more information, see the Smart Licensing, on page 39 chapter in this document.

Standards Compliance

Cisco SMF complies with the following 3GPP standards as per Release 15 June 2019:

- *3GPP TS 23.510, version 15.4.0*
- *3GPP TS 29.274, version 15.8.0*
- *3GPP TS 23.007, version 15.4.0*
- *3GPP TS 23.501, version 15.6.0*
- *3GPP TS 29.244, version 15.6.0*
- *3GPP TS 33.515, version 0.4.0*
- *3GPP TS 29.510, version 15.3.0*
- *3GPP TS 32.255, version 15.3.0*
- *3GPP TS 32.291, version 15.3.0*
- *3GPP TS 32.290, version 15.4.0*
- *3GPP TS 29.501, version 15.4.0*
- *3GPP TS 23.503, version 15.6.0*
- *3GPP TS 24.501, version 15.4.0*
- *3GPP TS 24.502, version 15.4.0*
- *3GPP TS 24.503, version 15.4.0*
- *3GPP TS 29.518, version 15.4.0*
- *3GPP TS 23.402, version 15.3.0*
- *3GPP TS 38.413, version 15.4.0*
- *3GPP TS 23.401, version 15.8.0*
- *3GPP TS 29.500, version 15.8.0*



CHAPTER 3

Deploying and Configuring SMF through Ops Center

- Feature Summary and Revision History, on page 33
- Feature Description, on page 34
- Deploying and Accessing SMF, on page 35
- SMF Service Configuration, on page 36
- Loading Day 1 Configuration, on page 37

Feature Summary and Revision History

Summary Data

Table 6: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 7: Revision History

Revision Details	Release
SMF deployment on bare metal server is supported and fully qualified in this release.	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF deployment and configuration procedure involves deploying the SMF through the Subscriber Microservices Infrastructure (SMI) Cluster Deployer and configuring the settings or customizations through the SMF Operations (Ops) Center. The Ops Center is based on the ConfD CLI. The SMF configuration includes the NRF profile data configuration and the externally visible IP addresses and ports.

SMF Ops Center

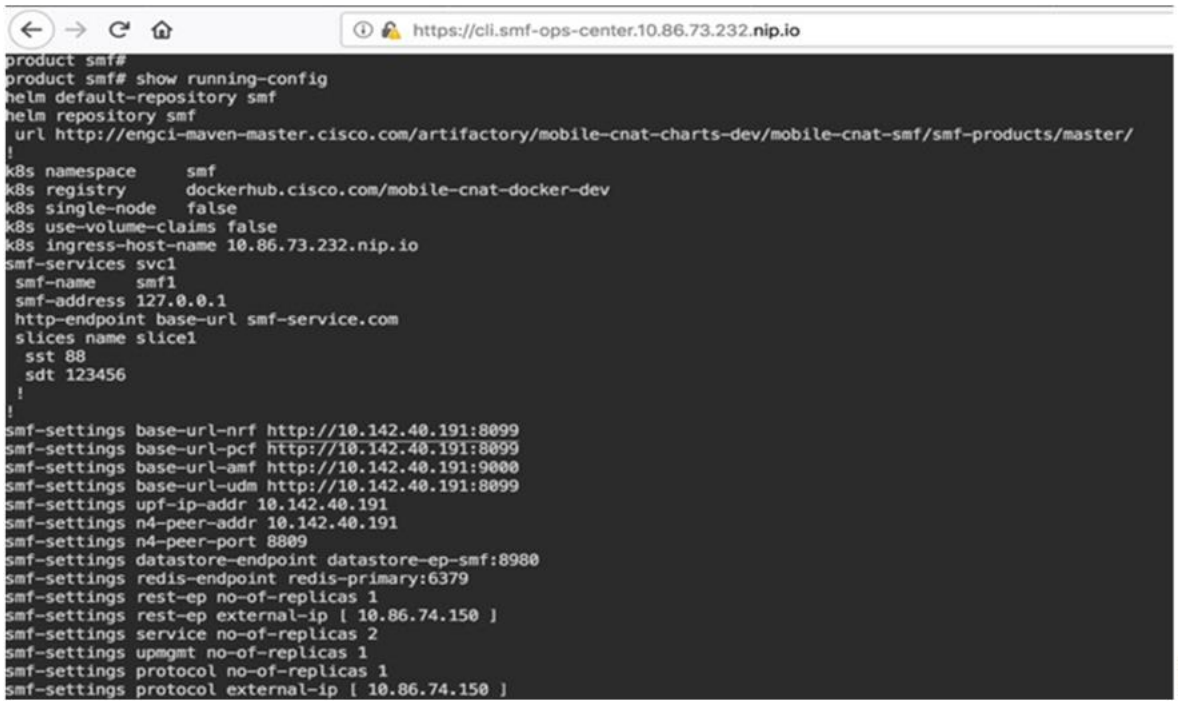
The Ops Center is a system-level infrastructure that provides the following functionality:

- A user interface to trigger a deployment of microservices with the flexibility of providing variable helm chart parameters to control the scale and properties of Kubernetes objects (deployment, pod, services, and so on) associated with the deployment.
- A user interface to push application-specific configuration to one or more microservices through Kubernetes configuration maps.
- A user interface to issue application-specific execution commands (such as show and clear commands). These commands:
  - Invoke some APIs in application-specific pods
  - Display the information returned on the user interface application

The SMF Ops Center allows you to configure the features such as licensing, SMF engine, REST Endpoint, and CDL.

The following screenshot shows the sample web-based command line interface:

Figure 11: Web-based CLI of Ops Center



Prerequisites

Before deploying SMF on the SMI layer:

- Ensure that all the virtual network functions (VNFs) are deployed.
- Run the SMI synchronization operation for the SMF Ops Center and Cloud Native Common Execution Environment (CN-CEE).
- Ensure that the node labels are configured as per the recommended pod deployment layout.
- Configure the external VIPs as per the NF requirement
- Enable Istio for pod-to-pod traffic load balancing

Deploying and Accessing SMF

This section describes how to deploy SMF and access the SMF Ops Center.

Deploying SMF

The Subscriber Microservices Infrastructure (SMI) platform is responsible for deploying and managing the Cloud Native 5G SMF application and other network functions.

For information on how to deploy SMF Ops Center on a vCenter environment, see *Deploying and Upgrading the Product* section in the *Ultra Cloud Core Subscriber Microservices Infrastructure—Operations Guide*.

For information on how to deploy SMF Ops Center on bare metal servers (currently Cisco UCS-C servers) environment, see *Operating the SMI Cluster Manager on Bare Metal* section in *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

Accessing the SMF Ops Center

You can connect to the SMF Ops Center through one of the following options:

- SSH
- Web-based console

To connect to the SMF Ops Center through SSH, use the following command:

ssh admin@*ops_center_pod_ip* **-p 2024**

Use the same user name and password as configured through the SMI Ops Center. For more information on the user management for access control, see the *CEE Configuration and Administration Guide*.

To connect to the Ops Center through Web-based console, perform the following steps:

1. Log on to the Kubernetes master node.
2. Run the following command:

   kubectl get ingress <*namespace*>

   The available ingress connections get listed.
3. Select the appropriate ingress and access the SMF Ops Center.
4. Access the following URL from your web browser:

   cli.<*namespace*>**-ops-center**.<*ip_address*>.**nip.io**

By default, the Day 0 configuration is loaded into the SMF.

To connect to the Ops center using FQDN and path-based URL routing, see the Configuring Hostname and URL-based Routing for Ingress section in the *Ultra Cloud Core Subscriber Microservices Infrastructure - Deployment Guide*.

SMF Service Configuration

The SMF service requires the basic configuration to process PDU Session Management API calls.

Mapping Pods with Node Labels

Prerequisites

- Ensure that the node labels are according to the pod deployment layout.
- Ensure that the external VIPs are according to the requirement of NF.
- Enable Istio for pod to pod traffic load balancing.

Node Labels are key and value pairs that are attached to nodes at cluster synchronization. Each node can have a set of key and value labels defined. Each key must be unique for a node. With labels, users can map their NF pods onto nodes in a loosely coupled manner.

Important

- The pod-level labeling configuration is applicable only when the SMF is deployed on a bare metal server.
- Ensure to configure the node label on the SMI cluster deployer before mapping the pods. Following is the sample command for master-1 labeling:

```
[cndp-clpnc-cm-cm-primary] SMI Cluster Deployer (config-nodes-master-1)# k8s node-labels
smi.cisco.com/svc-type smf-node
```

To map the pods with node labels, use the following sample configuration:

```
config
   k8 label protocol-layer key label_key value label_value
   k8 label service-layer key label_key value label_value
   k8 label cdl-layer key label_key value label_value
   k8 label oam-layer key label_key value label_value
   end
```

Following is an example configuration of pod to node-label mapping:

```
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
```

Loading Day 1 Configuration

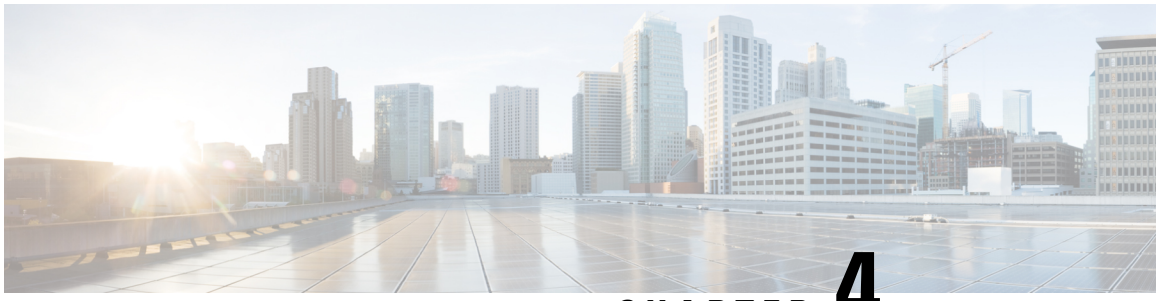
To load the Day 1 configuration for SMF, run the following command:

```
ssh admin@ops_center_pod_ip -p 2024  < Day1config.cli
```

Alternatively, you can copy the Day 1 configuration and paste it in the SMF Ops Center CLI to load the Day 1 configuration.

```
config
  <Paste the Day 1 configuration here>
  commit
  exit
```

To view the Day 1 configuration for SMF, see the Sample SMF Configuration, on page 1631 chapter.



CHAPTER 4

Smart Licensing

- Feature Summary and Revision History, on page 39
- Feature Description, on page 39
- Configuring Smart Licensing, on page 42
- Monitoring and Troubleshooting Smart Software Licensing, on page 52

Feature Summary and Revision History

Summary Data

Table 8: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 9: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Cisco employs two types of license models - Legacy Licensing and Smart Software Licensing. Legacy Licensing consists of software activation by installing Product Activation Keys (PAK) on to the Cisco product.

A Product Activation Key is a purchasable item, ordered in the same manner as other Cisco equipment and used to obtain license files for feature set on Cisco Products. This traditional licensing does not need any online communication with the Cisco licensing server.

Smart Software Licensing is a cloud-based licensing of the end-to-end platform through the use of a few tools that authorize and deliver license reporting. Smart Software Licensing functionality incorporated into the NFs complete the product registration and authorization. SMF supports the Smart Software Licensing model.

Smart Licensing simplifies the purchase, deployment, and management of Cisco software assets. Entitlements are purchased through your Cisco account through Cisco Commerce Workspace (CCW) and immediately available in your Virtual Account for usage. This approach eliminates the need to install license files on every device. Smart-enabled products communicate directly to Cisco to report consumption. A single location—Cisco Software Central—is available for customers to manage Cisco software licenses. License ownership and consumption are readily available to help make a better purchase decision that is based on consumption or business need.

For more information on Cisco Smart Licensing, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.

Cisco Software Central

Cisco Software Central (CSC) enables the management of software licenses and the smart account from a single portal. The CSC interface allows you to enable your product, manage entitlements, renew, and upgrade software. You need a functioning smart account to complete the registration process.

To access Cisco Software Central, see https://software.cisco.com.

Smart Accounts and Virtual Accounts

A Smart Account provides a single location for all smart-enabled products and entitlements. It helps in procurement, deployment, and maintenance of Cisco Software. When creating a smart account, you must have the authority to represent the requesting organization. After submission, the request goes through approval process.

A Virtual Account exists as a sub-account within the smart account. Virtual Accounts are customer-defined based on the organizational layout, business function, geography, or any defined hierarchy. Smart account administrator creates and maintains the virtual accounts.

For information on setting up or managing the Smart Accounts, see https://software.cisco.com.

Requesting a Cisco Smart Account

A Cisco Smart Account is an account where smart licensing-enabled products are available. A Cisco smart account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your smart licensing products. IT administrators can manage licenses and account users within the organization's smart account through Cisco Software Central. To create a Cisco Smart Account, perform the following steps:

Step 1 Visit the following URL:

```
https://software.cisco.com
```

Step 2 Log in using your credentials, and click **Request a Smart Account** in the **Administration** area.

The **Smart Account Request** window appears.

Step 3 Under **Create Account**, select one of the following options:

- **Yes, I have authority to represent my company and want to create the Smart Account**. If you select this option, you agree to authorize to create and manage product and service entitlements, users, and roles, on behalf of the organization.
- **No, the person specified below will create the account**. If you select this option, you must enter the email address of the person who creates the smart account.

Step 4 Under **Account Information**,

a) Click **Edit** beside **Account Domain Identifier**.
b) In the **Edit Account Identifier** dialog box, enter the domain, and click **OK**. By default, the domain is based on the email address of the person creating the account, and must belong to the company that will own this account.
c) Enter the **Account Name** (typically, the company name).

Step 5 Click **Continue**.

The Smart Account request will be in pending status until it is approved by the Account Domain Identifier. After the approval, you will receive an email confirmation with instructions for completing the setup process.

SMF Smart Licensing

The Smart Licensing feature supports application entitlement for online and offline licensing for all 5G applications (PCF, SMF, and NRF). The application usage is unrestricted during all stages of licensing including Out of Compliance (OOC) and expired stages.

Note A 90-day evaluation period is granted for all licenses in use. The functionality and operation of the 5G applications is unrestricted even after the end of the evaluation period.

Software Tags and Entitlement Tags

This section describes the software and entitlement tags that are available to identify report, and enforce licenses.

Software Tags

Software tags, also known as product tags, are unique identifiers for the Smart Licensing system to identify each licensable software product or product suite on a device. The Smart client uses this tag for identification during the addition of smart product instance in Cisco Software Central (CSC).

The following software tags exist for the SMF.

Product Type and Description	Software Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF,1.0_37ffdc21-3e95-4192-bcda-d3225b6590ce

Entitlement Tags

Entitlement tag is a part of the software that identifies the features in an image that are being used. These tags underlay the communication on usage and entitlements of software products that are installed on devices. The entitlement tag maps to both the product IDs (PID) license and the software image. Every Smart-enabled PID contains one or more entitlement tags.

The following entitlement tags identify licenses in use:

Product Type and Description	Entitlement Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF_BASE,1.0_b49f5997-21aa-4d15-9606-0cff88729f69

Note The license information is retained during software upgrades and rollback.

Configuring Smart Licensing

You can configure Smart Licensing after the SMF deployment.

Users with Access to CSC

This section describes how to configure Smart Licensing if you have access to CSC portal from your environment.

Setting Up the Product and Entitlement in CSC

Before you begin, you need to set up your product and entitlement in the CSC. To set up your product and entitlement:

1. Log on to your CSC account.
2. Click **Add Product** and enter the following details:
   - **Product name**–Specify the name of the deployed product. For example, SMF.
   - **Primary PM CEC ID**–Specify the primary Project Manager's CEC ID for the deployed product.
   - **Dev Manager CEC ID**–Specify the Development Manager's CEC ID for the deployed product.

- **Description** (Optional)–Specify a brief description of the deployed product.
- **Product Type**–Specify the product type.
- **Software ID Tag**–Specify the software ID Tag provided by the Cisco Accounts team.

3. Click **Create**.
4. Select your product from the **Product/Entitlement Setup** grid.
5. From the **Entitlement** drop-down list, select **Create New Entitlement**.
6. Select **New Entitlement** in **Add Entitlement** and enter the following details:
   - **Entitlement Name**–Specify the license entitlement name. For example, SMF_BASE.
   - **Description** (Optional)–Enter a brief description about the license entitlement.
   - **Entitlement Tag**–Specify the entitlement tag provided by the Cisco Accounts team.
   - **Entitlement Type**–Specify the type of license entitlement.
   - **Vendor String**–Specify the vendor name.
7. Click **Entitlement Allocation**.
8. Click **Add Entitlement Allocation**.
9. In **New License Allocation**, enter the following details:
   - **Product** – Select your product from the drop-down list.
   - **Entitlement** – Select your entitlement from the drop-down list.
10. Click **Continue**.
11. In **New License Allocation** window, enter the following details:
    - **Quantity**–Specify the number of licenses.
    - **License Type**–Specify the type of license.
    - **Expiring Date**–Specify the date of expiry for the license purchased.
12. Click **Create**.
13. Verify the status of Smart Licensing by using the following command.

    show license all

    Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed
```

```
License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Registering Smart Licensing

You must register the product entitled to the license with CSC. To register, you must generate an ID token from CSC.

1. Log on to your CSC account.
2. Click **General > New Token** and enter the following details:
   - **Description**–Provide a brief description about the ID token.
   - **Expires After**–Specify the number of days for the token to expire.
   - **Max. Number Users**–Specify the maximum number of users.
3. Click **Create Token**.
4. Select **New ID token** in **Product Instance Registration Token**.
5. Click **Actions > Copy**.

6. Log on to SMF Ops Center CLI and paste the **ID token** by using the following command.

   license smart register *idtoken*

   Example:

```
SMF# license smart register
Value for 'idtoken' (<string>): MTI2Y2FlNTAtOThkMi00YTAxLWE4M2QtOTNhNzNjNjY4ZmFiLTE2MTc4N
Tky%0AMTA5MDh8ck1jUHNwc3k1ZC9nWFFCSnVEcUp4QU1jTFoxOGxDTU5kQ3lpa25E%0Ab04wST0%3D%0A
SMF#
```

7. Verify the Smart Licensing status by using the following command.

   show license all

   Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems, Inc.
  Virtual Account: SMF-SMF
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Last Renewal Attempt: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Next Renewal Attempt: Oct 12 05:45:07 2020 GMT
  Registration Expires: Apr 15 05:40:31 2021 GMT

License Authorization:
  Status: AUTHORIZED on Apr 15 05:45:12 2020 GMT
  Last Communication Attempt: SUCCEEDED on Apr 15 05:45:12 2020 GMT
  Next Communication Attempt: May 15 05:45:12 2020 GMT
  Communication Deadline: Jul 14 05:40:40 2020 GMT

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
License Authorization Status: AUTHORIZED as of Apr 15 05:45:12 2020 GMT

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED_ALLOWED
```

```
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

NOTES:

- **license smart register** : Register Smart Licensing with CSC.
- *idtoken* : Specify the ID token generated from CSC.

Deregistering Smart Licensing

To deregister Smart Licensing:

1. Log on to SMF Ops Center CLI and use the following command.

   `license smart deregister`

2. Verify the Smart Licensing status by using the following command:

   `show license all`

   Example:

```
SMF# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=============
```

```
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13

SMF#
```

NOTES:

- **license smart deregister** : Deregisters Smart Licensing from CSC.

Users without Access to CSC

The Smart License Reservation feature – Perpetual Reservation – is reserved for customers without access to CSC from their internal environments. With this feature, Cisco allows customers to reserve licenses from their virtual account and tie them to their devices Unique Device Identifier (UDI). Smart License Reservation enables customers to use their devices with reserved licenses in a disconnected mode.

The subsequent sections describe the procedure involved in reserving Smart License for users without access to CSC from their internal environment.

Enabling Smart License Reservation

To enable Smart License reservation through SMF Ops Center CLI:

Log on to SMF Ops Center CLI and use the following configuration.

```
config
   license smart reservation
   commit
   exit
```

NOTES:

license smart reservation : Enable license reservation.

Generating Smart License Reservation Request Code

Note Before generating the Smart License reservation request code, complete the Enabling Smart License Reservation.

To generate the Smart License reservation request code, use the following command:

`license smart reservation request`

Example:

```
SMF# license smart reservation request
reservation-request-code CJ-ZSMF:6GKJ2OA-NMUWA7Y-Ai75GxtBs-3B
SMF#
Message from confd-api-manager at 2020-04-15 05:51:37...
Global license change NotifyReservationInProgress reason code Success - Successful.
SMF#
```

NOTES:

- **license smart reservation** : Enable license reservation request code.
- **license smart reservation request** : Generate the license reservation request code.

Important You must copy the generated license request code from the SMF Ops Center CLI.

Generating an Authorization Code from CSC

To generate an authorization code from CSC using the license reservation request code:

1. Log on to your CSC account.
2. Click **License Reservation** .
3. Copy the request code from the SMF Ops Center CLI and paste the request code in the **Reservation Request Code** text-box.
4. Click **Reserve a Specific License** option and select *UCC 5G SMF BASE*.

Note In the **Reserve** text-box enter the value *1*.

5. Review your selection.
6. Click **Generate Authorization Code**.
7. The authorization code is generated and displayed on-screen. Either click **Copy to Clipboard** or **Download as File** to download the authorization code.
8. Click **Close**.

Reserving Smart Licensing

There are two methods available to reserve the Smart License:

- Key-based: Using the copied clipboard content of the authorization code directly from the CSC.
- URL-based: Using the downloaded file containing the authorization code from CSC, saved on the local server.

To reserve Smart License for the deployed product:

1. Log on to SMF Ops Center CLI and enter the following command.

   Key-based:

   license smart reservation install *authorization_code*

   Example:

   SMF# license smart reservation install

```
Value for 'key' (<string>):
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>35757dc6-2bdf-4fa1-ba7e-4190f5b6ea22</piid><timestamp>1586929992297</timestamp>
<entitlements><entitlement><tag>regid.2020-04.com.cisco.SMF_BASE,1.0_60b1da6f-3832-4687-90c9-8879dc815a27</tag>
<count>1</count><startDate>2020-Apr-08 UTC</startDate><endDate>2020-Oct-05 UTC</endDate>
<licenseType>TERM</licenseType><displayName>UCC 5G SMF BASE</displayName>
<tagDescription>Ultra Cloud Core - Session Management Function (SMF), Base
Minimum</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQC/9v5LpgFoEk2l4omIgjjk83g5WXjzs09kQnsO8D0jRgIhAMh+
D6DRuYmqh1TlfJoZxNte0fPKw6fHEY5CEF3+kPQj</signature>
<udi>P:SMF,S:6GKJ2OA-NMUWA7Y</udi></specificPLR>
SMF#
```

   URL-based:

   license smart reservation install url { path *httpPath*
   [username *username* **| password** *password* **] }**

   Example:

```
SMF# license smart reservation install url { username smf password **** path http://
209.165.202.155:8000/AuthorizationCode_SN_6OUP5ZY-LMXHB2A.txt }
```

2. Verify the smart licensing status by using the following command.

   show license all

   Example:

   show license all

```
Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Wed Apr 15 05:53:31 GMT 2020
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020

Utility:
  Status: DISABLED
Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
```

```
License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF),
Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>
  Reservation:
    Reservation Status: SPECIFIC INSTALLED
    Total Reserved Count: 1
    Term expiration: 2020-Oct-05 GMT

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

NOTES:

- **license smart reservation install key** *authorization_code* : Installs a Smart License Authorization code.
- **license smart reservation install url** *path* : Downloads the file containing the authorization code from CSC, saved on the local server.

Returning the Reserved License

You can return the reserved license to CSC, if required. Use the following procedure to return the reserved license:

1. When you install the license reservation authorization in the SMF Ops Center.
   a. Log on to the SMF Ops Center CLI and use the following command.

      license smart reservation return

      Example:

      ```
      SMF# license smart reservation return
      reservation-return-code CJ6m3k-RAvu6b-hMNmwf-mrdcko-NoSwKL-tF7orz-9aNtEu-yVjGAm-D6j
      SMF#
      ```

Note If there is an issue with the return code generation, open a case with the Cisco Technical Assistance Center.

b. Copy the license reservation return code generated in SMF Ops Center CLI.

c. Log on to your CSC account.

d. Select your product instance from the list in the Product Instances tab.

e. Click **Actions** > **Remove**.

f. Paste the license reservation return code in **Return Code** text-box.

g. Select **Remove Product Instance**.

NOTES:

- **license smart reservation return** : Return a reserved Smart License.

2. When the license reservation authorization code is not installed in the SMF Ops Center.

   a. Log on to the SMF Ops Center CLI and use the following command to generate the return code.

   `license smart reservation return`
   `authorization_code`

   Paste the license reservation authorization code generated in CSC to generate the return code.

   b. Log on to your CSC account

   c. Select your product instance from the list in the Product Instances tab.

   d. Click **Actions** > **Remove**.

   e. Paste the license reservation return code in **Return Code** text-box.

   f. Select **Remove Product Instance**.

3. Verify the smart licensing status by using the following command.

   `show license all`

   Example:

   `SMF# show license all`

```
Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
  Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
  Next Communication Attempt: NONE
  Communication Deadline: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED
```

```
Utility:
  Status: DISABLED

Transport:
   Type: Smart Transport
   Registration URL: null
   Utility URL: null

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y

Agent Version
=============
Smart Agent for Licensing: 3.0.13

SMF#
```

Canceling License Reservation Request

To cancel a license reservation request through the SMF Ops Center CLI:

Log on to the SMF Ops Center CLI and use the following command.

`license smart reservation cancel`

Monitoring and Troubleshooting Smart Software Licensing

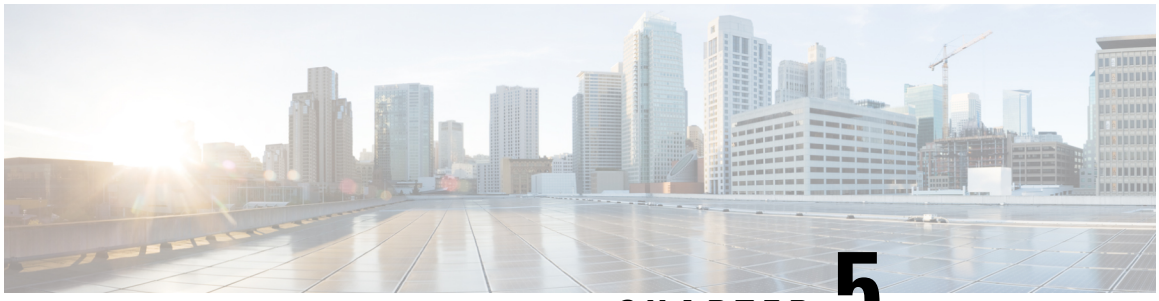
To view Smart Licensing related information in the SMF Ops Center, use the following show commands.

`show license [ all | UDI | displaylevel | reservation | smart | status | summary | tech-support | usage ]`

NOTES:

- **all** : Displays an overview of Smart Licensing information that includes license status, usage, product information, and Smart Agent version.
- **UDI**: Displays Unique Device Identifiers (UDI) details.
- **displaylevel**: Depth to display information.

- **reservation**: Displays Smart Licensing reservation information.
- **smart**: Displays Smart Licensing information.
- **status**: Displays the overall status of Smart Licensing.
- **summary**: Displays the summary of Smart Licensing.
- **tech-support**: Displays Smart Licensing debugging information.
- **usage**: Displays the license usage information for all the entitlements that are currently in use.



CHAPTER 5

SMF Rolling Software Update

- Feature Summary and Revision History, on page 55
- Feature Description, on page 56
- Updating SMF, on page 56

Feature Summary and Revision History

Summary Data

Table 10: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 11: Revision History

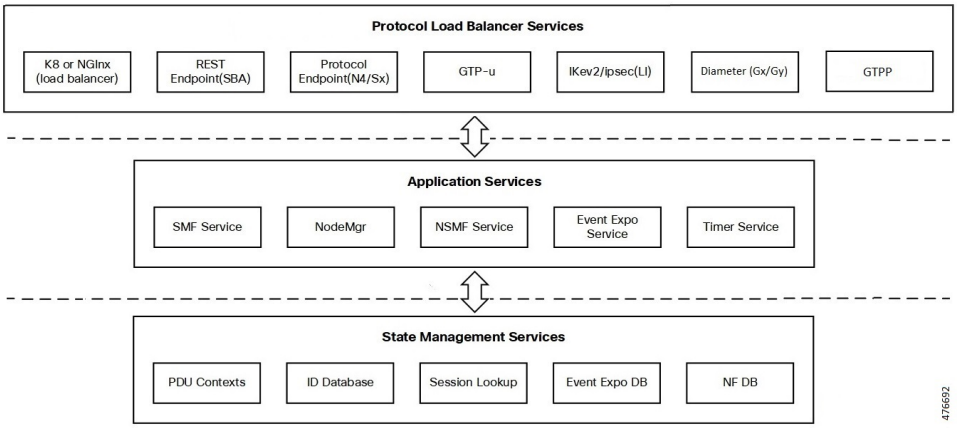
Revision Details	Release
Added Support for Diameter Gx, Gy, and GZ(GTP-Prime)	2023.02.0
First introduced.	Pre-2020.02.0

Feature Description

The Cisco SMF has a three-tier architecture consisting of Protocol, Service, and Session tiers. Each tier includes a set of microservices (pods) for a specific functionality. Within these tiers, there exists a Kubernetes Cluster comprising Kubernetes (K8s) master and worker nodes (including Operation and Management nodes).

For high availability and fault tolerance, a minimum of two K8s worker nodes are required for each tier. You can have multiple replicas for each worker node. Kubernetes orchestrates the pods using the StatefulSets controller. The pods require a minimum of two replicas for fault tolerance.

Figure 12: SMF Architecture



An SMF K8s Cluster contains 12 nodes:

- Three Master nodes.
- Three Operations and Management (OAM) worker nodes.

  OAM worker nodes host the Ops Center pods for configuration management and metrics pods for statistics and Key Performance Indicators (KPIs).

- Two Protocol worker nodes.

  Protocol worker nodes host the SMF protocol-related pods for service-based interfaces (N11, N7, N10, N40, NRF), UDP-based protocol interfaces (N4, S5/S8, RADIUS) and TCP-based interfaces Diameter (Gx/Gy), and GTPP (Gz).

- Two Service worker nodes.

  Service worker nodes host the SMF application-related pods that perform session management processing.

- Two Session (data store) worker nodes.

  Session worker nodes host the database-related pods that store subscriber session data.

Updating SMF

The following section describes the procedure involved in updating the SMF software.

Rolling Software Update Using SMI Cluster Manager

Rolling software upgrade is a process of upgrading or migrating the build from older to newer version or upgrading the patch for the prescribed deployment set of application pods.

Note The 2021.02 release does not support rolling upgrade or in-service upgrade in a non-HA deployment. To upgrade to release 2021.02 in a non-HA deployment, you must perform a fresh SMF deployment from the Ops Center.

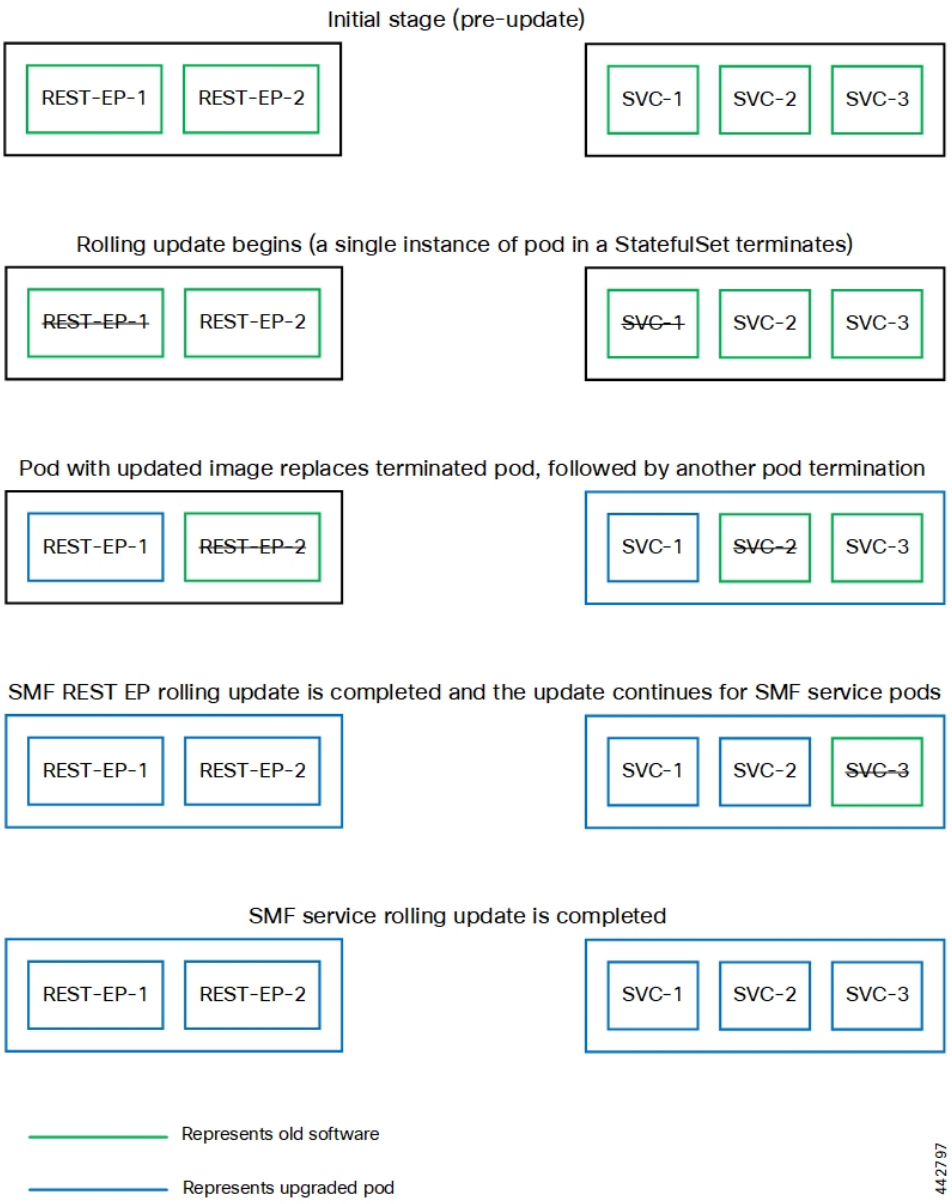
After the fresh deployment is complete, make sure that all the Geo Redundant (GR) instance-aware configuration changes are available. Also, make sure to clean up the etcd entries if the ***etcd persistence*** is enabled through ***k8s volume-claims true*** command. For the clean-up operation, use the ***kubectl exec -it etcd-<namespace>-etcd-cluster-0 -n cn-cn1 -- etcdctl del --prefix "*** command.

The SMF software update or in-service update procedure utilizes the K8s rolling strategy to update the pod images. In K8s rolling update strategy, the pods of a StatefulSet are updated sequentially to ensure that the ongoing process remains unaffected. Initially, a rolling update on a StatefulSet causes a single pod instance to terminate. A pod with an updated image replaces the terminated pod. This process continues until all the replicas of the StatefulSet are updated. The terminating pods exit gracefully after completing all the ongoing processes. Other in-service pods continue to receive and process the traffic to provide a seamless software update. You can control the software update process through the Ops Center CLI.

Note Each pod needs a minimum of two pods for high availability. In the worst-case scenario, the processing capacity of the pod may reduce to 50% while the software update is in progress.

The following figure illustrates an SMF rolling update for SMF REST Endpoint pods (two replicas) on Protocol worker nodes along with SMF Service pods (three replicas) on Service worker nodes.

Figure 13: SMF Rolling Update



Important ETCD v3.5.x does not support in-service downgrade to 3.4.x. If you're downgrading from 2023.04.0 builds to previous releases. perform system mode shutdown before downgrade.

Prerequisites

The prerequisites for upgrading SMF are:

- All the nodes including the pods are active.

- A patch version of the SMF software.

Note Major versions does not support rolling upgrade.

Important Trigger rolling update only when the CPU usage of the nodes is less than 50%.

SMF Health Check

Before you perform health check, ensure that all the services are running and the nodes are in ready state. To perform health check, log on to master node and use the following configuration:

```
kubectl get pods -n smi
kubectl get nodes
kubectl get pod --all-namespaces -o wide
kubectl get pods -n smf-wsp -o wide
kubectl get pods -n cee-wsp -o wide
kubectl get pods -n smi-vips -o wide
helm list
kubectl get pods -A | wc -l
```

Preparing the Upgrade

This section describes the procedure for creating a backup configuration, logs, and deployment files. To backup the files:

1. Log on to the SMI Cluster Manager Node as an **ubuntu** user.
2. Create a new directory for deployment.

   Example:

   ```
   test@smismf-cm01:~$ mkdir -p "temp_$(date +'%m%d%Y_T%H%M')" && cd "$_"
   ```

3. Move all the working files into the newly created deployment directory.
4. Untar the *smf* deployment file.

   Example:

   ```
   test@smi1smf01-cm01:~/temp_08072019_T1651$ tar -xzvf smf.2020.01.0-1.SPA.tgz
   ./
   ./smf_REL_KEY-CCO_RELEASE.cer
   ./cisco_x509_verify_release.py
   ./smf.2020.01.0-1.tar
   ./smf.2020.01.0-1.tar.signature.SPA
   ./smf.2020.01.0-1.tar.SPA.README
   ```

5. Verify the downloaded image.

   Example:

   ```
   test@smi1smf01-cm01:~/temp_08072019_T1651$ cat smf.2020.01.0-1.tar.SPA.README
   ```

Important Follow the procedure mentioned in the *SPA.README* file to verify the build before proceeding to the Back Up Ops Center Configuration section.

Back Up Ops Center Configuration

This section describes the procedure for creating a backup of the Ops Center configurations.

To perform a backup of the Ops Center configurations, use the following steps:

1. Log on to SMI Cluster Manager node as an **ubuntu** user.
2. Run the following command to backup the SMI Ops Center configuration to `/home/ubuntu/smiops.backup` file.

   ```
   ssh -p port_number admin@$(kubectl get svc -n smi | grep
   '.*netconf.*<port_number>' | awk '{ print $4 }') "show run | nomore"
   > smiops.backup_$(date +'%m%d%Y_T%H%M')
   ```

3. Run the following command to backup the CEE Ops Center configuration to `/home/ubuntu/ceeops.backup` file.

   ```
   ssh admin@<cee-vip> "show run | nomore" > ceeops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

4. Run the following command to backup the SMF Ops Center configuration to `/home/ubuntu/smfops.backup` file.

   ```
   ssh admin@<smf-vip> "show run | nomore" > smfops.backup_$(date
   +'%m%d%Y_T%H%M')
   ```

Back Up CEE and SMF Ops Center Configuration

This section describes the procedure to create a backup of CEE and Ops Center configuration from the master node.

To perform a backup of CEE and Ops Center configuration, , use the following steps:

1. Log in to the master node as an **ubuntu** user.
2. Create a directory to backup the configuration files.

   mkdir backups_$(date +'%m%d%Y_T%H%M') && cd "$_"

3. Backup the SMF Ops Center configuration and verify the line count of the backup files.

   ssh -p *port_number* **admin@$(kubectl get svc -n $(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep***port_number* **| awk '{ print $3 }') "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M') && wc -l smfops.backup_$(date +'%m%d%Y_T%H%M')**

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p 2024 admin@$(kubectl get svc -n
   $(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{ print
    $3 }') "show run | nomore" > smfops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
   smfops.backup_$(date +'%m%d%Y_T%H%M')
   admin@<ipv4address>'s password: smf-OPS-PASSWORD
   334 smfops.backup
   ```

4. Backup the CEE Ops Center configuration and verify the line count of the backup files.

   ssh -p *port_number* **admin@$(kubectl get svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep** *port_number* **| awk '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l ceeops.backup_$(date +'%m%d%Y_T%H%M')**

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p <port_number> admin@$(kubectl get
   svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk
   '{ print $3 }') "show run | nomore" > ceeops.backup_$(date +'%m%d%Y_T%H%M') && wc -l
   ceeops.backup_$(date +'%m%d%Y_T%H%M')
   admin@<ipv4address>'s password: CEE-OPS-PASSWORD
   233 ceeops.backup
   ```

5. Move the SMI Ops Center backup file from the SMI Cluster Manager to the backup directory.

   scp $(grep cm01 /etc/hosts | awk '{ print $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ scp $(grep cm01 /etc/hosts | awk '{ print
   $1 }'):/home/ubuntu/smiops.backup_$(date +'%m%d%Y_T%H%M') .
   ubuntu@<ipv4address>'s password: SMI-CM-PASSWORD
   smiops.backup                                                 100% 9346    22.3MB/s
      00:00
   ```

6. Verify the line count of the backup files.

   Example:

   ```
   ubuntu@posmf-mas01:~/backups_09182019_T2141$ wc -l *
     233 ceeops.backup
     334 smfops.backup
     361 smiops.backup
     928 total
   ```

Staging a New SMF Image

This section describes the procedure for staging a new SMF image before initiating the upgrade.

To stage the new SMF image:

1. Download and verify the new SMF image.
2. Log in to the SMI Cluster Manager node as an **ubuntu** user.
3. Copy the images to **Uploads** directory.

   sudo mv *smf_new_image.tar* **/data/software/uploads**

Note The SMI uses the new image available in the **Uploads** directory to upgrade.

4. Verify whether the image is picked up by the SMI for processing from the **Uploads** directory.

   sleep 30; ls /data/software/uploads

   Example:

```
ubuntu@posmf-cm01:~/temp_08072019_T1651$ sleep 30; ls /data/software/uploads
ubuntu@posmf-cm01:~/temp_08072019_T1651$
```

5. Verify whether the images were successfully picked up and processed.

   Example:

   ```
   auser@unknown:$ sudo du -sh /data/software/packages/*
   1.6G /data/software/packages/cee.2019.07
   5.3G /data/software/packages/smf.2019.08-04
   16K /data/software/packages/sample
   ```

   The SMI must extract the images into the **packages** directory to complete the staging.

Triggering the Rolling Software Upgrade

The SMF utilizes the SMI Cluster Manager to perform a rolling software update. To update SMF using SMI Cluster Manager, use the following configurations:

Important Before you begin, ensure that SMF is up and running with the latest version of the software.

1. Log in to SMI Cluster Manager Ops Center.
2. Download the latest TAR ball from the URL using the **software-packages download** *url* command.

   NOTES:

   software-packages download *url*: Specify the software packages to be downloaded through HTTP or HTTPS.

3. Verify whether the TAR balls are loaded.

   Example:

   ```
   SMI Cluster Manager# software-packages list
   [ smf-2019-08-21 ]
   [ sample ]
   ```

   NOTES:

   software-packages list: Specify the list of available software packages.

4. Update the product repository URL with the latest version of the product chart.

Note If the repository URL contains multiple versions, the Ops Center automatically selects the latest version.

```
configure
  cluster cluster_name
   ops-centers app_name smf_instance_name
       repository url
        exit
      exit
```

Example:

```
SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
```

```
SMI Cluster Manager(config-clusters-test2)# ops-centers smf data
SMI Cluster Manager(config-ops-centers-smf/data)# repository <url>
SMI Cluster Manager(config-ops-centers-smf/data)# exit
SMI Cluster Manager(config-clusters-test2)# exit
```

NOTES:

clusters *cluster_name* : Specify the information about the nodes to be deployed. *cluster_name* is the name of the cluster.

5. Run the following command to update to the latest version of the product chart.

   clusters *cluster_name* **actions sync run**

   Example:

   ```
   SMI Cluster Manager# clusters test2 actions sync run
   ```

NOTES:

- **ops-centers** *app_name instance_name* : Specifies the product Ops Center and instance. *app_name* is the application name. *instance_name* is the name of the instance.
- **repository** *url*: Specify the local registry URL for downloading the charts.
- **actions** : Specify the actions performed on the cluster.
- **sync run** : Trigger the cluster synchronization.

Important

- The cluster synchronization updates the SMF Ops Center, which in turn updates the application pods (through **helm sync** command) one at a time automatically.
- When you trigger rolling upgrade on a specific pod, the SMF avoids routing new calls to that pod.
- The SMF honors in-progress call by waiting for 30 seconds before restarting the pod where rolling upgrade is initiated. Also, the SMF establishes all the in-progress calls completely within 30 seconds during the upgrade period (maximum call-setup time is 10 seconds).

Monitoring the Upgrade

Use the following sample configuration to monitor the status of the upgrade through SMI Cluster Manager Ops Center:

```
config
  clusters cluster_name actions sync run debug true
  clusters cluster_name actions sync logs
  monitor sync-logs cluster_name
  clusters cluster_name actions sync status
  exit
```

NOTES:

- **clusters** *cluster_name*: Specifies the information about the nodes to be deployed. *cluster_name* is the name of the cluster.
- **actions**: Specifies the actions performed on the cluster.

- **sync run**: Triggers the cluster synchronization.
- **sync logs**: Shows the current cluster synchronization logs.
- **sync status**: Shows the current status of the cluster synchronization. **debug true**: Enters the debug mode.
- **monitor sync logs**: Monitors the cluster synchronization process.

Example:

```
SMI Cluster Manager# clusters test1 actions sync run
SMI Cluster Manager# clusters test1 actions sync run debug true
SMI Cluster Manager# clusters test1 actions sync logs
SMI Cluster Manager# monitor sync-logs test1
SMI Cluster Manager# clusters test1 actions sync status
```

Important You can view the pod details after the upgrade through CEE Ops Center. For more information on pod details, see Viewing the Pod Details section.

Viewing the Pod Details

Use the following sample configuration to view the details of the current pods through CEE Ops Center in CEE Ops Center CLI:

`cluster pods` *`instance_name pod_name`* **`detail`**

NOTES:

- **cluster pods** – Specifies the current pods in the cluster.
- *instance_name* – Specifies the name of the instance.
- *pod_name* – Specifies the name of the pod.
- **detail** – Displays the details of the specified pod.

The following example displays the details of the pod named *alertmanager-0* in the *smf-data* instance.

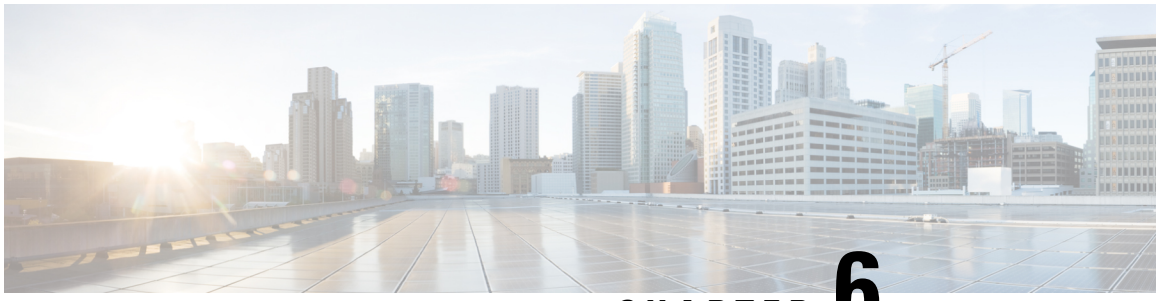
Example:

```
cee# cluster pods smf-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
    alermanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
  creationTimestamp: "2020-02-26T06:09:13Z"
  generateName: "alertmanager-"
  labels:
    component: "alertmanager"
    controller-revision-hash: "alertmanager-67cdb95f8b"
    statefulset.kubernetes.io/pod-name: "alertmanager-0"
  name: "alertmanager-0"
  namespace: "smf"
  ownerReferences:
  - apiVersion: "apps/v1"
    kind: "StatefulSet"
```

```
    blockOwnerDeletion: true
    controller: true
    name: "alertmanager"
    uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
  resourceVersion: "1654031"
  selfLink: "/api/v1/namespaces/smf/pods/alertmanager-0"
  uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
spec:
  containers:
  - args:
    - "/alertmanager/alertmanager"
    - "--config.file=/etc/alertmanager/alertmanager.yml"
    - "--storage.path=/alertmanager/data"
    - "--cluster.advertise-address=$(POD_IP):6783"
    env:
    - name: "POD_IP"
      valueFrom:
        fieldRef:
          apiVersion: "v1"
          fieldPath: "status.podIP"
    image: "<path_to_docker_image>"
    imagePullPolicy: "IfNotPresent"
    name: "alertmanager"
    ports:
    - containerPort: 9093
      name: "web"
      protocol: "TCP"
    resources: {}
    terminationMessagePath: "/dev/termination-log"
    terminationMessagePolicy: "File"
    volumeMounts:
    - mountPath: "/etc/alertmanager/"
      name: "alertmanager-config"
    - mountPath: "/alertmanager/data/"
      name: "alertmanager-store"
    - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
      name: "default-token-kbjnx"
      readOnly: true
  dnsPolicy: "ClusterFirst"
  enableServiceLinks: true
  hostname: "alertmanager-0"
  nodeName: "for-smi-cdl-1b-worker94d84de255"
  priority: 0
  restartPolicy: "Always"
  schedulerName: "default-scheduler"
  securityContext:
    fsGroup: 0
    runAsUser: 0
  serviceAccount: "default"
  serviceAccountName: "default"
  subdomain: "alertmanager-service"
  terminationGracePeriodSeconds: 30
  tolerations:
  - effect: "NoExecute"
    key: "node-role.kubernetes.io/oam"
    operator: "Equal"
    value: "true"
  - effect: "NoExecute"
    key: "node.kubernetes.io/not-ready"
    operator: "Exists"
    tolerationSeconds: 300
  - effect: "NoExecute"
    key: "node.kubernetes.io/unreachable"
    operator: "Exists"
```

```
    tolerationSeconds: 300
  volumes:
  - configMap:
      defaultMode: 420
      name: "alertmanager"
    name: "alertmanager-config"
  - emptyDir: {}
    name: "alertmanager-store"
  - name: "default-token-kbjnx"
    secret:
      defaultMode: 420
      secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "ContainersReady"
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID: "docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"

    image: "<path_to_docker_image>"
    imageID: "docker-pullable://<path_to_docker_image>"
    lastState: {}
    name: "alertmanager"
    ready: true
    restartCount: 0
    state:
      running:
        startedAt: "2020-02-26T06:09:05Z"
  hostIP: "<host_ipv4address>"
  phase: "Running"
  podIP: "<pod_ipv4address>"
  qosClass: "BestEffort"
  startTime: "2020-02-26T06:09:02Z"
cee#
```



CHAPTER 6

AN-initiated Session Modification and Release

- Feature Summary and Revision History, on page 67
- Feature Description, on page 67
- How it Works, on page 68

Feature Summary and Revision History

Summary Data

Table 12: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 13: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

The NG-AP signaling connection can be lost due to RAN or AMF failure. In this scenario, the RAN or AMF initiates the AN release procedure without relying on the signaling between RAN and AMF.

The AN-initiated PDU session release procedure involves releasing the logical NG-AP signaling connection for the UE between the RAN and the AMF and the associated N3 User Plane connections, and RAN signaling connection between the UE and the RAN and the associated RAN resources.

The initiation of AN release may be due to:

- RAN-initiated with cause, for example, O&M Intervention, Unspecified Failure, RAN (for example, Radio) Link Failure, User Inactivity, Inter-System Redirection, request for establishment of QoS Flow for IMS voice, Release due to UE-generated signaling connection release, mobility restriction, Release Assistance Information (RAI) from the UE, and so on, or
- AMF-initiated with cause like Unspecified Failure, and so on

Note For AN-initiated modification, SMF does not send policy update message towards PCF as mentioned in step 2 of section 4.3.3.2-1: UE or network requested PDU Session Modification in 3GPP TS 23.502.

How it Works

This section describes how the NG-AP signaling connection, UP connections, and AN resources associated with the PDU session are released.

RAN-initiated PDU Session Release Call Flow

The following call flow diagram represents the messages that are exchanged between UE and SMF when PDU session release is initiated by RAN or AMF. The RAN session release is as defined in 3GPP 23.502.

For this procedure, the impacted SMF and UPF are all under control of the PLMN serving the UE, for example, in Home-Routed roaming case, the SMF and UPF in HPLMN are not involved.

Figure 14: RAN-initiated PDU Session Release Call Flow

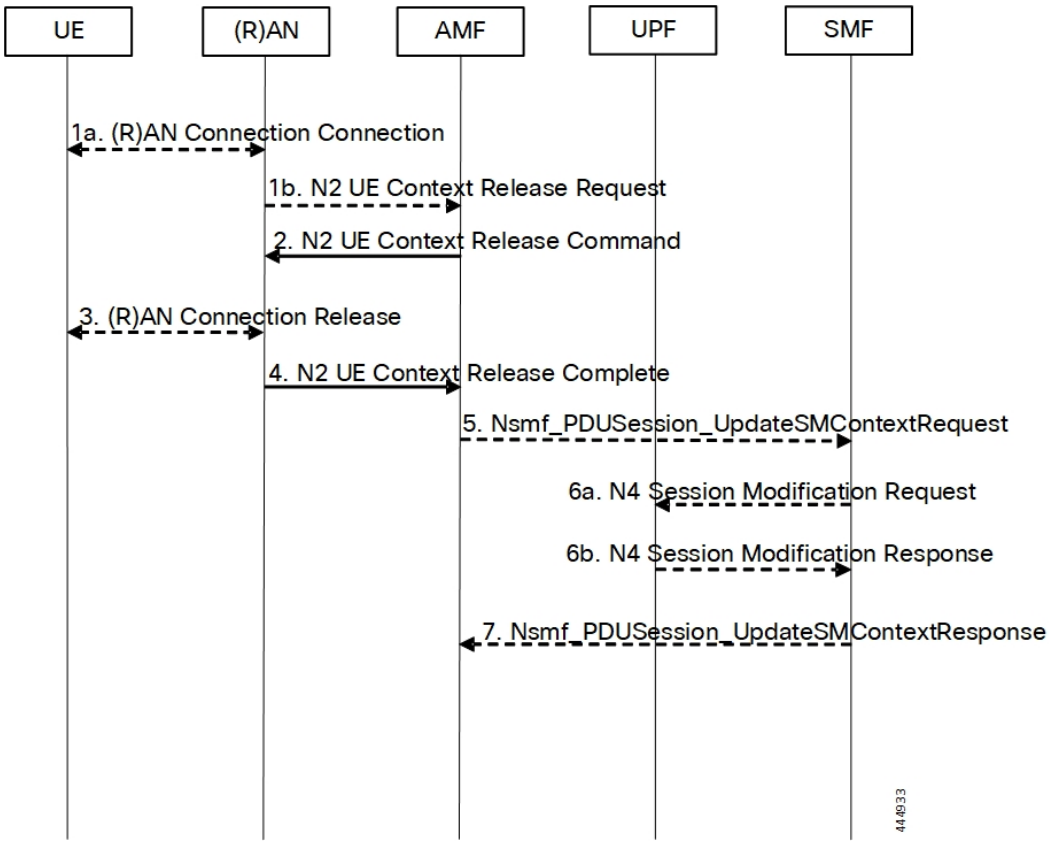


Table 14: RAN-initiated PDU Session Release Call Flow Description

Step	Description
1	In cases, such as Radio Link Failure or RAN internal failure, the RAN decides to initiate the UE context release and sends an N2 UE Context Release Request message to the AMF. If the reason for the release is the NG-RAN received an AS Release Assistance Indicator (RAI), NG-RAN does not release the RRC connection but sends an N2 UE Context Release Request message to the AMF. If the AS RAI indicates that only a single downlink transmission is expected, then NG-RAN sends only the N2 UE Context Release Request after a single downlink NAS PDU or N3 data PDU has been transferred. If N2 Context Release Request cause indicates the release, then release is requested due to user inactivity or AS RAI. Then, the AMF continues with the AN Release procedure unless the AMF is aware of pending MT traffic or signaling.

Step	Description
2	Upon receiving Release Request message from RAN, AMF sends N2 UE Context Release Command to RAN. If the AMF receives Service Request or Registration Request to establish another NAS signaling connection through RAN, after successfully authenticating the UE, the AMF releases the existing NAS signaling connection. Then, the AMF continues the Service Request or Registration Request procedure. The Cause indicates either the cause from (R)AN or the cause due to an AMF event.
3	If the UE connection is not released in Step 1, the RAN performs one of the following operations: • the RAN deletes the context of UE upon receiving RAN connection release confirmation • the RAN locally releases the RRC connection if the Cause in the Context Release Command indicates that the UE has locally released the RRC connection
4	**Note** When the UE does not acknowledge the RRC Connection Release, perform this step after Step 2. The RAN releases the N2 signaling connection with the AMF for the UE and sends an N2 UE Context Release Complete message to the AMF. This message includes the following information: • list of PDU session IDs that RAN serves with active N3 user plane • user location information • age of location information The AMF receives the UE Radio Capability information or NB-IoT specific UE Radio Access Capability Information from the NG-RAN node. The NG-RAN sends paging assistance data for CE-capable UE, if available, to AMF through the N2 UE Context Release Complete message. The AMF stores the received Paging Assistance Data for CE-capable UE in the UE context for subsequent paging procedure. **Note** If the PLMN has configured secondary RAT usage reporting, the NG-RAN node provides RAN usage data report.

Step	Description
5	For each of the PDU sessions in the N2 UE Context Release Complete, the AMF sends Nsmf PDU Session Update SM Context Request to SMF. This request message includes the following information: • PDU Session ID • PDU Session Deactivation • Cause (same as Step 2) • Operation Type • User Location Information • Age of Location Information • N2 SM Information (Secondary RAT usage data) If the Release Request message includes list of PDU session IDs with active N3 user plane as in Step 1, SMF and AMF perform Step 5 through Step 7 before Step 2. The Operation Type is set to "UP deactivate" to indicate deactivation of user plane resources for the PDU session. If the PDU sessions use Control Plane CIoT 5GS Optimization and if the UE negotiates the use of extended idle mode DRX, the AMF communicates that the UE is unreachable for downlink data to the SMF. If the PDU sessions use Control Plane CIoT 5GS Optimization and if the UE negotiates the use of MICO mode with active time, the AMF communicates that the UE is unreachable for downlink data to the SMF after the expiry of active time.
6	For PDU sessions not using Control Plane CIoT 5GS Optimization, the SMF sends an N4 Session Modification Request to the UPF. This request message includes the following details to indicate: • whether or not to remove the tunnel information of AN or UPF terminating N3. • whether or not to buffer the incoming DL PDU. If the AMF indicates that the UE is unreachable for downlink data, the SMF initiates an N4 Session Modification procedure to activate buffering in the UPF. If a PDU session uses multiple UPFs, the SMF sends the Modification Request to the specific UPF that terminates N3, and then releases the N4 session associated with that UPF. If the AN Release is due to user inactivity or UE redirection, the SMF preserves the GBR QoS Flows. Otherwise, the SMF triggers the PDU Session Modification procedure for the GBR QoS Flows of the UE after the AN Release procedure is completed. If the Ultra Reliable Low Latency Communication (URLLC) uses redundant I-UPFs, the SMF sends N4 Session Modification Request to each I-UPF. The SMF uses the buffering instructions to select the redundant I-UPFs for buffering, dropping, or forwarding the DL packets. If the URLLC uses redundant N3 tunnels, the SMF sends the modification request to the UPF of N3 termination point to remove the dual AN Tunnel Info for N3 tunnel of the corresponding PDU session.

Step	Description
6b	The UPF sends N4 Session Modification Response to the SMF.
7	The SMF sends Nsmf PDU Session Update SM Context Response to the AMF. Then, the AMF enters CM-IDLE state after releasing the N2 and N3 connection and sends an acknowledgment to the SMF.

RAN-initiated QoS Flow Mobility for Dual Connectivity

The RAN-initiated QoS flow mobility procedure involves transferring QoS flows to and from Secondary RAN Node without reallocation of SMF and UPF. It is assumed that the IP connectivity exists between the UPF and the primary RAN node, and between the UPF and the secondary RAN node.

The following call flow diagram represents the QoS flow exchange between Primary and Secondary RAN Nodes.

Figure 15: NG-RAN initiated QoS Flow Mobility Procedure

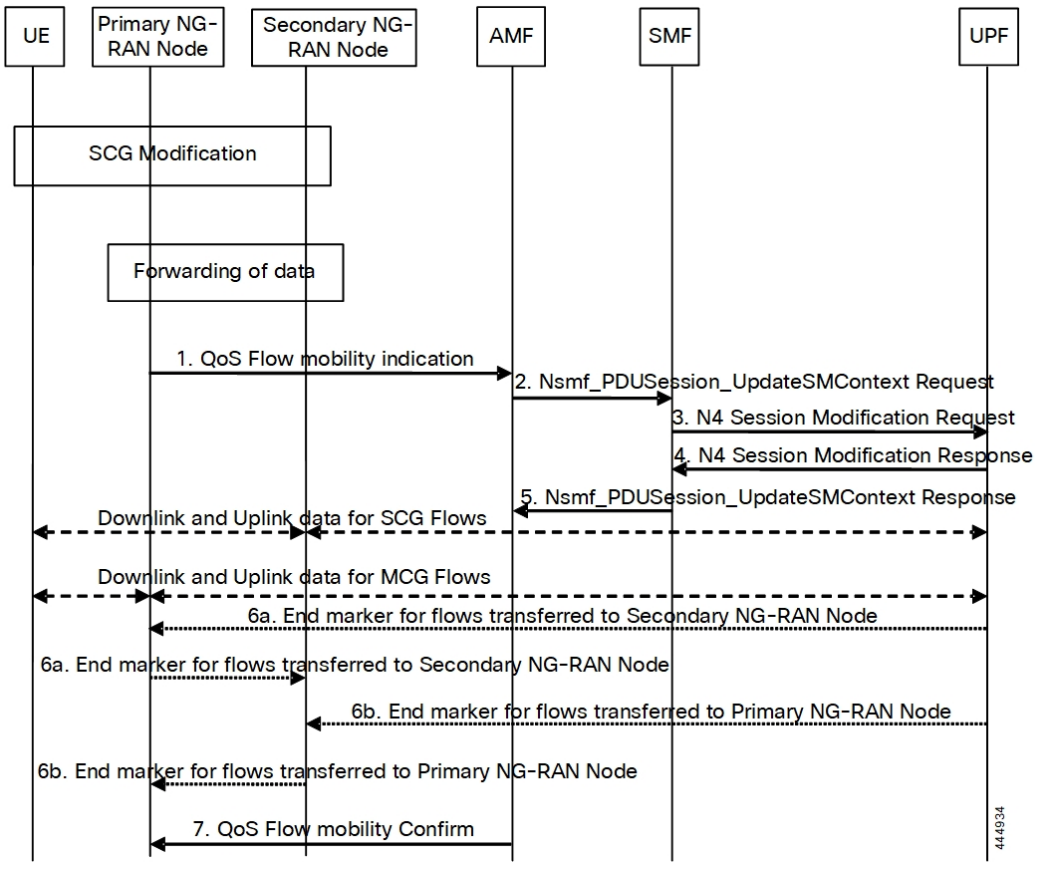
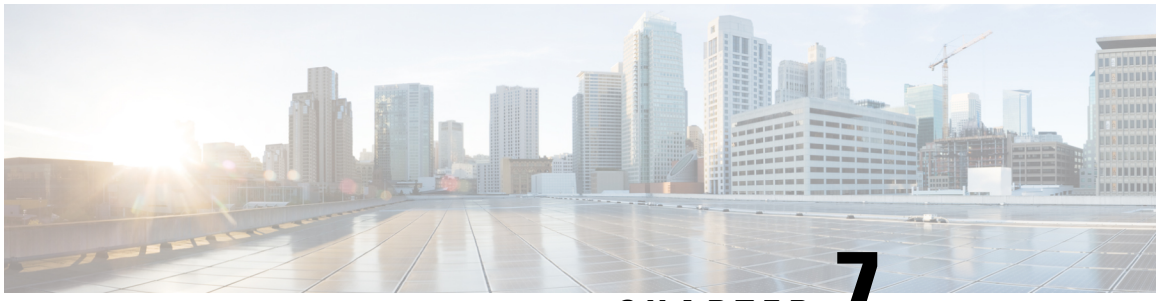


Table 15: NG-RAN initiated QoS Flow Mobility Call Flow Description

Step	Description
1.	The primary RAN node sends a N2 QoS Flow mobility indication message to the AMF. The QoS flow pertains to the Master Cell Group (MCG) and Secondary Cell Group (SCG). The indication message includes PDU session ID, QFIs, and AN tunnel information. The tunnel information includes the new RAN tunnel endpoint for the QFIs.
2.	AMF sends Nsmf PDU Session Update SM Context request to SMF. This request message includes N2 QoS flow mobility indication message and PDU session ID.
3.	The SMF sends an N4 Session Modification Request message to the UPF. This Modification Request includes PDU session IDs, QFIs, and AN tunnel information for downlink user plane.
4.	The UPF switches the requested QFIs, and then sends an N4 Session Modification Response message to the SMF. The response message includes CN tunnel information for uplink traffic. **Important** Step 7 can occur anytime after receipt of N4 Session Modification Response at the SMF.
5.	SMF sends Nsmf PDU Session Update SM Context response to AMF for QFIs of the PDU session which have been switched successfully. If none of the requested QFIs are switched successfully, the SMF sends an N2 QoS flow mobility failure message.
6.	To assist the reordering function in the Primary RAN node and/or Secondary RAN node, for each affected N3 tunnel, the UPF sends one or more "end marker" packets on the old tunnel immediately after switching the tunnel for the QFI. The UPF starts sending downlink packets to the target NG-RAN.
7.	The AMF sends an acknowledgement message to the primary RAN node. This message indicates the completion of QoS flow mobility procedure.



CHAPTER 7

Cisco Common Data Layer

- Feature Summary and Revision History, on page 75
- Feature Description, on page 76
- How it Works, on page 77
- Call Flows, on page 77
- Configuring the CDL Through SMF Ops Center, on page 79
- Configuring Event Trace Data, on page 81

Feature Summary and Revision History

Summary Data

Table 16: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 17: Revision History

Revision Details	Release
Added the failure handling support.	2023.03.0
Added the procedures for configuration and verification of the event trace data in the CDL database record.	2021.02.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF extends support to the Geo Redundant (GR) version of the Cisco Common Data Layer (CDL). When the primary CDL endpoint fails, the SMF attempts the same operation on the next highly rated secondary endpoint thus providing a non-disrupted N7 or Diameter message handling. If the next rated endpoint is unavailable, then the SMF reattempts the operation on the subsequent endpoint that has the highest rating and so on.

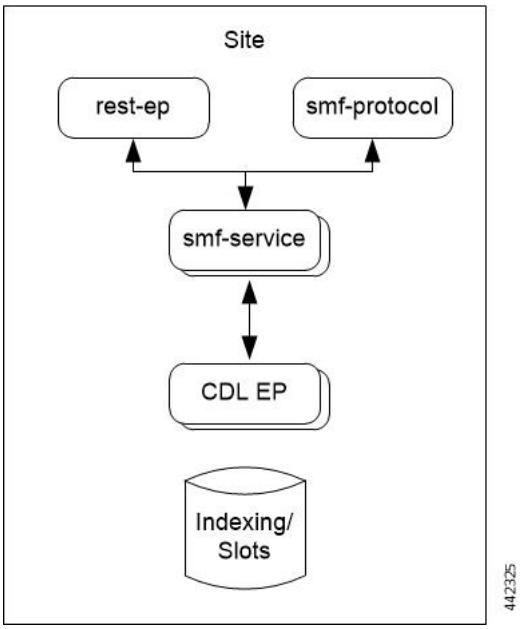
In case of specific errors or failures from CDL to SMF, the retry mechanism is used for the Create, Find, and Delete requests as well along with the earlier supported Update requests. The number of retries are as per the SLA.

When the SMF receives the successful response during the retries, then the retries are stopped and the response is sent to the application.

Architecture

The following figure depicts the failover that happens when the SMF service is unable to access the CDL datastore endpoint.

Figure 16: CDL Datastore Architecture



With relevance to this architecture, you can configure CDL through SMF Ops Center. When the SMF connects to the CDL, it uses the local endpoints.

How it Works

When CDL is configured in SMF through the SMF Ops Center, SMF gets enabled to support multiple CDL datastore endpoints. You can configure the endpoints by specifying the IP addresses, ports, and assigning ratings to each endpoint. By default, SMF considers the local endpoint as the primary endpoint, which has the maximum rating. SMF performs CDL API operations on the primary endpoint. If this endpoint is unavailable, then SMF routes the operations to the next maximum rated endpoint. SMF keeps failing over to the accessible secondary endpoint or until all the configured secondaries are exhausted. It does not reattempt a query on the next rated endpoint if the endpoint is reachable but responds with error or timeout.

If SMF is unable to access any of the endpoints in the cluster, then CDL operation fails with the "Datastore Unavailable" error.

The following table lists the scenarios, expected behavior, and the related error responses from CDL.

Table 18: Scenarios, Expected Behavior, and Error Responses from CDL

Scenario	Expected Behavior	Error Response from CDL
All pods are active and healthy and trigger the CDL operations.	CDL Create, Read, Update, Delete (CRUD) operations are not retried.	Not applicable
CDL endpoint pod restarts and triggers CDL operations.	CDL CRUD operations are retried.	CDL sends the following error responses with the error code: • ERROR_FROM_INDEXING [501] • ERROR_FROM_SLOT [502] • DATASTORE_EP_QUEUE_FULL [503] • MAX_CAPACITY_REACHED [507

Call Flows

This section describes the call flow that is associated with this feature.

• CDL Endpoint Failure Call Flow, on page 77

CDL Endpoint Failure Call Flow

This section describes the SMF local data store endpoint failure call flow.

Figure 17: CDL Endpoint Failure Call Flow

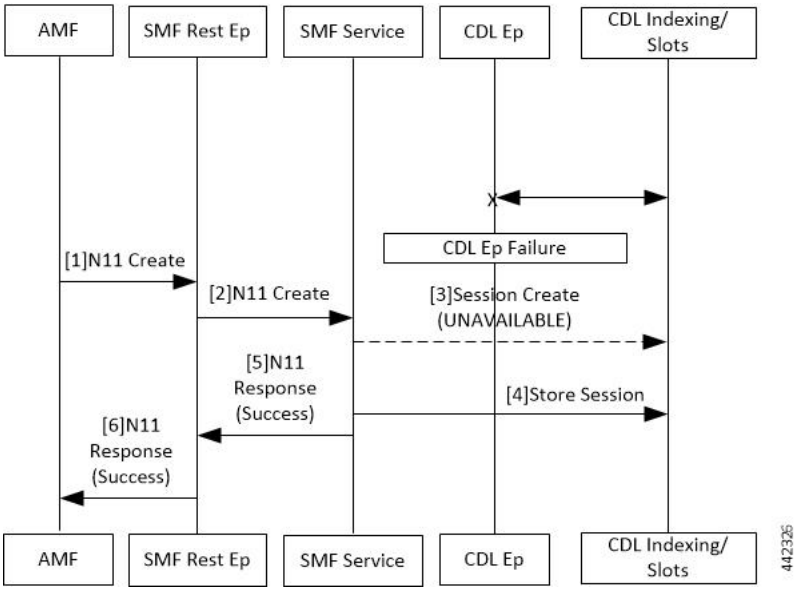


Table 19: CDL Endpoint Failure Call Flow Description

Step	Description
1	The AMF sends a Create Request to SMF REST endpoint over the N11 interface.
2	After receiving the request, the SMF REST endpoint forwards the Create Request to the SMF service.
3	The SMF service attempts to reach the CDL endpoint to send the session creation request. However, the CDL endpoint is unreachable.
4	The Create Request is evaluated in the stored session and the SMF service forwards the request to the CDL endpoint.
5	After the call request is successful, the SMF service notifies the Success Message to the SMF REST endpoint.
6	The SMF REST endpoint forwards the Success Message to the AMF.

Limitations

The CDL configuration in SMF has the following limitations:

- The SMF service attempts to reroute the calls only when it encounters gRPC errors, such as UNAVAILABLE. It does not acknowledge errors that the datastore endpoint returns and actual gRPC timeouts, such as DEADLINE_EXCEEDED gRPC status code.
- The SMF service does not resolve failures occurring with the datastore such as indexing and slot failures. The CDL layer must resolve these failures and if necessary, send an API call on the remote.
- By default, the maximum retry limit for a request is three. After reaching this limit, the retry is stopped and the response is sent to the application.

- On receiving the response message as success during the retries, the further retry is stopped and the response is sent to the application.

Configuring the CDL Through SMF Ops Center

The configuration of the CDL using SMF Ops Center involves the following steps:

1. Configuring the CDL Session Database and Defining the Base Configuration, on page 79
2. Configuring the Zookeeper in CDL, on page 80

Configuring the CDL Session Database and Defining the Base Configuration

Use the following sample configuration to configure the CDL session database and define the base configuration in SMF:

```
config
   cdl system-id system_id
   cdl node-type node_type
   cdl zookeeper replica zookeeper_replica_id
   exit
   cdl logging default-log-level debug_level
   cdl datastore session
      cluster-id cluster_id
      endpoint replica 1
      endpoint replica num_replica
      index map map_value
      slot replica num_replica
      slot map num_map/shards
      slot write-factor write_factor
      slot notification host host
      slot notification port port
      slot notification limit tps
      index replica num_replica
      index map num_map/shards
      index write-factor write_factor
      slice-names cdl_slice_name
      end
```

NOTES:

- **cdl system-id** *system_id*: This is an optional command. Specifies the system or Kubernetes cluster identity. The default value is 1.
- **cdl node-type** *node_type*: This is an optional command. Specifies the Kubernetes node label to configure the node affinity. The default value is “session.” Accepted length of the value is 0–64 alphabets.
- **cdl zookeeper replica** *zookeeper_replica_id*: Specifies the zookeeper replica server's ID.
- **endpoint replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. Must be an integer in the range of 1–16.

- **slot replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. num_replica must be an integer in the range of 1–16.
- **slot map** *num_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024.
- **slot write-factor** *write_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16. Make sure that the value is lower than or equal to the number of replicas.
- **slot notification host** *host*: This is an optional command. Specifies the notification server hostname or IP address. The default value is datastore-notification-ep.
- **slot notification port** *port*: This is an optional command. Specifies the notification server Port number. The default value is 8890.
- **slot notification limit** *tps*: This is an optional command. Specifies the notification limit per second. The default value is 2000.
- **index replica** *num_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 2. num_replica must be an integer in the range of 1–16.
- **index map** *num_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. num_map/shards must be an integer in the range of 1–1024. Avoid modifying this value after deploying the CDL.
- **index write-factor** *write_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. write_factor must be an integer in the range of 0–16.
- **slice-names** *cdl_slice_name*: Specify the CDL slice names. *cdl_slice_name* must be an alphanumeric string from 1 to 16 characters in length.

Configuring the Zookeeper in CDL

Use the following sample configuration to define the Zookeeper in CDL:

```
config
  cdl zookeeper data-storage-size data_storage_size_in_gb
    log-storage-size log_storage_size_in_gb
    replica number_of_replicas
    enable-JMX-metrics boolean_value
    enable-persistence boolean_value
    end
```

NOTES:

All the following parameters are optional.

- **cdl zookeeper data-storage-size** *data_storage_size_in_gb*: Specifies the size of the Zookeeper data storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.
- **log-storage-size** *log_storage_size_in_gb*: Specifies the size of the Zookeeper data log's storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.

- **replica** *num_replicas*: Specifies the number of replicas that must be created. The default value is 3. Accepted value is an integer in the range of one to 16.
- **enable-JMX-metrics** *boolean_value*: Specifies the status of the JMX metrics. The default value is true.
- **enable-persistence** *boolean_value*: Specifies the status of the persistent storage for Zookeeper data. The default value is *false*.

Sample Configuration

This section shows a sample configuration of CDL in a HA environment.

```
config
cdl system-id system_id
cdl zookeeper replica num_zk_replica
cdl datastore session
 endpoint replica ep_replica
 index map index_shard_count
 slot replica slot_replica
 slot map slot_shard_count
 slice-names cdl_slice_name
exit
```

Configuring Event Trace Data

This section describes how to configure the SMF to store event trace data in CDL database record. With this configuration, the SMF allows to enable or disable the storage of event trace data in the CDL database record. The event trace data shows the call flow event for the subscribers.

Note Configuring the event trace to disabled saves approximately 1 KB of database storage for each SMF database record.

To enable or disable the storage of event trace data in the CDL database record, use the following sample configuration:

```
config
   system-diagnostics event-trace [ enable | disable ]
      end
```

NOTES:

- **system-diagnostics event-trace [enable | disable]**: Enable or disable the storage of event trace data in the CDL database record for system diagnostics.

Verifying Event Trace Data

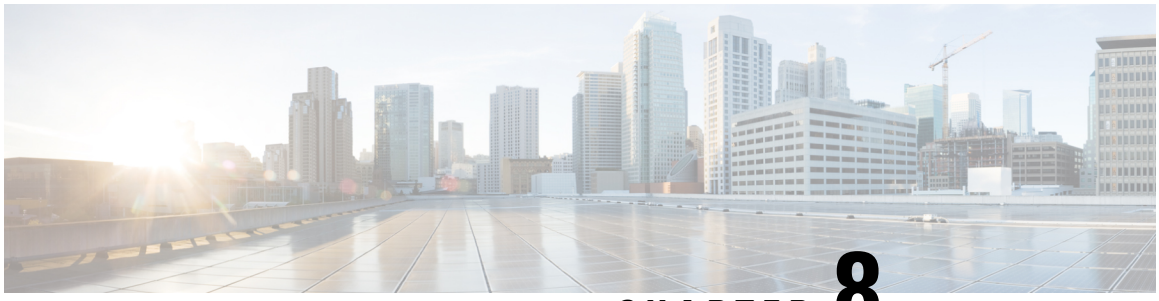
This section describes how to verify the event trace data in SMF.

Use the show running-config command system-diagnostics event-trace CLI command to view if the event trace data is enabled or disabled.

The following is a sample output of the show running-config system-diagnostics event-trace CLI command.

show running-config system-diagnostics event-trace

```
system-diagnostics event-trace enabled
```



CHAPTER 8

Content Filtering and X-Header Enrichment

- Feature Summary and Revision History, on page 83
- Feature Description, on page 83
- Content Filtering, on page 84
- X-Header Insertion, on page 85

Feature Summary and Revision History

Summary Data

Table 20: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 21: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the following functionality:

- Content Filtering
- X-header Enrichment

Content Filtering

Feature Description

The Content Filtering (CF) service prevents subscribers from inadvertently getting exposed to universally unacceptable content, or content that is inappropriate as per subscriber preferences. Based on the URLs in the subscriber requests, the CF service filters HTTP and WAP requests from mobile subscribers. Operators can filter and control the content for an individual subscriber to access.

Configuring Content Filtering

This section describes how to configure CF support.

Note Apart from the following configurations, all other configurations are used only in the UPF, and SMF sends it to the UPF. The SMF doesn't use these configurations. For more information on how to enable the feature on UPF, see the *UCC 5G UPF Configuration and Administration Guide*.

Configuring Content Filtering under Active Charging Service

To configure CF under the active charging service, use the following sample configuration:

```
config
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
      end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

Configuring Content Filtering under Rulebase

To configure CF under the rulebase, use the following sample configuration:

```
config
   active-charging service service_name
      rulebase rulebase_name
         content-filtering category policy-id cf_policy_id
         end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

Configuring Content Filtering under APN

To configure CF under the APN, use the following sample configuration:

```
config
   apn apn_name
      content-filtering category policy-id cf_policy_id
      end
```

NOTES:

- **content-filtering category policy-id** *cf_policy_id*: Specify the CF policy number. *cf_policy_id* must be an integer in the range of 1-4294967295.

Content Filtering Policy ID on N7 Interface

The CF categories are configured under the active charging service under specific policy IDs. The rulebase and APN also have an associated policy ID. For any session, one policy ID can be associated with the session at anytime. The categories configured under that CF policy ID are applicable for the session on the UPF.

The PCF can override the CF policy ID by sending this value on the N7 interface. For this purpose, a proprietary IE is available in the YAML definition for the N7 interface. The hierarchy for the CF policy ID is as follows:

```
smPolicyDecision
   ciscoAvpSet:
      cfPolicyId: uint32 value
```

When the PCF does not send a CF policy ID, the existing CF policy ID in the rulebase configuration or the policy ID configured in the APN configuration is selected, in the order of precedence. This CF policy ID value is sent to the UPF in PFCP Session Establishment Request message in the "Subscriber Parameters" attribute. During PDU Session Modification, if the PCF changes the CF policy ID, the ID is sent to the UPF in PFCP Session Modification Request message.

X-Header Insertion

With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on).

Supported X-Header Information

Out of all the configurable X-header information, some information requires SMF to send the corresponding values to the UPF. The following table lists the information that is sent from the SMF to the UPF for X-header insertion.

Table 22: X-header Information

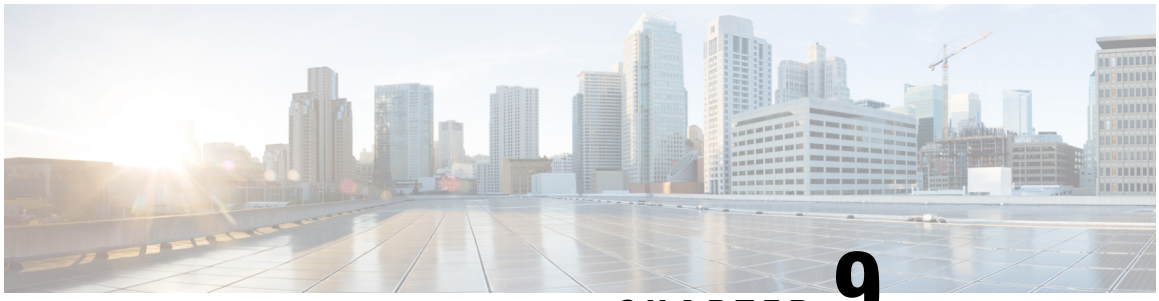
Xheader Field	Description	Present in Session Establishment	Modified in Session Modification
String Constant	Inserts the configured string in xheader	—	—
Charging ID	Per Flow or Bearer Charging Id	Yes	—
IMEI	IMEI for the call	Yes	—
IMSI	IMSI for the call	Yes	—
Rat-Type	RAT type for the UE session	Yes	Yes
s-mcc-mnc	MCC or MNC of the SGW or AMF	Yes	—
Sgsn-address	AMF or SGW address	Yes	Yes
ULI	User Location Info	Yes	Yes
GGSN-Address	N4 or or S5 endpoint of SMF	Yes	Yes
Radius-station-ID	MSISDN of the UE	—	—
Sn-rulebase	Rulebase for a call	Yes	Yes
Subscriber-ip-address	IP address allocated to UE	—	—
Msisdn-no-cc	Obtained from MSISDN	Yes	No

The subscriber-specific fields—IMSI, MSIDN, and IMEI—are encoded in the "User ID" standard IE. For more details, see 3GPP 29.244, Section 8.2.101.

Rest of the fields are sent in the "Subscriber Parameters" proprietary AVP. Some fields, such as the "Rulebase" and "UE IP address", are sent as a part of the created PDRs.

Note

- All the parameters are always sent from the SMF to the UPF irrespective of whether X-header configuration is available. These parameters ensure that any change in configuration after session creation is immediately applied on the UPF.
- The SMF supports X-header insertion-related configurations. The SMF does not require these configurations for its functionality. These configurations are sent to the UPF.



CHAPTER 9

Diameter Endpoint

- Feature Summary and Revision History, on page 87
- Feature Description, on page 88
- How it Works, on page 93
- Configuring Diameter Endpoint, on page 93
- Dynamic Configuration Change, on page 104
- Destination Host AVP for CCR and Retried Messages, on page 105
- Peer Management, on page 106
- Failure Handling, on page 113
- OAM Support, on page 118
- Troubleshooting Information, on page 127

Feature Summary and Revision History

Summary Data

Table 23: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 24: Revision History

Revision Details	Release
Added the following support: • Gx and Gy custom dictionary support for RAR messages • DWR and DWA handling • Bounded peer	2023.04.0
First introduced.	2023.03.0

Feature Description

The Diameter Endpoint is an App-infra-based service that enables the Diameter functionality for the SMF service. In SMF, Diameter Endpoint implements the Gx and Gy clients. The Diameter endpoint leverages the Ops Center for configuration, operational, and action CLI commands and App-infra features, such as interpod communications, RPCs, Monitor Subscriber, Monitor Protocol, logging, and statistics.

The Diameter Endpoint provides the following support:

- Diameter peer and connection management for both the Gx and Gy interfaces.
- Failure handling templates for the configuration of failure handling and retry behavior for the Diameter messages.
- Ability to peer to multiple Diameter routing agents (DRA) and route the Diameter messages to remote Diameter endpoints through the DRAs.

Note The Diameter stack doesn't implement the ability to act as a DRA.

- Monitor Protocol and Monitor Subscriber (SUPI and IMSI subscriber key) for Diameter messages.
- Logging and statistics.

To use a Diameter endpoint, deploy a pair of Diameter pods with an Active or Standby configuration for each interface, which is Gx and Gy. Deploy these pods in the host networking configuration with a pair of internal and external VIPs.

For online charging, the Diameter Credit Control application is used. The online client, Charging Transfer Function (CTF), requests resource allocation and reports credit control information to the Online Charging System (OCS). To support Credit Control through Diameter, the CCR (Credit Control Request) and the CCA (Credit Control Answer) messages are used.

Service pod sends the gRPC messages to the Diameter endpoint for Credit Control messages. The Diameter endpoint converts the Diameter CCR messages and sends them to Gx and Gy servers, which are PCRF or

OCS. After receiving the CCA, the CCA message is converted to the gRPC message and sent to the SMF as a response.

Supported Interfaces

SMF supports the following interfaces:

- Gx interface
- Gy interface

For the features related to the Gx and Gy interfaces, see the Interfaces Support chapter.

Important It should not be assumed that the Diameter interface features available on the SMF have full feature parity and functionality with StarOS or CUPS product. Furthermore, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with StarOS legacy or CUPS products.

Please contact your Cisco Account or Support representative for any questions about parity between this product and any StarOS legacy or CUPS products.

Diameter Endpoint Instance

A Diameter endpoint instance is used to configure the Diameter endpoints for different interfaces, such as Gx and Gy. This configuration determines the number of Diameter endpoint pods to be deployed. Configuring a Diameter endpoint instance is mandatory.

Diameter Client Profile

A Diameter client is a Diameter node that supports Diameter client applications and the base protocol. A Diameter client is implemented in the devices that are placed at the edge of a network and provides access control services for that network.

A Diameter profile provides network access information for the Diameter application. Each Diameter client profile is associated with an existing endpoint profile and with a failure handling template by its name. SMF uses the client profile name to allow the Diameter endpoint fetch the associated endpoint profile. SMF uses this profile to evaluate the matching endpoint to send the messages.

For encoding Credit Control Requests (CCR) and decoding of the corresponding responses, Credit Control Answer (CCA) messages, you have to configure a dictionary in the Diameter client profile. A dictionary includes the list of AVPs with their descriptions that are used in the CCR and CCA messages, with the standard AVPs or vendor-specific AVPs.

Diameter Endpoint Profile

A Diameter endpoint profile provides the following information:

- Origin configuration, such as the origin realm, origin host name, origin state ID, and origin address.

For the origin state ID, the SMF provides the Diameter endpoint-originated OSI support for the Credit Control Request (CCR) or Device Watchdog Request (DWR) messages. You can enable or disable the dynamic OSI value through Ops Center using the **dynamic-origin-state-id** CLI command. The Nodemgr updates the OSI value in the cache pod. Then, the Diameter endpoint uses this value to send the Capability Exchange Request (CER), CCR, and DWR messages.

- Peer configuration, such as the peer realm, destination host name, peer IP, and peer port.
- Global parameters, such as destination host AVP, VSA support, and maximum outstanding messages.
- Timeout duration.

You can configure the Diameter endpoint profiles for each interface. These profiles are provisioned to the Diameter endpoint pods corresponding to the interface. Then, these profiles are associated with a specific Diameter client profile.

Note Configure the Diameter endpoint profile for the Diameter pods deployment.

Disconnect Peer Request Management

This section describes about the Disconnect Peer Request (DPR), Disconnect Peer Answer (DPA), and its related CLI commands to configure the DPR and DPA in the Diameter endpoint.

Feature Description

The SMF supports the DPR and it handles the received DPR from server. The DPR is sent to a peer to inform its intentions to shut down the transport connection. When the peer node sends the DPR to another node, the node validates the DPR for all required AVPs. If the validation isn't successful, the node sends the DPA with the error to the peer node.

If the validation is successful:

- The SMF node waits till the drain time before it sends any DPA to the peer node. DrainTime is the time interval between receiving a DPR by diameter endpoint and sending a DPA response. No new requests are initiated by the diameter-ep to the peer during this interval. However any messages received from the peer are processed during this interval. Drain time is a configurable parameter. It's recommended to configure the drain time value less than the timeout value for inbound messages. It's advised that no new request to be sent to that peer during this time, but in case any requests comes from the peer, it must be responded.
- Regardless of whether any messages have previously been forwarded to the client and are waiting for a response, transmit DPA successfully. The peer node sends the DPA with success.

If a server wants to disconnect itself from a peer SMF node, it sends DPR with disconnect cause AVP.

- If disconnect cause is REBOOTING, defer connecting back based on Tc Timer. Tc timer is a configurable parameter.
  - The Reboot time is the time duration after which connection is reattempted to peer from which DPR is received with disconnect cause "REBOOTING". This interval starts after sending the DPA response and connection teardown.

- If the disconnect cause is BUSY or DO_NOT_WANT_TO_TALK_TO_YOU, defer connecting back for longer duration. Duration is a configurable parameter. As it's recommended not to connect back in case of BUSY or DO_NOT_WANT_TO_TALK_TO_YOU. So, you can configure negative or zero as value to never connect back.
  - DoNotTalkTime is the time duration after which connection is reattempted to peer from which DPR is received with disconnect cause "DO_NOT_WANT_TO_TALK_TO_YOU". This interval starts after sending the DPA response and connection teardown.
  - BusyTime is the time duration after which the connection is reattempted to peer from which DPR is received with disconnect cause "BUSY". This interval starts after sending the DPA response and connection teardown.
- The time duration for reconnecting back is applicable across all pod restarts or pod failover but doesn't apply to site failover.

DWR and DWA Handling

Feature Description

Diameter endpoint handles the incoming Device Watchdog Request (DWR) from a peer and responds with a Device Watchdog Answer (DWA) with the success result code. The Diameter endpoint also supports detection of the peer having an issue or transport failure on an idle connection by sending the DWR messages.

How it Works

To send a DWR to a peer, the Diameter endpoint uses the app-infra provided host monitoring to check if DWR needs to be generated.

On each host monitoring check, the Diameter endpoint checks for any message exchanges happened between the last check and now. When there's both a request and response for a message, then Diameter endpoint considers it a message exchange. A message exchange isn't considered in the following scenarios:

- If the Diameter endpoint sends a request but receives no response from a peer.
- If the Diameter endpoint received the request but failed to send the response to the peer.

If no message exchange happens between the Diameter endpoint and peer, then Diameter endpoint generates a DWR toward peer. The Diameter endpoint considers the following scenarios as the DWR failure:

- If sending the DWR fails.
- If no DWA is received in the time configured in the **basemsg retransmission-timeout** parameter.
- If there's a response but with a failure result code.

In the case of DWR failure, a retry occurs if the **basemsg retransmissions** parameter value is configured to a nonzero value. The retry is performed in the next host monitoring check. During retries, if the Diameter endpoints received a DWA for any of the earlier sent DWR, then the Diameter endpoint ignores it and doesn't consider it toward the successful DWR.

Even after the configured retries, if the DWR isn't successful then the status is reported as a failure, and the connection is reset. After the connection is reset only during the next host monitoring check, the connection is reestablished. Then, the Capability Exchange Request (CER) and DWR are sent. However, the Diameter

endpoint sends no messages to the peer if DWR or DWA isn't successful. In the case of DWR or DWA failure, the connection is reset.

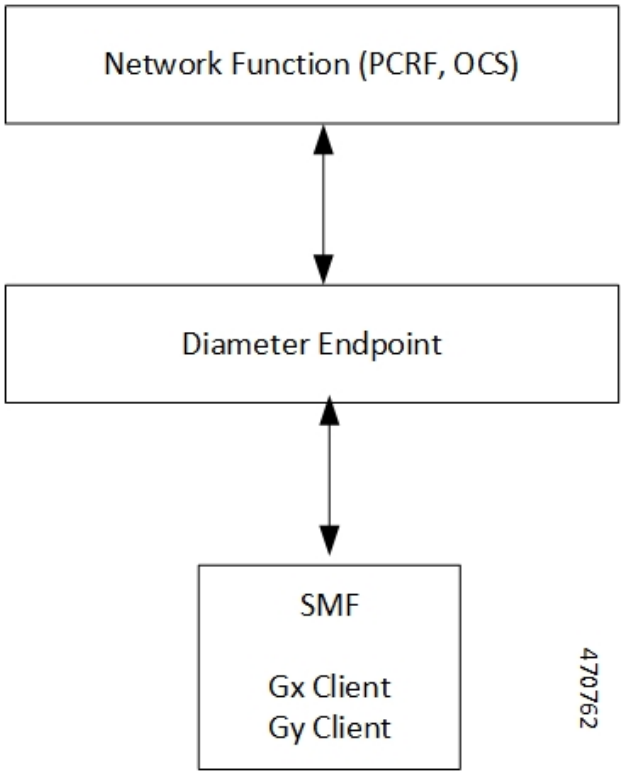
Note While the host monitoring for all hosts is performed in parallel, the monitoring completes after it's completed for all the hosts. Delay in monitoring for one host leads to delay in next monitoring for all the hosts.

Architecture

Diameter common stack, which is the Diameter endpoint, is an interface between the NFs and both client and server modes for a supported application.

The following diagram shows the architecture of the common Diameter stack.

Figure 18: Common Diameter stack



The common Diameter stack includes the following components:

- Network Functions—Policy and Charging Rules Function (PCRF) and Online Charging System (OCS)
- Diameter Endpoint
- Diameter interfaces on SMF—Gx and Gy clients

For more information on the supported Diameter interfaces and their related features, see the *Interfaces Support* chapter.

How it Works

The Diameter endpoint uses the App-infra framework for sending or receiving the Diameter messages to the Diameter peers and internal IPC messages to other pods. For example, P-GW service, cnBNG service. In SMF, the Diameter endpoint implements the Gx and Gy clients.

To support Credit Control through the Diameter, the two Diameter messages—Credit Control Request (CCR) and the Credit Control Answer (CCA) are used. A service pod sends the gRPC messages to the Diameter endpoint for conversion of the gRPC messages to the Credit Control messages. Then, the Diameter endpoint sends the CCR messages to the Gx or Gy servers, which are PCRF or OCS. After the Gx or Gy server sends the CCA message, the Diameter endpoint converts the CCA message to the gRPC message and sends it to the P-GW service as a response.

The Diameter supports the standard AVPs, as per the *3GPP 29.212 version 15.3.0* and *3GPP 32.299 version 12.9.0* specifications for the Gx and Gy interfaces.

Standards Compliance

The Diameter endpoint complies with the following standards:

- *3GPP 29.212 version 15.3.0*
- *3GPP 32.299 version 12.9.0*

Limitations

The Diameter endpoint has the following limitation:

- The Diameter endpoint supports only one pair of pods for each interface.

Configuring Diameter Endpoint

The configuration of the Diameter endpoint includes the following steps:

1. Configuring Diameter Endpoint Instances, on page 93
2. Configuring Diameter Client Profile, on page 95
3. Configuring Diameter Profile Endpoint on the Gx and Gy Interfaces, on page 96

Configuring Diameter Endpoint Instances

To configure the Diameter endpoint instances, use the following sample configuration:

```
config
  instance instance-id instance-id
    endpoint diameter
    interface interface_name
      internal-vip ip_address
```

```
      vip-ip ip_address
      mode mode_value
    exit
```

NOTES:

- **instance instance-id** *instance-id* **endpoint diameter** : Specify the number of Diameter endpoint pods to be deployed.
- **interface** *interface_name*: Specify the interface, such as Gx and Gy, for the Diameter endpoints.
- **internal-vip** *ip_address*: Specify the internal VIP IP address for the Diameter endpoint to listen for requests from the service. **internal-vip** is a mandatory parameter.
- **vip-ip** *ip_address*: Specify the VIP IPv4 address for the corresponding to the Diameter clients. **vip-ip** is a mandatory parameter.
- **mode** *mode_value*: Specify the Diameter endpoints with a specific mode. **mode** is a mandatory parameter.

Note SMF supports only the *client* as *mode_value*.

Configuration Example

The following is an example configuration of Diameter endpoint instances.

```
instance instance-id 1
endpoint diameter
  interface gy
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
   exit
  exit
  interface gx
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
  exit
```

Configuration Verification

To verify if the Diameter endpoint instances are configured, use the following **show running-config instance instance-id** *instance_id* **endpoint diameter** command.

```
smf# show running-config instance instance-id 1 endpoint diameter
instance instance-id 1
endpoint diameter
  interface gy
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
   exit
  exit
  interface gx
   internal-vip 209.165.200.234
   vip-ip 209.165.200.234
   mode client
  exit
```

Configuring Diameter Client Profile

Table 25: Feature History

Feature Name	Release Information	Description
Same dictionary support extended to RAR messages.	2023.04	In the previous releases, for CCR-I, CCA-U, and CCA-T messages, the dictionary specified under the client, which is a custom dictionary, was applied. For RAR message, a common dictionary was being used. With this release, RAR messages also use the same dictionary that CCR-I, CCA-U, and CCA-T messages use.

To configure the Diameter client profile, use the following sample configuration:

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint_profile_name
    failure-handling-profile profile_name
    dictionary-name { dcca-custom8 | default | r8-gx-standard }
    end
```

NOTES:

- **profile diameter-client** *diameter_client_name*: Specify a Diameter client profile name.
- **endpoint** *endpoint_profile_name*: Specify an existing endpoint profile name to associate it with a Diameter client profile. You can define a maximum of 100 client profiles.
- **failure-handling-profile** *profile_name*: Specify an existing failure handling profile to associate it with a Diameter client profile.
- **dictionary-name { dcca-custom8 | default | r8-gx-standard }**: Specify one of the following dictionaries:
  - **dcca-custom8**: This dictionary is the standard Gy dictionary.
  - **default**: This dictionary is the default dictionary.
  - **r8-gx-standard**: This dictionary is the standard Gx dictionary.

Note The specified dictionary is used for Credit Control - Initial (CCR-I), Credit Control - Update (CCR-U), Credit Control - Terminate (CCR-T), and Re-Authorization Request (RAR) messages.

Configuration Example

The following is an example configuration of the Diameter client profile.

```
profile diameter-client gydc01
    endpoint gxProf1
    failure-handling-profile fh1
    exit
```

Configuration Verification

To verify if the Diameter client profile is configured, use the following **show running-config profile diameter-client** command:

```
[smf] smf# show running-config profile diameter-client
profile diameter-client gydc01 endpoint gxProf1 failure-handling-profile fh1 dictionary-name
 kt-gy
exit
profile diameter-client gydc11 endpoint gyProf1 failure-handling-profile fh2
exit
profile diameter-client gydc12 endpoint gyProf2 failure-handling-profile fh3
exit
profile diameter-client gxdc02 endpoint gxProf1 failure-handling-profile fh4
exit
```

Configuring Diameter Profile Endpoint on the Gx and Gy Interfaces

Table 26: Feature History

Feature Name	Release Information	Description
VRF support for the Diameter Gx and Gy interfaces	2023.04	SMF supports the client-side VRF for the Diameter Gx and Gy interfaces. The profile Diameter endpoint refers to the VRF name and interface name that you configure from the Diameter endpoint. The Diameter endpoint uses the VRF name to create a TCP connection from the Diameter client.

To configure the Diameter profile endpoint on the Gx and Gy interfaces, use the following sample configuration:

```
config
  profile diameter-endpoint interface_name
    name profile_name
    internal-vip ip_address
      destination-host-avp message_type
      vsa-support vendorId-source
      max-outstanding number_of_messages
      response-timeout response_timeout_value
      connection-timeout connection-timeout_value
      basemsg retransmission-timeout retransmission_timeout_value
      basemsg retransmissions max_retry_value
      basemsg watchdog-interval interval_value
      dscp [ dscp_value | af11 | af12 | af13 | af21 | af22 | af23 | af31
| af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 |
```

```
cs6 | cs7 | ef ]
        origin realm realm_name
        origin host host_name address ipv4 ip_address
        origin peer origin_peer_name
        realm  realm_name
        address ipv4 ip_address
        address vrf vrf_name
        port peer_port
        destination-host-name  destination_host_name
        load-balancing-algorithm highest-weight
        route-entry host [ host-name | * ] realm [ realm-name | * ] peer
peer_name weight weight_value
        route-failure deadtime deadtime_value result-code result_code_value
threshold  number
        route-failure result-code result_codes_value
        route-failure threshold  threshold_number
       route-failure recovery-threshold percent  recovery_threshold_percentage

        dynamic-route expiry-timeout  expiry_timeout_value
        dynamic-origin-state-id  boolean_value
        exit
```

NOTES:

- **profile diameter-endpoint** *interface_name*: Specify a Diameter profile for the Gx or Gy interface.
- **name** *profile_name*: Specify the profile name of the Diameter profile interface. Each profile configures the Diameter source information and the peer information for the Diameter messages that go toward those peers.

Note You can define a maximum of 100 profiles per interface.

- **internal-vip** *ip_address*: Specify an internal VIP IP address for communication with service pods. **internal-vip** is a mandatory parameter.
- **destination-host-avp** *message_type*: Specify the type of message in which the destination host AVP is to be encoded.

Note SMF supports only the *always* value for the *message_type*.

- **vsa-support** *vendorId-source*: Specify the source of vendor IDs DIABASE to be used for negotiation of Diameter peer capabilities.

Note SMF supports only the *all-from-dictionary* value for the *vendorId-source*.

- **max-outstanding** *number_of_messages*: Specify the maximum number of Diameter messages to be sent to any peer in the profile, while awaiting the responses. The default value is 256. *number_of_messages* must be in the range of 1–4096.
- **response-timeout** *response_timeout_value*: Specify the maximum allowed response time for request messages that the Diameter applications send to the Diameter server. The default value is 60. *response_timeout_value* must be in the range of 1–300.
- **connection-timeout** *connection-timeout_value*: Specify the maximum allowed time for establishing the transport layer connectivity, such as the TCP connection, toward the Diameter server. The default value is 30. *connection-timeout_value* must be in the range of 1–300.
- **basemsg retransmission-timeout** *retransmission_timeout_value*: Specify the timeout value between retransmissions of the base messages, such as Device Watchdog Request (DWR) and Capability Exchange Request (CER), toward the Diameter server. The default value is 30. *retransmission_timeout_value* must be in the range of 1–120.
- **basemsg retransmissions** *max-retries*: Specify the maximum number of times the base messages must be retransmitted. The default value is 1. *max-retries* must be in the range of 1–10.
- **basemsg watchdog-interval** *interval_value*: Specify the minimum time interval between the two DWR messages that are sent toward the Diameter server. The default value is 5. *interval_value* must be in the range of 5–30.
- **dscp [** *dscp_value* **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef]** : Specify the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages that are sent toward the Diameter server. The default value is **be**. *dscp_value* must be in the range of 0–63. Choose in the following other DSCP values, as required:
  - **af**xx: Specify this value for the use of an assured forwarding xx per hop behavior (PHB).
  - **be**: Specify this value for the use of the best effort forwarding PHB. **be** is the default value.
  - **cs**x: Specify this value for the use of class selector x per PHB.
  - **ef**: Specify this value for the use of expedited forwarding PHB.
- **origin realm** *realm_name*: Specify the name of the realm for the Diameter endpoint. This parameter is mandatory.
- **origin host** *host_name* **address ipv4** *ip_address* : Specify the host name, which is the FQDN of the Diameter endpoint. Specify the IPv4 address, which is the Diameter endpoint Bind IP address for the Diameter client connections.
- **origin peer** *origin_peer_name* : Specify the identifier for a Diameter peer. This parameter is mandatory.

Note You can configure a maximum of 5000 peers.

- **realm** *realm_name*: Specify the name of the realm for a peer with the name of the peer. This parameter is mandatory.
- **address ipv4** *ip_address*: Specify the IP address of the Diameter peer.
- **address vrf** *vrf_name*: Specify the VRF name that is to be referenced from the Diameter endpoint.

- **port** *peer_port*: Specify the port of the Diameter peer. This parameter is mandatory.
- **destination-host-name** *destination_host_name*: Specify the custom destination host name to be used in destination host AVP. This parameter is optional.
- **load-balancing-algorithm highest-weight** : Choose an idle server with the highest weight in failure scenarios. If multiple servers have the same high weight, then the load balancing happens among those servers.
- **route-entry host [host-name | *] realm [realm-name | *] peer** *peer_name* **weight** *weight_value* : Use this command to configure two static entries, such as a peer in the route table. If you configure an entry with the existing same flag, host, realm, then only the weight is updated with the higher of the two of them. The **host** and **realm** parameters allow wildcard character values. The **weight** is an optional parameter with the default value as 10. The **peer** is a mandatory parameter.

Note You can configure multiple route entries with the same host and realm but a different peer without being overridden.

- **route-failure deadtime** *deadtime_value* **result-code** *result_code_value* **threshold** *number*: Specify the duration in seconds for which the system keeps the route in the **FAILED** status. After the configured duration expires, the system changes the status to **AVAILABLE**. *deadtime_value* must be an integer in the range of 1–86400. The default value is 60.
- **route-failure recovery-threshold percent** *recovery_threshold_percentage*: Specify the percentage value at which the failure counter is reset when provisionally changing the status from **FAILED** to **AVAILABLE**. For example, a failure counter of 16 caused the **AVAILABLE** status to change to **FAILED** status. After the configured deadtime expires, the status changes to **AVAILABLE**. If you configured *recovery_threshold_percentage* with 75 percent, the failure counter resets to 12, which is 75 percent of 16. The default value is 90.
- **dynamic-route expiry-timeout** *expiry_timeout_value*: Specify the expiration time for dynamic routes that you created after reaching the Diameter destination host. The default value is 86400 secs, which equals one day.
- **dynamic-origin-state-id** *boolean_value* : Specify whether you want to enable or disable the dynamic origin state ID. The default value is true.

Note After the configuration changes from dynamic to static, if the peer is started with either the dynamic origin state ID or the static origin state ID, the peer sends the default static value. Similarly, for a configuration change from the dynamic to static, the peer sends the dynamic value that the Diameter endpoint fetches from the cache pod. In this case, there's a reconnection.

Configuration Example

The following is an example configuration of the Diameter endpoint on the Gy interface.

```
profile diameter-endpoint gy
 internal-vip 209.165.200.234
 name gyProf1
```

```
  destination-host-avp always
  vsa-support all-from-dictionary
  max-outstanding  128
  response-timeout 80
  connection-timeout 20
  dscp af11
  basemsg retransmission-timeout 20
  basemsg retransmissions 2
  basemsg watchdog-interval 25
  origin realm gy-cisco
  origin host gy.cisco.com
   address ipv4 209.165.200.229
  exit
  peer gyPeer1
   realm  GyServer1.com
   destination-host-name dest.host2.com
   address ipv4 209.165.200.230
   port 3900
  exit
  peer gyPeer2
   realm GyServer2.com
   address ipv4 209.165.200.231
   port 3901
  exit
exit
```

The following is an example configuration of the Diameter endpoint that is associated with the VRF.

```
profile diameter-endpoint gx
instance instance-id 1
  name gxProf1
   destination-host-avp always
   vsa-support all-from-dictionary
   max-outstanding 128
   response-timeout 20
   connection-timeout 5
   dscp be
   basemsg retransmission-timeout 2
   basemsg retransmissions 10
   basemsg watchdog-interval 6
   origin realm gx-cisco
   origin host gx.cisco.com
    address ipv4 209.165.200.230
    address vrf vrf_signaling
   exit
   peer gxPeer1
    realm dummyDestRealm.com
    address ipv4 209.165.200.231
    port  3868
   exit
   peer gxTest
    realm xyznetworks.com
    address ipv4 209.165.200.232
    port  4868
   exit
  exit
 exit
exit
```

Configuration Verification

To verify if the Diameter endpoint on the Gx or Gy interface is configured, use the following **show running-config profile diameter-endpoint** command:

```
[smf] smf# show running-config profile diameter-endpoint
 profile diameter-endpoint gx
 internal-vip 209.165.200.234
 name gxProf1
  destination-host-avp always
  vsa-support all-from-dictionary
  origin realm gx-cisco
  origin host gx.cisco.com
   address ipv4 209.165.200.235
  exit
  peer gxPeer1
   realm  GxServer1.com
   destination-host-name dest.host1.com
   address ipv4 ipv4 209.165.200.230
   port 3870
  exit
  peer gxPeer2
   realm GxServer2.com
   address ipv4 10.84.27.161
  exit
 exit

profile diameter-endpoint gy
 internal-vip 209.165.200.234
 name gyProf1
  destination-host-avp always
  vsa-support all-from-dictionary
  max-outstanding  128
  response-timeout 80
  connection-timeout 20
  dscp af11
  basemsg retransmission-timeout 20
  basemsg retransmissions 2
  basemsg watchdog-interval 25
  origin realm gy-cisco
  origin host gy.cisco.com
   address ipv4 209.165.200.229
  exit
  peer gyPeer1
   realm  GyServer1.com
   destination-host-name dest.host2.com
   address ipv4 209.165.200.230
   port 3900
  exit
  peer gyPeer2
   realm GyServer2.com
   address ipv4 209.165.200.231
   port 3901
  exit
exit
```

To verify if the Diameter endpoint is associated with a VRF, use the following **show running-config profile diameter-endpoint gx** command:

```
profile diameter-endpoint gx
instance instance-id 1
  name gxProf1
   destination-host-avp always
   vsa-support all-from-dictionary
   max-outstanding 128
   response-timeout 20
   connection-timeout 5
   dscp be
   basemsg retransmission-timeout 2
   basemsg retransmissions 10
```

```
   basemsg watchdog-interval 6
   origin realm gx-cisco
   origin host gx.cisco.com
    address ipv4 209.165.200.230
   address vrf vrf_signaling
   exit
   peer gxPeer1
    realm dummyDestRealm.com
    address ipv4 209.165.200.231
    port  3868
   exit
   peer gxTest
    realm xyznetworks.com
    address ipv4 209.165.200.232
    port  4868
   exit
  exit
 exit
exit
```

Configuring Busy Time for DPR

To configure the busy time for DPR in diameter ep, use the following configuration:

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        busy time time_duration
        end
```

NOTES:

- **profile diameter-client** *diameter_client_name*: Specify a Diameter client profile name.
- **endpoint** *endpoint-profile-name*: Specify an existing endpoint profile name to associate it with a Diameter client profile.
- **peer** *peer_name*: Specify the name of the peer node.
- **busy time** *time_duration*: Specify the time duration after which the connection is reattempted to peer. The time duration value must be an integer in the range of 1–300 seconds. The default value is 3 seconds.

Configuring Do Not Talk Time for DPR

To configure the do not talk time for DPR in diameter ep, use the following configuration:

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        do not talk time time_interval
        end
```

NOTES:

- **profile diameter-client** *diameter_client_name*: Specify a Diameter client profile name.
- **endpoint** *endpoint-profile-name*: Specify an existing endpoint profile name to associate it with a Diameter client profile.
- **peer** *peer_name*: Specify the name of the peer node.
- **do not talk time** *time_interval*: Specify the time interval between receiving of DPR by diameter endpoint and sending of DPA response. The time interval value must be the integer in the range of 1–300 seconds. The default value is 3 seconds.

Configuring Drain Time for DPR

To configure the drain time for DPR in diameter ep, use the following configuration:

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        drain time time_interval
        end
```

NOTES:

- **profile diameter-client** *diameter_client_name*: Specify a Diameter client profile name.
- **endpoint** *endpoint-profile-name*: Specify an existing endpoint profile name to associate it with a Diameter client profile.
- **peer** *peer_name*: Specify the name of the peer node.
- **drain time** *time_interval*: Specify the time interval between receiving of DPR by diameter endpoint and sending of DPA response. The time interval value must be an integer in the range of 1 to 10 seconds. The default value is 3 seconds.

Configuring Reboot Time for DPR

To configure the reboot time for DPR in diameter ep, use the following configuration:

```
config
  profile diameter-client diameter_client_name
    endpoint endpoint-profile-name
      peer peer_name
      disconnect peer request
        reboot time time_duration
        end
```

NOTES:

- **profile diameter-client** *diameter_client_name*: Specify a Diameter client profile name.
- **endpoint** *endpoint-profile-name*: Specify an existing endpoint profile name to associate it with a Diameter client profile.

- **peer** *peer_name*: Specify the name of the peer node.
- **reboot time** *time_duration*: Specify the time duration after which the connection is reattempted to peer. The time duration value must be an integer in the range of 1–300 seconds. The default value is 3 seconds.

Dynamic Configuration Change

Feature Description

The SMF allows you to change the Diameter endpoint configuration dynamically without impacting the existing calls.

How it Works

The following table lists the impact of dynamic update to the various Diameter endpoint configurations:

Table 27: Dynamic Update of Diameter Endpoint Configuration

Configuration	Dynamic Change	Impact on Existing Sessions
Connection attributes: • BaseMsg attributes, such as retransmissionTimeout, retransmissions • connectionTimeout • responseTimeout • originStateId • Origin attributes, such as Host Address, Host Name, and Realm • Peer attributes, such as address, port, and realm	Allowed	Change in connection attributes has the following impact: • RPC is deregistered and registered with new values for all peers in the endpoint profile. • All the messages initiated on the peer fail when the connection is down. • All the requests in transit on the peer are dropped. Server can't send request messages (RAR) and response messages (CCA) on these connections for existing calls.
DisconnectPeerRequest Properties: • drainTime • rebootTime • doNotTalkTime • busyTime	Not allowed	When the DisconnectPeerRequest Properties are updated for a peer, the new values are effective only after the pod restart or after the connection is reset.

Configuration	Dynamic Change	Impact on Existing Sessions
Route-entry update or addition	Allowed	An update or addition to route entry has the following impact: • Route entries are recreated after change. • After a peer is deregistered, all route entries for the peer are deleted.
Diameter-endpoint profile removal	Allowed	The removal of an endpoint profile has the following impact: • All the peers of the endpoint profile are deregistered. • Existing calls using these peers or routes fail. • No new calls are initiated on those peers.

Destination Host AVP for CCR and Retried Messages

Feature Description

The destination-host AVP is used for forwarding or routing a Diameter request message. The destination host name that an application, such as Gx and Gy, uses is identified from the incoming application-level messages. The absence of the destination-host AVP causes a message to be sent to any Diameter server that supports the application within the realm specified in destination-realm AVP.

Based on the end user configuration, you can include the destination-host AVP for the CCR and the retried messages.

Configuring Destination Host AVP

To configure the destination host AVP, use the following sample configuration:

```
config
  profile diameter-endpoint interface_name
    instance instance-id instance-id
      name profile_name
        destination-host-avp [ always | session-binding ]
  exit
```

NOTES:

- **profile diameter-endpoint** *interface_name*: Specify a Diameter endpoint profile, which is either Gx or Gy interface.

- **instance instance-id** *instance-id* : Specify the GR instance.
- **name** *profile_name*: Specify the Diameter endpoint profile name.

Note You can define a maximum of 100 profiles per interface.

- **destination-host-avp [always | session-binding]**: Specify one of the following types of message in which the destination host AVP is to be encoded:
  - **always**—If destination-host-avp is configured to this message type, include the destination-host-avp in both the CCR-I, CCR-U, or CCR-T messages and the retried messages. **always** is the default message type.
  - **session-binding**—If destination-host-avp is configured to this message type, encode the destination-host-avp in CCR-U and CCR-T messages, and not CCR-I and retried messages.

Configuration Example

The following is an example configuration of the destination host AVP.

```
profile diameter-endpoint gx
   instance instance-id 1
      name gxProf1
         destination-host-avp session-binding
exit
```

Peer Management

Feature Description

The SMF supports peer management in routing. It allows to choose an appropriate peer for a transaction to occur.

The peer selection logic depends on the Diameter Endpoint and Host Selection configuration.

The Diameter servers connect to the gateway in direct and indirect ways through DRA. The entities involved in the peer management are as follows:

1. Destination-Host: A Diameter entity servicing the request or the final destination for the Diameter message
2. Peer: Connects with the Diameter entity that establishes transport (TCP) connection directly. It can be either a DS or DRA.
3. Route Entry: Defines a path for reaching a Diameter entity from the gateway, essentially the next immediate peer to contact to reach a particular Diameter entity.
4. Routing Table: The diabase library maintains the table of route-entries. The construction of a routing table is through the configuration under the Diameter Endpoint (peer and route-entry CLI) and also dynamically learned from the response messages.

5. Multipath Routes: Multipath Routes are when there are more than one route entry to reach a particular Diameter entity.

Route Flags

Following are the route flags in Diameter Endpoint:

Table 28: Route Flags

Flag Name	Description
Static (S)	Static routes are the route entries based on the configuration under the Diameter Endpoint.
Path-Cache (P)	Every Diameter session has a reference to the route entry in the routing table. When you select a static route for a session, a copy of that static route or a path-cache route is created. It is as same as the static route except for the flag value.
Dynamic (D)	Dynamic routes are the route entries learned from the response messages from the peer.

Route Status

The route statuses for peers in Diameter Endpoint are as follows:

Table 29: Route Status

Route Status	Description
Pending	All the static routes start with this status and confirms the registration of an RPC host.
Active	After a successful Ping method, the Pending status moves to Active status.
Inactive	If the Ping method fails, it marks all the routes with that peer as Inactive. This status remains until the peer becomes reachable.
Failed	An Active route moves to a Failed status when it meets the route failure criteria.
Deleted	None of the routes are hard deleted but they remain soft deleted with a Deleted status.
Expired	Dynamic routes, after expiration, are set to Expired status.

Route Status	Description
Cloned	When the Path-Cache route is created from the Static route, the status of the original static route changes to Cloned. Cloned is an internal state and not borrowed from legacy implementation.

Considerations for Peer Management

Following are the considerations for peer management in Diameter Endpoint:

- The DRA creates a route table for every endpoint profile. Peers configured within the endpoint are a primary source of route entries in the route table.
- Peers have an optional CLI to set the Destination-Host-Name that is different from the peer name. If the destination host name is not set, it copies the peer name into the Destination-Host-Name.
- Each peer creates a direct and a realm-based route entry. It adds one more route entry when the Destination-Host-Name is different from the peer name.
- The default weight of the static route is 10. You cannot configure the weight of routes formed from the peer entries. However, you can override them with a higher value using a route entry with the same host and realm combination.
- The route table gets populated on the endpoint profile update notification, with each entry status as ‘Pending’.
- You can add the dynamic route in the response path only if the session is referring a realm-based route entry. For a direct route entry, you cannot add the dynamic route in the response path.
- The weight of a new dynamic route is the same as the route selected in the request path.
- Dynamic routes have the expiration time configured. The active time of the dynamic routes enables during the selection of routes.

Route Selection

The route selection process and its usage in retries are as follows:

1. While providing a response for a CCR-I or CCR-U message, the Diameter endpoint sends the details of the primary host, secondary host, realm, and bounded peer as part of the route data. The same details are provided by the service as part of subsequent requests.
2. In the absence of a route data field in the request from the service, the Diameter endpoint determines primary host, secondary host, and realm from the host selection profile, which is associated with the client profile, specified in the request.
3. Host selection profile has a mandatory primary and an optional secondary host-realm pair. While realm is an optional CLI, it sets to a default value.
4. The host and realm serve as an input to the route search algorithm to find possible multiple matching routes. The order depends on the status, flag and weight.
5. In the absence of host selection profile configuration, the peer management module selects and sorts all the active routes in the route table.

Note Routes selection happens through the round robin method from the ordered routes list of the primary host or secondary host. This method avoids trying all the routes of the primary host and then trying all the routes of the secondary host.

Route Sort Order

The route sort orders for entries in the Diameter peer are as follows:

- The routes with the active status take the highest precedence.
- Among the routes with the same status, if a route matches the bounded peer, then that route takes the highest precedence. Then, the next precedence is for the dynamic routes followed by the Path-Cache routes.
- The peer arranges multiple routes of the same flags among themselves based on their weight, where the higher value takes precedence.
- Weight always outweighs routes with the exact match of host and realm entries.
- Exact match entries have the priority only if there are two routes with equal weights.

Host Selection

This section describes about the host selection, its implementation, and the sample configuration for host selection on the Diameter endpoint.

Feature Description

The Diameter endpoint keeps the data of an individual profile name with algorithm and list of primary and secondary host details. The local data structure can keep a maximum of 64 host details in the indexed form. The host details include the primary host-realm, and secondary host-realm.

How it Works

The peer management module sends the request to the host selection module with the profile name, MSISDN, and IPv4 address. The host selection module checks the profile name in the local data structure that is populated from the configuration map. If the profile name matches, then it derives the host details with following algorithms.

- MSISDN modules—The MSISDN is converted into numeric value. Then, the index is calculated by the available number of MSIDN mod host entries.
- IP address modules—IP address is converted into numeric value. Then the index is calculated by the available number of numeric IP address value mod host entries.
- Round robin—The default algorithm is the round robin of available entries per profile name.

Note A host selection profile is bound with the Diameter client. You can bind one host selection profile for the multiple Diameter clients.

Configuring Host Selection through Diameter Endpoint

Diameter host selection configuration is available in the Diameter profile. You can configure multiple Diameter hosts and then bind these hosts to a different Diameter client.

To configure the host selection through the Diameter endpoint, use the following sample configuration:

```
config
   profile diameter-host-selection host_selection_name
      algorithm algorithm-name
      hosts hosts_number
         primary host host_ip_address
         primary realm realm_name
         secondary host host_ip_address
         secondary realm realm_name
      end
```

NOTES:

- **profile diameter-host-selection** *host_selection_name*: Specify the Diameter host selection profile name.
- **algorithm***algorithm-name*: Choose the algorithm to select the host. *algorithm-name* has the **ipaddr-modulus**, **msisdn-modulus**, and **round-robin** values.
- **hosts** *hosts_number*: Specify the precedence of the host in the form of index from 1-64.
- **primary host** *host_ip_address*: Specify the primary host name.
- **primary realm** *realm_name*: Specify the primary host realm.
- **secondary host** *host_ip_address*: Specify the secondary host name.
- **secondary realm** *realm_name*: Specify the secondary host realm.

Configuration Example

The following is an example configuration of the host selection.

```
profile diameter-host-selection hs1
 algorithm ipaddr-modulus
 hosts 1
  primary host 209.165.200.239
  primary realm cisco.com
  secondary host g192.168.2.1
  secondary realm google.com
 exit
 hosts 2
  primary host 209.165.200.240
  primary realm facebook.com
  secondary host 209.165.200.241
  secondary realm conflunt.com
 exit
exit

profile diameter-client dc1
 endpoint       gxProf1
 host-selection hs1
exit
profile diameter-client dc2
 endpoint       gyProf1
```

```
 host-selection hs1
exit
```

Route Failure

Feature Description

A route failure counter starts at zero. This counter is incremented in the following scenarios:

- When the transaction is attempted using that route times out.
- When a response is received with the result code matching the configured failure result codes.

The count is decremented each time that a successful response is received. When the failure count exceeds the threshold, the route is marked as failed. Periodically, the route failure count is reduced by a recovery threshold value to allow the failed route to become available.

Configuring Route Failure

To configure the route failure, use the following sample configuration:

```
config
  profile diameter-endpoint interface_name
    name profile_name
    internal-vip ip_address
      route-failure deadtime deadtime_valueresult-code result_code_value
threshold  number
       route-failure result-code result_codes_value
       route-failure threshold  threshold_number
       route-failure recovery-threshold percent  recovery_threshold_percentage
exit
```

NOTES:

- **route-failure deadtime** *deadtime_value***result-code** *result_code_value* **threshold** *number*: Specify the duration in seconds for which the system keeps the route in the **FAILED** status. After the configured duration expires, the system changes the status to **AVAILABLE**. *deadtime_value* must be an integer in the range of 1–86400. The default value is 60.
- **route-failure result-code** *result_codes_value*: Specify the answer messages that are to be considered as failures, in addition to the requests that time out.

Note You can specify up to 16 result codes.

- **route-failure threshold** *threshold_number*: Specify the number of errors that cause the **FAILED** status. The default value is 16.

Note The error counter begins at zero. In a case of a good response, the error counter decrements or increments. This counter does not decrement below zero or increment above the configured threshold number.

- **route-failure recovery-threshold percent** *recovery_threshold_percentage*: Specify the percentage value at which the failure counter is reset when provisionally changing the status from **FAILED** to **AVAILABLE**. For example, a failure counter of 16 caused the **AVAILABLE** status to change to **FAILED** status. After the configured deadtime expires, the status changes to **AVAILABLE**. If *recovery_threshold_percentage* is configured with 75 percent, the failure counter resets to 12, which is 75 percent of 16. The default value is 90.

Configuration Example

The following is an example configuration of route failure.

```
profile diameter-endpoint gydc01
   name gyProf1
   internal-vip ip_address
      route-failure deadtime  600
      recovery-threshold 16
      percent 90
      result-code rc1
exit
```

Configuration Verification

To verify if the Diameter endpoint on the Gx or Gy interface is configured, use the following **show running-config profile diameter-endpoint** command:

```
[smf] smf# show running-config profile diameter-endpoint
 profile diameter-endpoint gx
 internal-vip 209.165.200.234
 name gxProf1
   internal-vip ip_address
      route-failure deadtime 600
      recovery-threshold 16
      percent 90
      result-code rc1
exit
```

Bounded Peer

Feature Description

A peer with which the last Credit Control Request - Initial (CCR-I) or Credit Control Request - Update (CCR-U) interaction happened is considered as the bounded peer. Based on current request processing, the Diameter endpoint communicates to the service for the primary host or secondary host and the bounded peer. Then, the service communicates to the Diameter endpoint for the primary host or secondary host and the bounded peer that is to be used for the request processing.

Matching of route for the bounded peer takes the highest precedence for sending the subsequent CCR-U or Credit Control Request - Terminate (CCR-T) message. If the route list of a host has an active entry and the peer matches with the bounded peer, then the route entry takes the highest precedence for the request processing.

How it Works

This section describes how the bounded peer works.

- The details on the primary and secondary host and the bounded peer are included in the request from the service. Similarly, these details are included in the response to the service.

- If the route list of a host has one or more active entries and the peer matches with the bounded peer, then the route entries take priority for request processing.
- The bounded peer, which is specified in the request or response, is always associated with the primary host and realm.

Failure Handling

Feature Description

Failure handling is managed by configuring the failure handling profiles for the Diameter messages and failures. With this configuration, the behavior of a Diameter pod is determined in failure scenarios. You can configure any number of failure handling profiles.

After configuring the failure handling profiles, associate them with a specific Diameter client profile. If you don't associate a configured failure handling profile with a Diameter client profile, then a default failure profile is considered.

How it Works

Failure handling works in the following way:

- If there is a failure, the Diameter endpoint fetches the applicable failure handling profile.
- If the failure handling profiles are not defined or if a profile is defined with no message and failure type that should match the failed request, then the default failure handling is applied. The default failure handling is no retry with the **action terminate** and subaction as *with-term-req*, which implies with no termination request.
- Diameter endpoint reattempts request with the alternate peers or routes until the request is successful or the reattempt the reaches the configured retry count as specified by applicable failure handling profile.
- Routes are selected in the round robin method from the ordered routes list of each host. For example, on failure for route of host1, the next route in the list of routes of host2 is used for retrying. During retries, if the route list of one of the hosts exhausts, then the remaining route of other hosts is used for retries.
- During retries if an already tried route is found, then the route is skipped.
- If the applicable peer or route count is lower than the retry count, then remaining retries are discarded after all the applicable peers or routes are attempted.
- Retry count, which is determined during the first failure after the request is sent out, is used. If there is a failure during retries and that failure corresponds to a different failure handling profile with a different retry count, then also Diameter endpoint continues with the retry count that is determined during the first failure.
- Retry counting starts only after a minimum of one request is sent. Failure before the retry count is not considered.
- Even after all the reattempts or all peers or routes reattempts, if the request is not successful, then the Diameter endpoint send the action and subaction as part of response to the service.

- Action and subaction applicable for the most recent failure is used in the response.
- No additional handling is done on the Diameter endpoint for any action or subaction because action for those are taken on the service side as follows:

  Action

  - **continue**: Continue with the session
  - **terminate**: Terminate the session. This action is the default action.

  Subaction

  - **discard-traffic**: Block or discard the data traffic. This subaction is associated with action with the **continue** . action and is applicable only for the Gy interface.
  - **local-fallback**: Apply local policies. This subaction is associated with the **continue** action.
  - **none**: No action. This subaction is associated with the Associated with **continue** action and is applicable only for the Gy interface. **none** is the default option for the Gy calls for the **continue** action.
  - **retry-server-on-event**: Reconnect to server on credit control update requests. This subaction is associated with the **continue** action and is applicable only for the Gx interface.
  - **send-ccrt-on-call-termination**: Send CCR-T request to PCRF for credit control update request failure. This subaction is associated with the **continue** action and is applicable only for the Gx interface. **send-ccrt-on-call-termination** is the default option for Gx calls for **continue** action.
  - **with-term-req**: Terminate the session by sending the termination request (CCR-T). This subaction is associated with the **terminate** action and is applicable only for the Gx interface. **with-term-req** is the default option for the Gx calls for **terminate** action.

Configuring Failure Handling

Configuration of failure handling includes the following steps:

1. Configuring Failure Handling Profile, on page 114
2. Associating the failure handling profile to the Diameter client profile. To configure the Diameter client profile, see the Configuring Diameter Client Profile, on page 95 procedure.

Configuring Failure Handling Profile

To configure a failure handling profile, use the following sample configuration:

```
config
  profile failure-handling failure_handling_profile_name
    interface diameter
      message [ any | credit-control-initial | credit-control-terminate
 | credit-control-update ]
         failure-type [ any | local-error | result-code {result-code-value
| result-code-range-start-value | result-code-range-end-value |
comma-separated-result-code-value-or-range } | experimental-result-code
experimental-result-code-value | experimental-result-code-start-value |
```

```
experimental-result-code-end-value |
comma-separated-experimental-result-code-value-or-range
}experimental-result-code-value | experimental-result-code-start-value |
experimental-result-code-end-value | comma-separated-experimental-result-code-value-or-range
 ]
              retry count
            action [ continue discard-traffic | local-fallback | retry-server-on-event
 | send-ccrt-on-call-termination | terminate with-term-request | without-term-request ]

  exit
```

NOTES:

- **profile failure-handling** *failure_handling_profile_name*: Specify a name for the failure handling profile.
- **interface diameter**: Specify the failure handling profile for the Diameter interface.
- **message [any | credit-control-initial | credit-control-terminate | credit-control-update]**: Choose a message value from the available options. This is a mandatory parameter.
- **failure-type [any | local-error | result-code {***result-code-value* | *result-code-range-start-value* | *result-code-range-end-value* | *comma-separated-result-code-value-or-range* **| experimental-result-code experimental-result-code-value | experimental-result-code-start-value | experimental-result-code-end-value | comma-separated-experimental-result-code-value-or-range }***experimental-result-code-value* | *experimental-result-code-start-value* | *experimental-result-code-end-value* | *comma-separated-experimental-result-code-value-or-range* **]**: Specify a Diameter failure type for which an action must be taken. Choose a failure type value from the available options. This is a mandatory parameter.

Note You can configure multiple failure types.

- **retry** *count*: Specify the number of alternate peers or routes to retry on receiving a failure response. The default value is zero.
- **action [continue** *discard-traffic* | *local-fallback* | *retry-server-on-event* | *send-ccrt-on-call-termination* **| terminate** *with-term-request* | *without-term-request* **]**: Choose an action value as **continue** or **terminate** . Choose subactions of the selected action from the available options, as required.

Note To clear a subaction or reset a subaction of **continue** or **terminate** action to default, perform the following steps before saving the configuration:

1. **no profile failure-handling** *failure-handling-profile-name*

   interface diameter message*diameter-message*
   failure-type*failure_name* **result-code** *result_code*
   action*action_name sub_action*
   exit

2. **profile failure-handling** *failure-handling-profile-name*
   interface diameter message*diameter_message*
   failure-type*failure_name* **result-code** *result_code*
   action*action_name*
   exit

Configuration Example

The following is an example configuration of the failure handling.

```
profile failure-handling fh1
  interface diameter
    message credit-control-initial
      failure-type any
        retry 2
        action terminate with-term-req
      exit
      failure-type local-error
        retry 3
        action continue local-fallback
      exit
      failure-type result-code 3000
        retry 2
        action continue discard-traffic
       exit
      exit
      failure-type result-code 4000
        action continue retry-server-on-event
       exit
      exit
      failure-type result-code 4001-4010
        action continue send-ccrt-on-call-termination
       exit
      exit
      failure-type result-code 4011-4020,4025,4030-4040
        action terminate without-term-req
       exit
      exit
      failure-type exp-result-code 5000
        action terminate with-term-req
       exit
      exit
      failure-type exp-result-code 5010-5015
        action terminate
       exit
      exit
    exit
```

```
    message credit-control-terminate
      failure-type any
        retry 2
        action terminate
      failure-type local-error
        action continue retry-server-on-event
      exit
    exit

    message credit-control-update
      failure-type any
        action continue send-ccrt-on-call-termination
      exit
      failure-type local-error
        action continue discard-traffic
      exit
    exit

    message any
      failure-type any
        action continue discard-traffic
      exit
      failure-type local-error
        action continue
      exit
    exit
  exit
exit

profile failure-handling fh2
  interface diameter
    message credit-control-update
      failure-type any
        retry 2
        action continue
      exit
      failure-type local-error
        action terminate without-term-req
      exit
    exit
  exit
exit
```

Configuration Verification

To verify if the failure handling is configured, use the following **show running-config profile diameter-client** command:

```
show running-config profile diameter-client
   profile diameter-client dc2
    endpoint gyProf1
       failure-handling-profile FH1
exit
```

OAM Support

Bulk Statistics Support

The SMF maintains the following metrics as part of the Diameter endpoint.

diameter_request_message_total

Description: Indicate the count of diameter requests processed by diameter endpoint.

Note

- The peer_address counter is empty for inbound requests and depending on the point of failure, this counter can be empty for the outbound requests.
- The retry counter is always logged as zero for IPC timeout.
- The transaction_type counter is hard-coded to "origin".
- The endpoint_name counter is empty for inbound requests and depending on the point of failure, this counter can empty for outbound requests.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **interface**: gx, gy
- **message_name**: ccri, ccru, ccrt, rar, asr peer_address
- **status**: attempted, peer_down, err_cfg, err_maxout, timeout_ipc, err_ipc, err_unmarshal
- **retry**: retry count gr_instance transcation_type
- **endpoint_name**: name of endpoint profile used during processing
- **message_direction**: inbound, outbound

Label Production:

- interface
- message_name
- peer_address status

Label Debug:

- retry
- gr_instance
- transaction_type

Label Trace:

- endpoint_name
- message_direction

diameter_response_message_total

Description: Indicate the count of diameter responses that the Diameter endpoint processes.

Note

- The peer_address counter is empty for inbound requests and depending on the point of failure, this counter can be empty for the outbound requests.
- The result_code counter is logged as " " for outbound responses, local failure, response timeout, and IPC timeout.
- The action or subaction counter is empty for outbound responses and "success" responses.
- The endpoint_name counter is empty for inbound requests and depending on the point of failure, this counter can empty for outbound requests.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **interface**: gx, gy
- **message_name**: ccai, ccau, ccat, raa, asa
- **peer_address**
- **status**: success, err_cfg, err_maxout, err_send, timeout_res, timeout_ipc, err_ipc, err_unmarshal, err_rc, err_exp_rc
- **result_code**: result-code or experimental-result-code that the Diameter node encountered during the response processing
- **action**: continue, terminate
- **subaction**: discard-traffic, local-fallback, retry-server-on-event, send-ccrt-on-call-termination, with-term-req, without-term-req
- **endpoint_name**: name of endpoint profile used during processing
- **gr_instance**
- **message_direction**: inbound, outbound

Label Production:

- interface
- message_name
- peer_address status

- status
- result_code

Label Debug:

- action
- subaction
- gr_instance

Label Trace:

- endpoint_name
- message_direction

diameter_response_message_seconds_total

Description: Indicate the cumulative response time in seconds of diameter requests that the Diameter endpoint processes.

Note

- The peer_address counter is empty for inbound requests and depending on the point of failure, this counter can be empty for the outbound requests.
- The result_code counter is logged as " for outbound responses, local failure, response timeout, and IPC timeout.
- The action or subaction counter is empty for outbound responses and "success" responses.
- The endpoint_name counter is empty for inbound requests and depending on the point of failure, this counter can empty for outbound requests.
- This counter is not incremented for local failure or IPC timeout.

Default Level: MetricsVerboseLevelProduction

Label Details:

- **interface**: gx, gy
- **message_name**: ccai, ccau, ccat, raa, asa
- **peer_address**
- **status**: success, err_cfg, err_maxout, err_send, timeout_res, timeout_ipc, err_ipc, err_unmarshal, err_rc, err_exp_rc
- **result_code**: result-code or experimental-result-code that the Diameter node encountered during the response processing
- **action**: continue, terminate
- **subaction**: discard-traffic, local-fallback, retry-server-on-event, send-ccrt-on-call-termination, with-term-req, without-term-req

- **gr_instance**
- **endpoint_name**: name of endpoint profile used during processing
- **message_direction**: inbound, outbound

Label Production:

- message_name
- origin_host
- origin_realm
- disconnect_cause
- result_code

Label Debug:

- action
- subaction
- gr_instance

Label Trace:

- endpoint_name
- message_direction

diam_base_msg_total

Description: Indicate the count of diameter base message requests that the Diameter endpoint processes.

Note

- The DPR counter is supported only for the DPR that is received from a peer.
- The result_code counter is logged as 5012 if the DPR received has the mandatory AVP missing or if origin-host and origin-realm in DPR does not match with destination-host and destination-realm in connection details.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **message_name**: DPR
- **origin_host**
- **origin_realm**
- **disconnect_cause**: REBOOTING, BUSY, DO_NOT_WANT_TO_TALK_TO_YOU
- **result_code**: 2001, 5012

- **gr_instance**

Label Production:

- message_name
- origin_host
- origin_realm
- disconnect_cause
- result_code

Label Debug:

- gr_instance

Label Trace:

- endpoint_name
- message_direction

diam_base_msg_seconds_total

Description: Indicate the cumulative response time in seconds of diameter base message requests that the Diameter endpoint processes.

Note

- The DPR counter is supported only for the DPR that is received from a peer.
- The result_code counter is logged as 5012 if the DPR received has the mandatory AVP missing or if origin-host and origin-realm in DPR does not match with destination-host and destination-realm in connection details.

Default Level: MetricsVerboseLevelProduction

Label Details:

- **message_name**: DPR
- **origin_host**
- **origin_realm**
- **disconnect_cause**: REBOOTING, BUSY, DO_NOT_WANT_TO_TALK_TO_YOU
- **result_code**: 2001, 5012
- **gr_instance**

Label Production:

- interface
- message_name

- diameter_dictionary_type
- status
- unknown_avp

Label Debug:

- gr_instance

diameter_encode_message_total

Description: Indicate the count of diameter base message requests that the Diameter endpoint processes.

Note

- The DPR counter is supported only for the DPR that is received from a peer.
- The result_code counter is logged as 5012 if the DPR received has the mandatory AVP missing or if origin-host and origin-realm in DPR does not match with destination-host and destination-realm in connection details.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **interface**: gx, gy, ""
- **message_name**: ccri, ccru, ccrt, raa, asa
- **endpoint_name**: name of endpoint profile used during processing
- **dict_name**
- **status**: success, failure, partial
- **unknown_avp**: 0, 1
- **gr_instance**

Label Production:

- interface
- message_name
- diameter_dictionary_type
- status
- unknown_avp

Label Debug:

- status_code
- gr_instance

diameter_decode_message_total

Description: Indicate the count of decoding that the Diameter endpoint performed.

Note

- The interface is empty for unsupported interface or command code.
- The message_name counter is empty for the unsupported interface or command code
- The dict_name counter is empty when default dictionary is used. Else, this counter indicates the name of dictionary that is used for an operation.
- The status counter is logged as failure only for the unsupported interface or command code. This counter is logged as partial if an issue that is seen during the encoding is ignored. For example, an unknown AVP.
- The unknown_avp counter indicates if any unknown AVPs are found during encoding, where zero indicates not found and 1 indicates found.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **interface**: gx, gy, ""
- **message_name**: ccai, ccau, ccat, rar, asr
- **endpoint_name**: name of endpoint profile used during processing
- **dict_name**
- **status**: success, failure, partial
- **unknown_avp**: 0, 1
- **gr_instance**

Label Production:

- interface
- message_name
- diameter_dictionary_type
- status
- unknown_avp

Label Debug:

- status_code
- result_code
- gr_instance

Label Trace:

- endpoint_name

diameter_pod_status

Description: Indicate the pod status as active or standby.

Note

- Value 1 indicates the status as active and zero indicates the status as standby.
- The VIP counter is not used to determine the pod status when a Diameter pod is running in server mode. In this case, VIP is empty in the server mode.

Metrics Type: Gauge

Default Level: MetricsVerboseLevelProduction

Label Details:

- **vip**: VIP used for determining pod status

Label Production:

- vip

Label Debug:

- gr_instance

Label Trace:

- endpoint_name

dispatch_error_total

Description: Indicate the count of inbound requests that had error or timeout during dispatch to service.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **application**
- **command_code**
- **error_code**
- **gr_instance**

Label Production:

- application
- command_code

- error_code

Label Debug:

- gr_instance

dispatch_error_seconds_total

Description: Indicate the cumulative time in seconds spent during dispatching of inbound requests to service that had error or timeout.

Default Level: MetricsVerboseLevelProduction

Label Details:

- **application**
- **command_code**
- **error_code**
- **gr_instance**

Label Production:

- application
- command_code
- error_code

Label Debug:

- gr_instance

policy_engine_message_total

Description: Indicate the count of messages that are sent to service for which response is received.

Metrics Type: Counter

Default Level: MetricsVerboseLevelProduction

Label Details:

- **application**
- **command_code**
- **gr_instance**

Label Production:

- application
- command_code

Label Debug:

- gr_instance

policy_engine_message_seconds_total

Description: Indicate the cumulative time in seconds spent during processing of a message sent to service.

Default Level: MetricsVerboseLevelProduction

Label Details:

- **application**
- **command_code**
- **gr_instance**

Label Production:

- application
- command_code

Label Debug:

- gr_instance

Troubleshooting Information

Monitor Protocol and Monitor Subscriber

Feature Description

SMF supports the SUPI and IMSI subscriber key for the Monitor Protocol and Monitor Subscriber functionality for the Diameter messages. Use the Monitor Protocol to add the interface type as Diameter.

Monitor Subscriber

Using the CLI commands, you can view the messages for a specific subscriber or a set of subscribers. For interworking, use the NF service as SMF.

Monitor Protocol

For the Diameter interface, SMF uses the Monitor Protocol for packets.

Note For the Diameter client, the monitor protocol doesn't work until you connect a minimum of one peer to the leader pod.

How it Works

You can configure the Monitor Subscriber and Monitor Protocol feature through the CLI commands in the Ops Center.

Configuring the Monitor Subscriber and Monitor Protocol Support

This section describes how to configure the Monitor Subscriber and Monitor Protocol support.

Monitoring the Subscriber Session

To monitor the subscriber in the SMF, use the following CLI command:

monitor subscriber [capture-duration *duration* **| dump filename** *file_name* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [yes] | list** *file_list* **| nf-service [sgw | smf] | supi** *supi_id* **| transaction-logs [yes | no]]**

NOTES:

- **capture-duration** *duration*: Specify the duration in seconds during which a monitor subscriber is enabled. The default value is 300 seconds (5 minutes). This is an optional parameter.
- **dump filename** *file_name*: Specify the file name to view the sorted file on the SMF Ops Center.
- **gr-instance** *gr_instance_id*: Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **imei** *imei_id*: Specify the subscriber IMEI. For example: 123456789012345, *
- **imsi** *imsi_value*: Specify the subscriber IMSI. For example: 123456789, *
- **internal-messages [yes | no]**: Enable or disable viewing the internal messages. By default, **yes** option is disabled. This is an optional parameter.
- **nf-service [sgw | smf]** : Enable the specified NF service. By default, **nf-service** is set to none. This is a mandatory parameter.

Important The **nf-service** keyword replaces the **namespace** keyword in Release 2021.02 and beyond.

- **supi** *supi_id*: Specify the subscriber identifier. For example: imsi-123456789, imsi-123*
- **transaction-logs [yes | no]**: Enable transaction logs when set to **yes**. By default, this parameter is disabled. This is an optional parameter.

  To view the transaction history logs, use the **dump transactionhistory** command.

Note The most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

Monitoring the Diameter Interface Protocol

To monitor the Diameter interface protocol on the SMF, use the following CLI command:

monitor protocol interface diameter [capture-duration *duration* **| gr-instance** *gr_instance_id* **| pcap yes gr-instance** *gr_instance_id* **]**

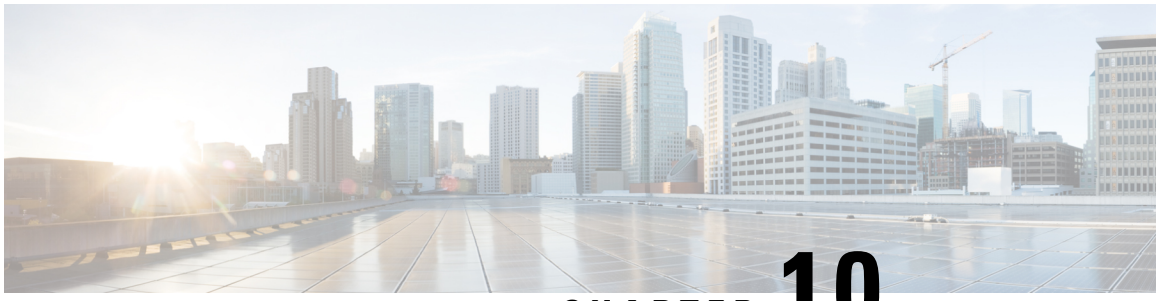
NOTES:

- **interface diameter** : Specify the interface name as Diameter.
- **capture-duration** *duration*: Specify the duration in seconds during which pcap is captured. The default is 300 seconds (5 minutes).
- **gr-instance** *gr_instance_id*: Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **pcap yes gr-instance** *gr_instance_id*: Configure this option to enable PCAP file generation. By default, this option is disabled.

Debugging Data Collection

While debugging issues with the Diameter, use the output of the following commands through the Ops Center:

- **kubectl get pods -n** *namespace*
- **kubectl get statefulsets -n** *namespace*
- **kubectl get cm -n** *namespace*
- **kubectl get service -n** *namespace*
- **helm list**
- **show full-configuration** or **show running-configuration**



CHAPTER 10

DSCP Marking

- Feature Summary and Revision History, on page 131
- Feature Description, on page 131
- DSCP Marking for Data Packets, on page 132
- DSCP Marking for Control Plane Signaling, on page 134

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
Provided support for DSCP marking of control plane signaling messages	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports a mechanism for Differentiated Services Code Point (DSCP) marking of user plane data packets and control plane signaling messages.

The DSCP Marking feature enables the SMF to perform traffic classification and prioritization to provide the appropriate quality of service (QoS) treatment. DSCP is a significant bit in the DiffServ field.

This feature uses CLI commands to configure DSCP parameters for both signaling messages and data packets. For configuration details, see the Configuring 5QI-QoS Mapping, on page 132 and Configuring DSCP Marking for Control Plane Signaling, on page 136 sections in this chapter.

Note This feature is also applicable on 4G calls with legacy interfaces.

DSCP Marking for Data Packets

Feature Description

DSCP Marking supports granular configuration. For Interactive Traffic Class (ITC), the SMF supports per-APN configurable DSCP marking for Uplink and Downlink direction that is based on 5QI and ARP-Priority level. This support allows the users to assign different DSCP values for flows with the same 5QI but different ARP priority values. For example, the ability to assign DSCP values that are based on 5QI+ARP can be used to meet compliance on priority and emergency calling via VoLTE.

DSCP Marking is a CLI-controlled feature, which enables to create and map 5QI and ARP values to enforceable QoS parameters.

The SMF sends the configured DSCP value to the UPF. Then, the UPF applies the DSCP marking on the uplink and downlink packets based on the 5QI and ARP.

How the DSCP Marking Works for Data Packets

This section describes how the DSCP marking can be performed for the data packets.

Allocation of different DSCP values for flows with the same 5QI, but different ARP values, works as follows:

- Allows DSCP marking of packets based on 5QI and ARP combination.
- 5QI and ARP configuration overrides any pre-entry of DSCP marking of packets that was based on 5QI and ARP combination.
- 5QI-only DSCP entry overrides all the existing 5QI and ARP configuration.
- Allows implementation of associated DSCP marking for 5QI and ARP for uplink and downlink traffic.

Configuring 5QI-QoS Mapping

Use the following sample configuration to create and map 5QI values to enforceable QoS parameters.

```
config
   profile qos qos_profile_name
      dscp-map qi5 qos_id
      arp-priority-level arp_value uplink user-datagram dscp-marking
```

```
dscp_marking_value
      arp-priority-level arp_value downlink { encsp-header { copy-inner |
dscp-marking dscp_marking_value } | user-datagram dscp-marking dscp_marking_value
 } }
      commit
```

NOTES:

- **dscp-map qi5** *qos_id*: Specify the ID for the authorized QoS parameters. *qos_id* must be an integer in the range of 1-255.

Note If the DSCP configuration is unavailable at the QoS flow level but available at the QoS profile level, then DSCP configuration is used from the QoS profile level.

- **arp-priority-level** *arp_value* **uplink user-datagram dscp-marking** *dscp_marking_value*: Configure the ARP priority level and then set the DSCP value in the inner IP header in uplink direction. This DSCP value is applied to the packets with the configured 5QI value.

  arp_value must be an integer in the range of 1-255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.

- **arp-priority-level** *arp_value* **downlink { encsp-header { copy-inner | dscp-marking** *dscp_marking_value* **} | user-datagram dscp-marking** *dscp_marking_value* **} }**: Configure the ARP priority level and then set the DSCP value to be applied to encapsulation header or user datagram.

  If **encsp-header** is configured, set the DSCP in the outer-ip header in downlink direction or copy the DSCP value from inner IP header to the outer IP header.

  If **user-datagram** is configured, set the DSCP in the inner IP header in downlink direction.

  arp_value must be an integer in the range of 1-255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.

The following is an example configuration.

```
profile qos test
 dscp-map qi5 1 downlink encaps-header copy-inner
 dscp-map qi5 1 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x3b encaps-header copy-inner
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x3b encaps-header dscp-marking 0x3f
 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3b

 dscp-map qi5 1 arp-priority-level 1 downlink encaps-header copy-inner
 dscp-map qi5 2 arp-priority-level 2 downlink encaps-header dscp-marking 0x3b
 dscp-map qi5 4 arp-priority-level 3 downlink user-datagram dscp-marking 0x3b
 dscp-map qi5 2 arp-priority-level 4 downlink user-datagram dscp-marking 0x3b encaps-header
 copy-inner
 dscp-map qi5 4 arp-priority-level 5 downlink user-datagram dscp-marking 0x3b encaps-header
 dscp-marking 0x3f
 dscp-map qi5 4 arp-priority-level 5 uplink user-datagram dscp-marking 0x3b
```

Verifying DSCP Configuration for UP Packets

This section describes how to verify the DSCP Marking feature configuration for the UP packets.

Use the **show running-config profile qos** command to verify the DSCP configuration for UP packets.

The following is an example output of the **show running-config profile qos** command.

```
smf# show running-config profile qos
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
exit
profile qos qos_1
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 2 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 2 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 3 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 3 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 6 downlink encsp-header copy-inner
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x01
exit
```

DSCP Marking for Control Plane Signaling

Feature Description

The SMF supports marking of DSCP values to control packets as per the configuration at the interface.

Note The current implementation of DSCP marking supports only per interface and protocol endpoint. Also, the customers should be aware of the DSCP code value range and its denoted priority.

How the DSCP Marking Works for Control Signaling

The SMF marks the ingress and egress packets after the QoS classification. The protocol endpoints provide the DSCP values at the time of registering the endpoint and interface.

The SMF uses the **dscp** command in the endpoint and interface configuration to define the DSCP values.

The following table lists the commonly used DSCP values as described in RFC 2475.

Table 30: Commonly Used DSCP Values

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	—	101 - Critical
000 000	0	Best Effort	—	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2
011 000	24	CS3		3
100 000	32	CS4		4
101 000	40	CS5		5
110 000	48	CS6		6
111 000	56	CS7		7
000 000	0	Default		
101 110	46	EF		

Limitations

The DSCP Marking feature has the following limitation:

- The DSCP Marking is per interface basis and not per peer or session.

Configuring DSCP Marking for Control Plane Signaling

This section describes how to configure the DSCP Marking feature for CP signaling messages.

Configuring the DSCP Marking feature involves the following steps:

- Configuring DSCP Marking per Endpoint, on page 136
- Configuring DSCP Marking per Interface, on page 136

Configuring DSCP Marking per Endpoint

Use the following sample configuration to configure the DSCP values at the endpoint level.

```
config
   instance instance-id gr_instance_id
      endpoint { gtp | li | protocol | radius | sbi }
         dscp dscp_value
         commit
```

NOTES:

- The DSCP Marking configuration is applicable only to the following endpoints:
  - protocol
  - sbi
  - gtp
  - radius
  - li
- **dscp** *dscp_value*: Specify the DSCP value for the control plane signaling messages. *dscp_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.

Configuring DSCP Marking per Interface

Use the following sample configuration to configure the DSCP values at the interface level.

```
config
   instance instance-id gr_instance_id
      endpoint { gtp | li | protocol | radius | sbi }
         interface { coa-nas | gtpu | n4 | n7 | n10 | n11 | n16 | n40 |
nrf | radius-client | s2b | s5 | s8 | upf-rcm-conn | upf-rcm-reg }
            dscp dscp_value
            commit
```

NOTES:

- The DSCP marking configuration is applicable to all the interfaces defined within the configured endpoints.
- **dscp** *dscp_value*: Configures the DSCP value for the control plane signaling messages. *dscp_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.
- The Service-based Interface (SBI) configuration applies to all the interfaces. If a specific interface configuration is present, it overrides the DSCP values.
- For the interfaces to work properly, it is mandatory to configure vip-ip, vip-port, and loopbackPort at each interface level.

Verifying DSCP Configuration for CP Signaling Messages

This section describes how to verify the DSCP Marking feature configuration for the CP signaling messages.

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint** command to verify the DSCP configuration for control packets.

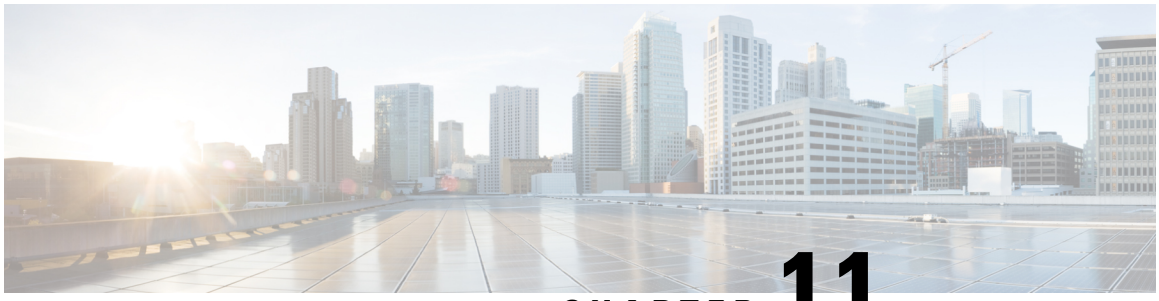
The following is an example output of the **show running-config instance instance-id 1 endpoint** command.

```
smf# show running-config instance instance-id 1 endpoint
instance instance-id 1
 endpoint sbi
  replicas 2
  nodes 1
  dscp 24
  vip-ip 209.165.200.230
  interface nrf
   loopbackPort 9050
   vip-ip 209.165.200.236 vip-port 8090
   dscp 24
  exit
 exit
exit
```

OAM Support for DSCP Marking

Monitoring Support

The SMF uses the **monitor protocol** and **monitor subscriber** commands to view the configured DSCP value.



CHAPTER 11

Dynamic Routing by Using BGP

- Feature Summary and Revision History, on page 139
- Feature Description, on page 140
- How it Works, on page 140
- Configuring Dynamic Routing Using BGP, on page 147
- Monitoring and Troubleshooting, on page 150

Feature Summary and Revision History

Summary Data

Table 31: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Disabled – Configuration required to enable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 32: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

Border Gateway Protocol (BGP) allows you to create loop-free inter-domain routing between autonomous systems (AS). An AS is a set of routers under a single technical administration. The routers can use an Exterior Gateway Protocol to route packets outside the AS. The Dynamic Routing by Using BGP feature enables you to configure the next-hop attribute of a BGP router with alternate local addresses to service IP addresses with priority and routes. The SMF BGP speaker pods enable dynamic routing of traffic by using BGP to advertise pod routes to the service VIP.

This feature supports the following functionality:

- Dynamic routing by using BGP to advertise service IP addresses for the incoming traffic.
- Learn route for outgoing traffic.
- Handling a BGP pod failover.
- Handling a protocol pod failover.
- Statistics and KPIs for the BGP speakers.
- Log messages for debugging the BGP speakers.
- Enable or disable the BGP speaker pods.
- New CLI commands to configure BGP.

How it Works

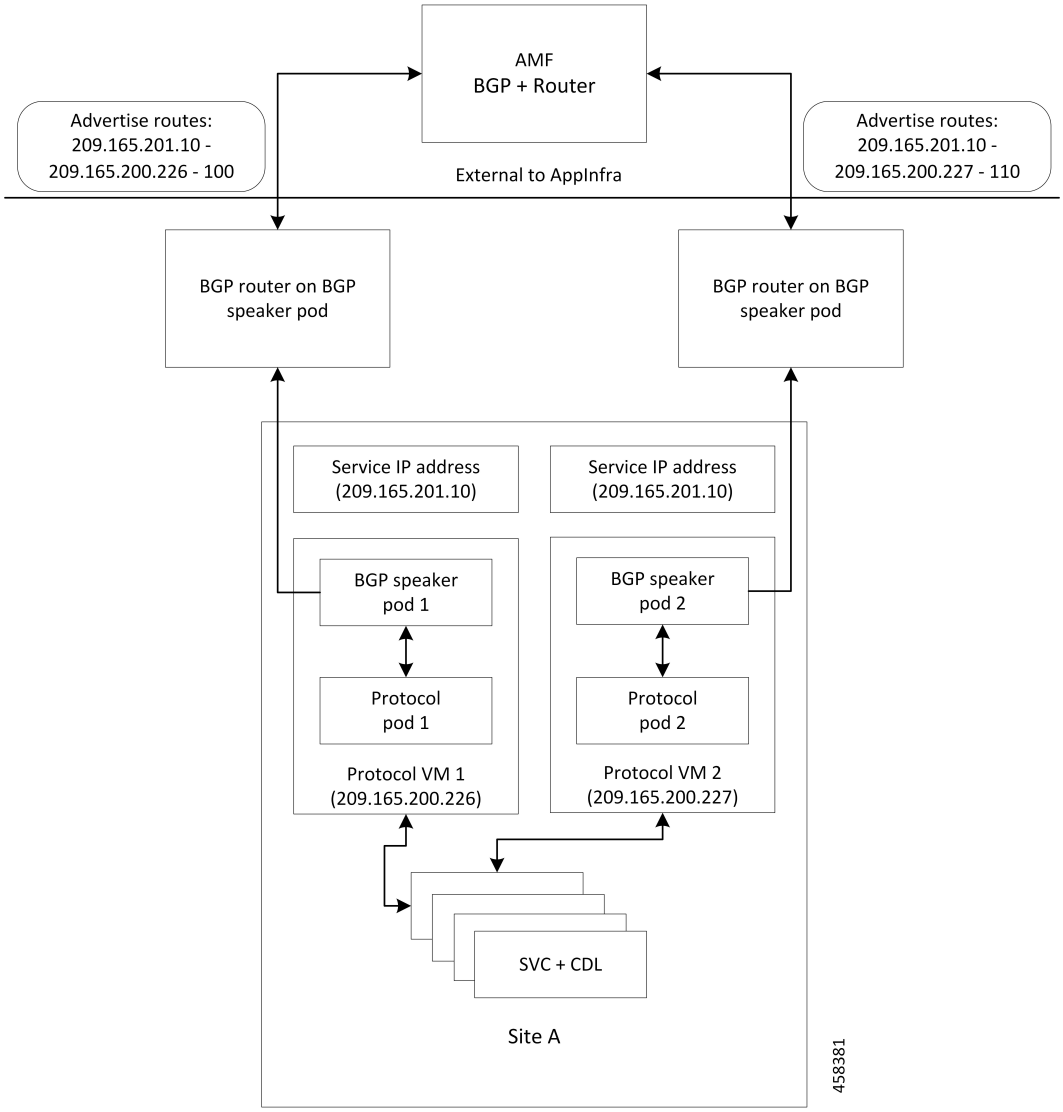
This section describes the operation of the Dynamic Routing feature.

Incoming Traffic

BGP uses TCP as the transport protocol, on port 179. Two BGP routers form a TCP connection between one another. These routers are peer routers. The peer routers exchange messages to open and confirm the connection parameters.

The BGP speaker publishes routing information of the protocol pod for incoming traffic in the active/standby mode. Use the following image as an example to understand the dynamic routing functionality. There are two protocol pods, pod1 and pod2. Pod1 is active and pod2 is in the standby mode. The service IP address, 209.165.201.10 is configured on both the nodes, 209.165.200.226 and 209.165.200.227. Pod1 is running on host 209.165.200.226 and pod2 on host 209.165.200.227. The host IP address exposes the pod services. BGP speaker publishes the route 209.165.201.10 through 209.165.200.226 and 209.165.200.227. It also publishes the preference values, 110 and 100 to determine the priority of pods.

Figure 19: Dynamic Routing for Incoming Traffic in the Active-standby Topology



For high availability, each cluster has two BGP speaker pods with active/standby topology. Kernel route modification is done at host/network level where the protocol pod runs.

MED Value

The Local Preference is used only for IGP neighbors, whereas the MED Attribute is used only for EGP neighbors. A lower MED value is the preferred choice for BGP.

Table 33: MED Value

Bonding Interface Active	VIP Present	MED Value	Local Preference
Yes	Yes	1210	2220
Yes	No	1220	2210

Bonding Interface Active	VIP Present	MED Value	Local Preference
No	Yes	1215	2215
No	No	1225	2205

Bootstrap of BGP Speaker Pods

The following sequence of steps set up the BGP speaker pods:

1. The BGP speaker pods use TCP as the transport protocol, on port 179. These pods use the AS number that is configured in the Ops Center CLI.
2. Register the Topology manager.
3. Select the Leader pod. The active speaker pod is the default choice.
4. Establish connection to all the BGP peers provided by the Ops Center CLI.
5. Publish all existing routes from ETCD.
6. Configure import policies for routing by using CLI configuration.
7. Start gRPC stream server on both the speaker pods.
8. Similar to the cache pod, two BGP speaker pods must run on each Namespace.

External Network Failure

The NF instance start-up causes the BGP Speaker K8s pod to configure the next-hop attribute of the BGP router with alternate local addresses to service IP addresses with priority and routes.

After the Geo HA is triggered, the path selection is based on the destination service IP address, path connectivity and the priority value.

Note The subscriber sessions are not impacted because of the transparent migration between pods.

Geo Switchover

The SMF achieves geo switchover by transparently migrating service IP address to mated peer K8s cluster, rack collocated, or geo-located. During the NF start-up, all the K8s cluster Namespaces register with the next-hop BGP router to advertise its service IP address and local IP address along with the priority and route modifier values.

Each logical NF exposes separate NF instance toward NRF or DNS, separate configuration, and separate LCM for a Namespace.

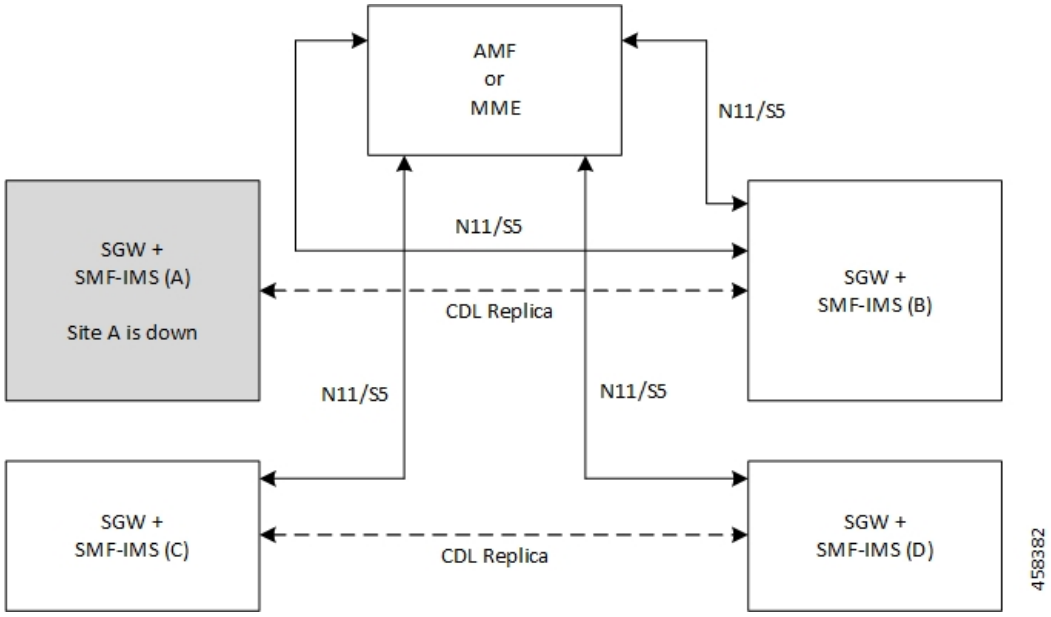
Internal Network Failure

If a functioning K8s cluster has an internal network failure due to a disrupted server communication with the master node, BFD failure, or a K8s pod networking issue, Geo HA is triggered due to K8s dependency checks that are based on the K8s liveliness failure.

In the example shown in the following figure, the AMF or MME transparently starts using the alternate rack server. The N11/S11/S5 and N4/Sxa service addresses are migrated to site B rack B. The system continues signalling from rack B for rack A. At rack B, the session continues without any impact to existing subscriber sessions.

Note Few in-transit calls might fail depending on the state where it is terminated before the UE re-attaches.

Figure 20: Geo HA for Internal Network Failure



Local Switchover

The SMF achieves geo switchover by transparently migrating service IP address to mated peer K8s cluster or rack collocated within the same data center. During the NF start-up, all the K8s cluster Namespaces register with the next-hop BGP router to advertise its service IP address and local IP address along with the priority and route modifier values. Each logical NF exposes separate NF instance toward NRF or DNS, separate configuration, and separate LCM for a Namespace.

Recovery and Failback

For a seamless failover and failback, the UE sessions and the corresponding service IP addresses are grouped together.

The following scenarios describe the seamless failover and failback mechanism for the UE sessions:

- **Normal** - The UE sessions set is created, updated, or deleted from first rack and replicated to second rack.
- **Failure** - The UE sessions set is created, updated, or deleted from second rack and is not replicated to first rack due to its unavailability.
- **Recovery** - The CDL for first rack performs an auto-sync with the CDL for second rack to recover all the UE session data. During the recovery, the second rack continues to handle traffic from the sessions set.

Call Flows

This section describes the key call flows for Dyanmic Routing by Using BGP.

Publish Route for Incoming Traffic in an Active-Standby Mode

The following sections describe the Control Plane and Data Plane call flows in an active/standby mode.

Control Plane Call Flow

This section describes the Control Plane call flow.

Figure 21: Control Plane Call Flow

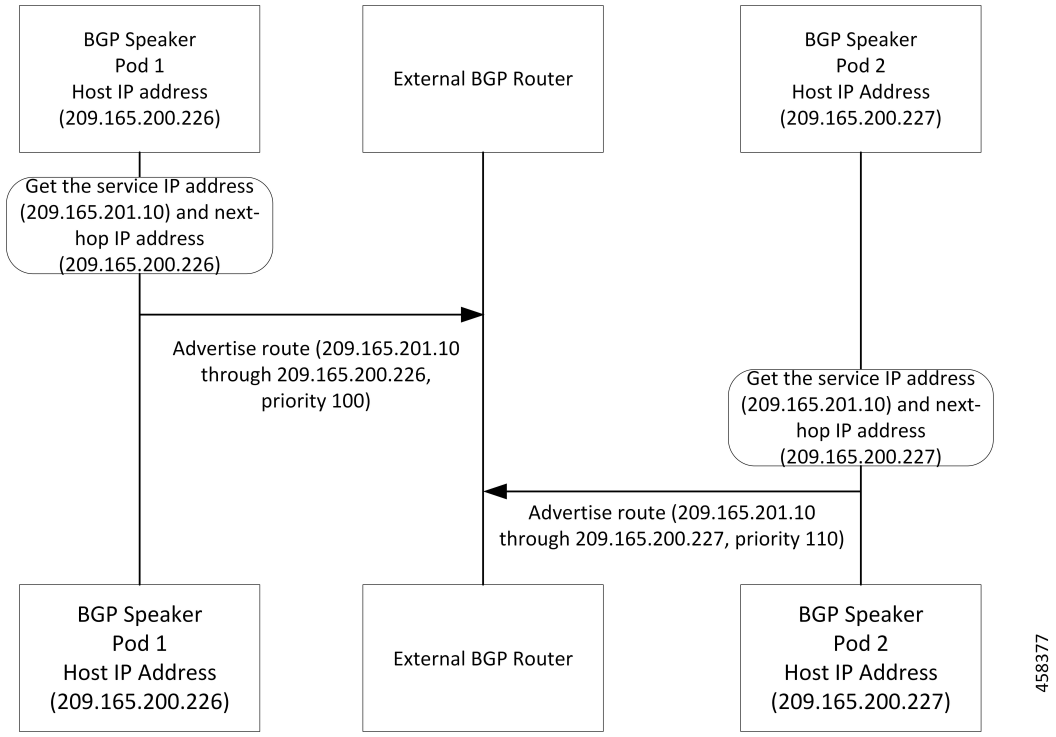


Table 34: Control Plane Call Flow Description

Step	Description
1	The BGP speaker pod starts and fetches the service IP address, next-hop IP address (host IP or loopbackEth), and the Instance ID for the BGP speaker pod. The pod service is exposed through host IP or configured loopbackEth. The NF Instance ID is used to find the route priority or preference.
2	The BGP speaker pod advertises routes by fetching vip-ip (service IP addresses) from the Ops Center.

Data Plane Call Flow

This section describes the data plane call flow.

Figure 22: Data Plane Call Flow

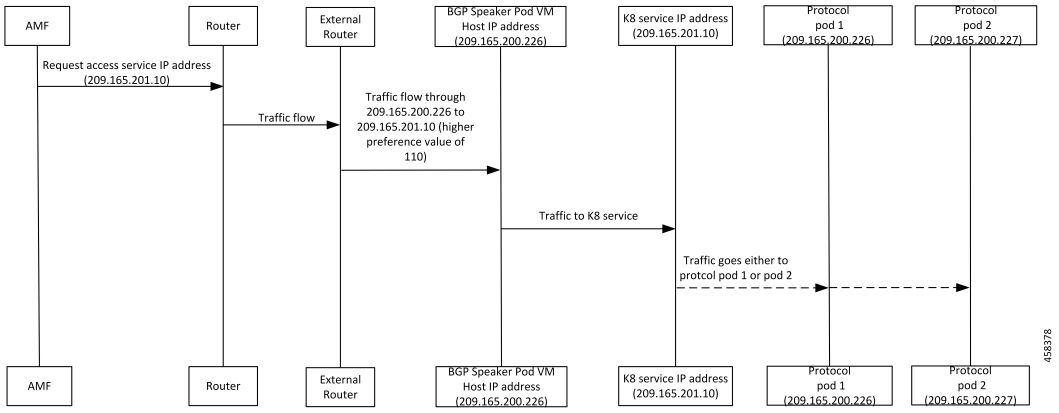


Table 35: Data Plane Call Flow Description

Step	Description
1	AMF requests for service IP address. The request is sent to the nearest connected router through multiple external routers. Then, the router sends the request to the BGP speaker pod with highest priority.
2	The BGP router sets the data plane flow based on the preference value. In the preceding call flow example, the router routes the service request through the host, 209.165.200.226 to pod 1 due to its higher preference value. From host 209.165.200.226, traffic is forwarded to the K8 service IP address, 209.165.201.10, which is then sent to either protocol pod 1 (209.165.200.226) or pod 2 (209.165.200.227).

Single Protocol Pod Failure Call Flow

The following section describes the Single Protocol Pod Failure call flow.

Figure 23: Single Protocol Pod Failure Call Flow

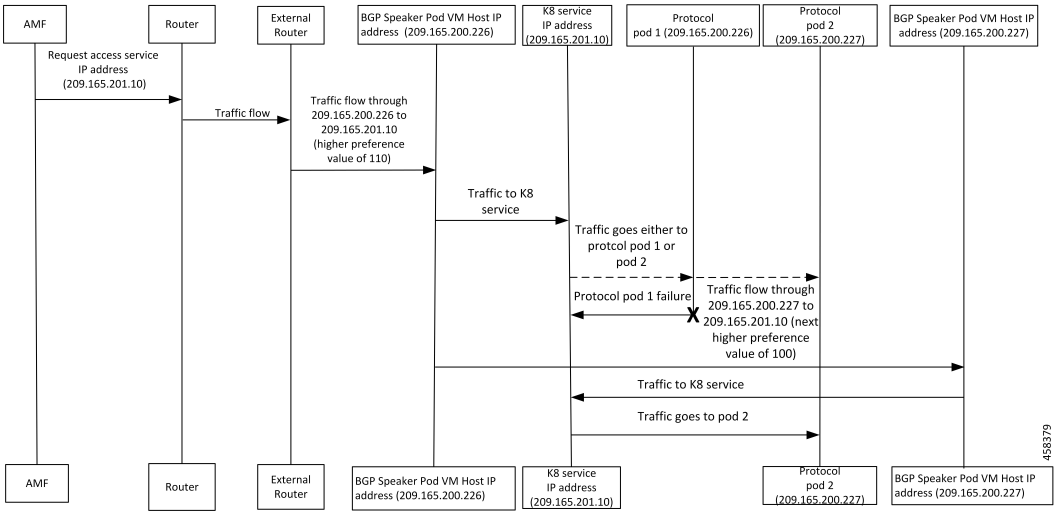


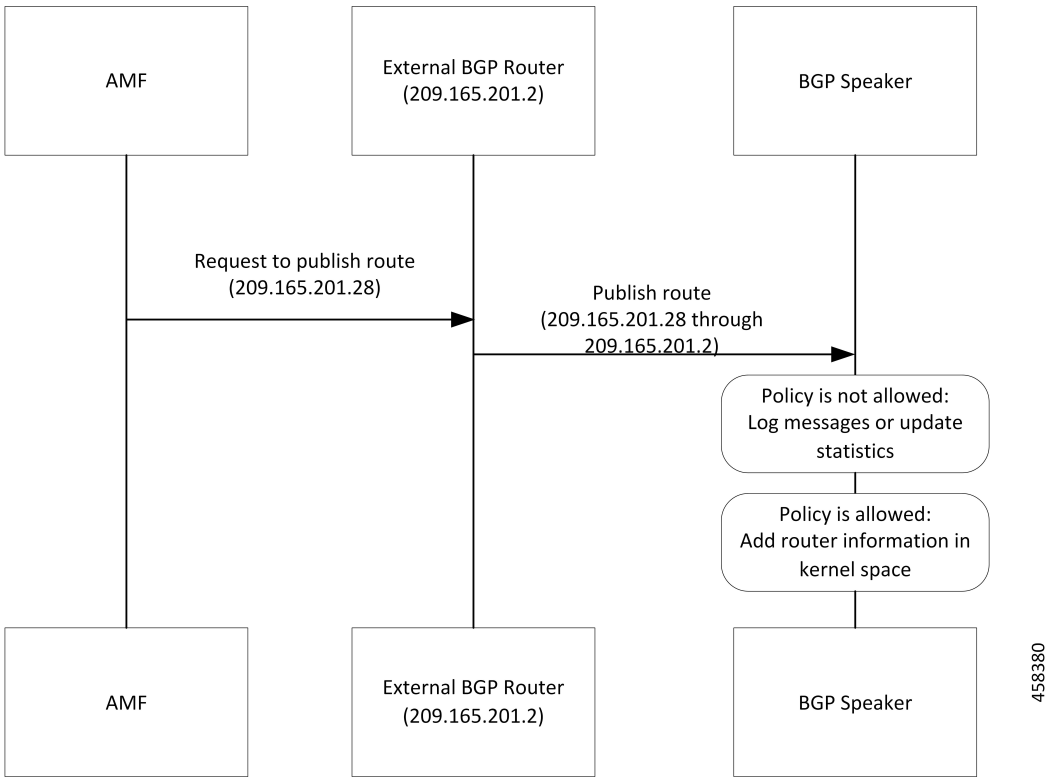
Table 36: Single Protocol Pod Failure Call Flow Description

Step	Description
1	AMF requests for service IP address. The request is sent to the nearest connected BGP router through multiple external routers based on the next highest preference value.
2	The BGP router sets the data plane flow based on the preference value. If the pod with the highest preference value is not available, then the request is routed to the pod with the next highest preference value through the K8 service pod. In the example shown in the preceding call flow figure, pod 2 with the IP address, 209.165.200.227 serves the request due to its higher preference value.

Learn Route for Outgoing Traffic Call Flow

This section describes the Learn route for outgoing traffic call flow.

Figure 24: Learn Route for Outgoing Traffic Call Flow



AMF or other systems advertise route to the external BGP route. In turn, the external BGP router advertises routes for its service through BGP.

Table 37: Learn Route for Outgoing Traffic Call Flow Description

Step	Description
1	The BGP speakers receive the routing information.
2	Learn the route by using the BGP protocol.
3	Based on the configure policy, the system either checks the routing information or ignores it.
4	If the policy is not allowed, then the system logs the messages and updates the statistics.
5	The protocol pods configures the route in Kernel space on host through the netlink go APIs.

Configuring Dynamic Routing Using BGP

This section describes how to configure the dynamic routing using BGP.

Configuring AS and BGP Router IP Address

To configure the AS and IP address for the BGP router, use the following commands:

```
config
   router bgp local_as_number
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.

Configuring BGP Service Listening IP Address

To configure the BGP service listening IP address, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.

Configuring BGP Neighbors

To configure the BGP neighbors, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
      neighbor neighbor_ip_address remote-as as_number
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.
- **neighbor** *neighbor_ip_address*—Specify the IP address of the neighbor BGP router.
- **remote-as** *as_number*—Specify the identification number for the AS.

Configuring Bonding Interface

To configure the bonding interface related to the interfaces, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
      bondingInterface interface_name
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.
- **bondingInterface** *interface_name*—Specify the related bonding interface for an interface. If the bonding interface is active, then the BGP gives a higher preference to the interface-service by providing a lower MED value.

Configuring Learn Default Route

If the user configures specific routes on their system and they need to support all routes, then they must set the **learnDefaultRoute** as **true**.

Note This configuration is optional.

To configure the Learn Default Route, use the following commands:

```
config
   router bgp local_as_number
      learnDefaultRoute true/false
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **learnDefaultRoute** *true/false*—Specify the option to enable or disable the **learnDefaultRoute** parameter. When set to true, BGP learns default route and adds it in the kernel space. By default, it is false.

Configuring BGP Port

To configure the Port number for a BGP service, use the following commands:

```
config
   router bgp local_as_number
      loopbackPort port_number
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **loopbackPort** *port_number*—Specify the port number for the BGP service. The default value is 179.

Policy Addition

The BGP speaker pods learns many route information from its neighbors. However, only a few of them are used for supporting the outgoing traffic. This is required for egress traffic handling only, when SMF is sending information outside to AMF/PCF. Routes are filtered by configuring import policies on the BGP speakers and is used to send learned routes to the protocol pods.

A sample CLI code for policy addition and the corresponding descriptions for the parameters are shown below.

```
$bgp policy <policy_Name> ip-prefix 209.165.200.225 subnet 16 masklength-range 21..24
as-path-set "^65100"
```

Table 38: Import Policies Parameters

Element	Description	Example	Optional
as-path-set	AS path value	"^65100"	Yes
ip-prefix	Prefix value	"209.165.200.225/16"	Yes
masklength-range	Range of length	"21..24"	Yes
interface	Interface to set as source IP (default is VM IP)	eth0	Yes
gateWay	Change gateway of incoming route	209.165.201.30	Yes
modifySourceIp	Modify source ip of incoming route Default value is False.	true	Yes
isStaticRoute	Flag to add static IP address into kernel route Default value is False.	true	Yes

Monitoring and Troubleshooting

This section describes the show commands that are supported by the Dynamic Routing by Using BGP feature.

show bgp-kernel-route

Use the **show bgp-kernel-route** command to view all the kernel level routes for a BGP router.

The following configuration is a sample output of the **show bgp-kernel-route** command:

```
kernel-route

-----bgpspeaker-pod-1 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.239   209.165.200.239

-----bgpspeaker-pod-2 ----

 DestinationIP       SourceIP        Gateway

 209.165.200.235     209.165.200.229   209.165.200.244
```

show bgp-global

Use the **show bgp-global** command to view all BGP global configurations.

The following configuration is a sample output of the **show bgp-global** command:

```
global-details

-----bgpspeaker-pod-1 ----
AS:        65000
Router-ID: 209.165.200.239
Listening Port: 179, Addresses: 209.165.200.239
AS:        65000
Router-ID: 209.165.200.232
Listening Port: 179, Addresses: 209.165.200.232

-----bgpspeaker-pod-2 ----
AS:        65000
Router-ID: 209.165.200.235
Listening Port: 179, Addresses: 209.165.200.235
AS:        65000
Router-ID: 209.165.200.246
Listening Port: 179, Addresses: 209.165.200.246
```

show bgp-neighbors

Use the **show bgp-neighbors** command to view all BGP neighbors for a BGP router.

The following configuration is a sample output of the **show bgp-neighbors** command:

```
neighbor-details

-----bgpspeaker-pod-2 ----
Peer             AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:34:20 Establ      |       10        10
Peer           AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:34:16 Establ      |        3         3

-----bgpspeaker-pod-1 ----
Peer             AS  Up/Down State       |#Received  Accepted
209.165.200.244 60000 00:33:53 Establ      |       10        10
Peer           AS  Up/Down State       |#Received  Accepted
209.165.200.250 60000 00:33:53 Establ      |        3         3
```

show bgp-neighbors *ip*

Use the **show bgp-neighbors** *ip* command to view details of a neighbor for a BGP router.

The following configuration is a sample output of the **show bgp-neighbors** *ip* command:

```
neighbor-details

-----bgpspeaker-pod-1 ----
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:34:50
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
```

```
                        Sent       Rcvd
    Opens:                 1          1
    Notifications:         0          0
    Updates:               1          2
    Keepalives:           70         70
    Route Refresh:         0          0
    Discarded:             0          0
    Total:                72         73
  Route statistics:
    Advertised:            0
    Received:             10
    Accepted:             10

-----bgpspeaker-pod-2 ----
BGP neighbor is 209.165.200.244, remote AS 60000
  BGP version 4, remote router ID 209.165.200.244
  BGP state = ESTABLISHED, up for 00:35:17
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                        Sent       Rcvd
    Opens:                 1          1
    Notifications:         0          0
    Updates:               1          2
    Keepalives:           71         71
    Route Refresh:         0          0
    Discarded:             0          0
    Total:                73         74
  Route statistics:
    Advertised:            0
    Received:             10
    Accepted:             10
```

show bgp-route-summary

Use the **show bgp-route-summary** command to view all the route details of a BGP router.

The following configuration is a sample output of the **show bgp-route-summary** command:

```
route-details

-----bgpspeaker-pod-1 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5

-----bgpspeaker-pod-2 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5
```

show bgp-routes

Use the **show bgp-routes** command to view all the routes for a BGP router.

The following configuration is a sample output of the **show bgp-routes** command:

```
bgp-route

-----bgpspeaker-pod-1 ----
   Network              Next Hop            AS_PATH       Age        Attrs
*> 209.165.200.235/24   209.165.200.250     60000         00:36:39   [{Origin: i} {Med:
0}]
*> 209.165.200.227/32   209.165.200.232                   00:36:44   [{Origin: e} {LocalPref:
 220} {Med: 3220}]
*> 209.165.200.247/24   209.165.200.250     60000         00:36:39   [{Origin: i} {Med:
0}]
*> 209.165.200.251/24   209.165.200.250     60000         00:36:39   [{Origin: i} {Med:
0}]
*> 209.165.200.252/32   209.165.200.232                   00:36:44   [{Origin: e} {LocalPref:
 220} {Med: 3220}]

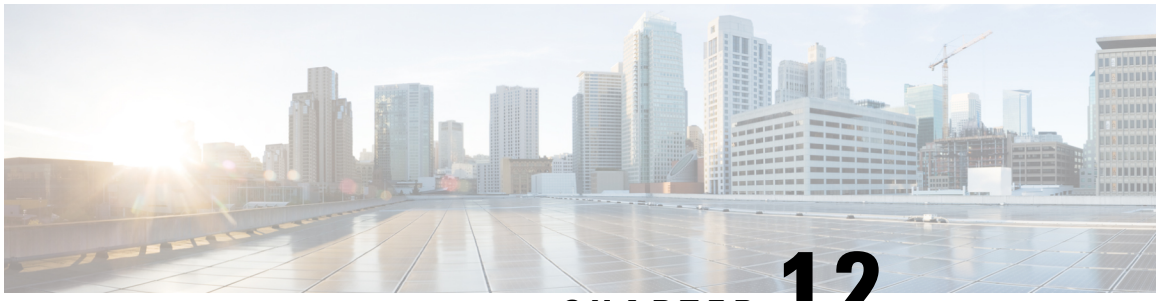
-----bgpspeaker-pod-2 ----
   Network              Next Hop            AS_PATH        Age        Attrs
*> 209.165.200.235/24   209.165.200.250     60000          00:37:02   [{Origin: i} {Med:
0}]
*> 209.165.200.227/32   209.165.200.246                    00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
*> 209.165.200.228/24   209.165.200.234     60000          00:37:02   [{Origin: i} {Med:
0}]
*> 209.165.200.229/24   209.165.200.234     60000          00:37:02   [{Origin: i} {Med:
0}]
*> 209.165.200.230/32   209.165.200.246                    00:37:11   [{Origin: e}
{LocalPref: 220} {Med: 3220}]
```

KPIs

The following KPIs are supported for this feature:

Table 39: Statistics for Dynamic Routing by Using BGP

KPI Name	Type	Description/Formula	Label
bgp_outgoing_route request_total	Counter	Total number of outgoing routes.	local_pref, med, next_hope, service_IP
bgp_outgoing_failedroute request_total	Counter	Total number of failed outgoing routes.	local_pref, med, next_hope, service_IP
bgp_incoming_route request_total	Counter	Total number of incoming routes.	interface, next_hope, service_IP
bgp_incoming_failedroute request_total	Counter	Total number of failed incoming routes.	interface, next_hope, service_IP
bgp_peers_total	Counter	Total number of peers added.	peer_ip, as_path
bgp_failed_peerstotal	Counter	Total number of failed peers.	peer_ip, as_path, error



CHAPTER 12

Emergency SoS Support

- Feature Summary and Revision History, on page 155
- SoS Emergency Service Fallback to LTE, on page 156
- Emergency Services Support, on page 160

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 40: Revision History

Revision Details	Release
First introduced.	2020.02.5.t1

SoS Emergency Service Fallback to LTE

Feature Description

The Emergency SoS Support feature enables the co-located cloud-native SMF and PGW-C to support SoS emergency over LTE for subscribers camped on the 4G network and SoS emergency service fallback to LTE for subscribers camped on the 5G network.

The Emergency SoS Support feature supports the following functionalities:

- Provides a new configuration to skip UDM interaction.
- Enables an emergency PDN connection creation in 4G (LTE) for PGW-C.
- Supports emergency service fallback to LTE requirement for SMF serving subscriber in NR.
- Supports interworking with an existing charging interface failure handling to ‘continue’ emergency call creation upon failure.
- Supports interworking with an existing secondary authentication using radius to skip radius authentication for emergency calls when not configured.
- Provides inter-RAT handover support (4G to 5G and 5G to 4G) for EPS interworking capable subscribers.

How it Works

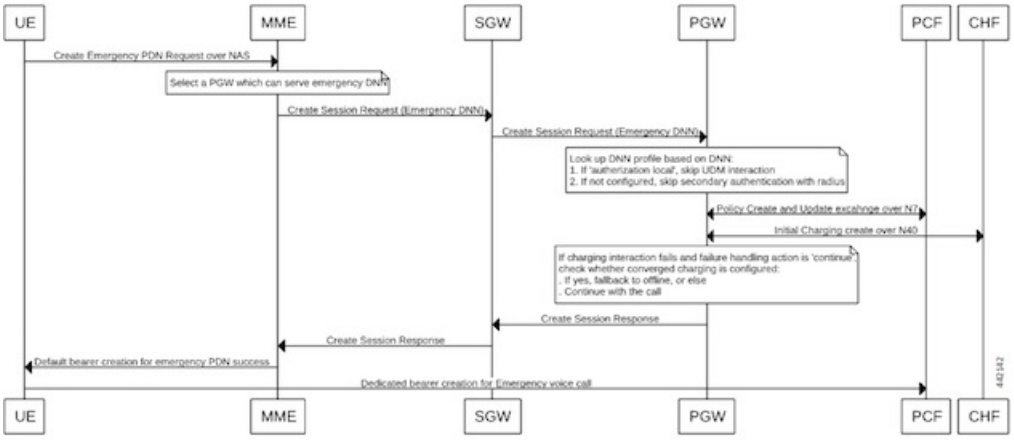
This section provides a brief of how the Emergency SoS Support feature works.

Call Flows

This section includes the following call flows.

Emergency Session Creation in LTE Call Flow

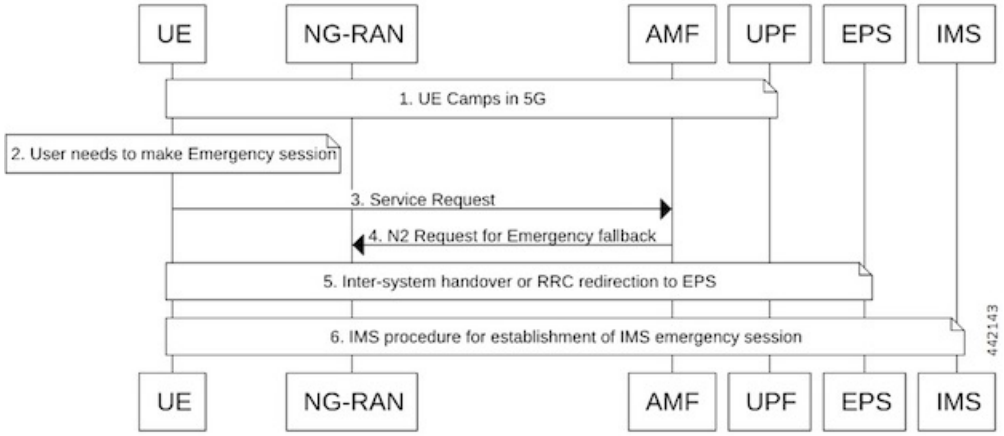
Figure 25: Emergency Session Creation in LTE



Step	Description
1	When an emergency service is required and an emergency PDU session is not already established, the UE initiates the UE-requested PDU session establishment procedure with a request type indicating, "Emergency Request" in LTE.
2	The MME selects an APN or DNN for the emergency PDN creation, and sends a ‘Create Session Request’ to the PGW-C via the S-GW.
3	The DNN profile lookup at PGW-C is based on the subscriber policy or DNN policy. These policies are associated in the SMF profile. The subscriber policy has higher precedence over DNN policy when both the configurations are present.
4	The DNN policy can have the DNN profile configuration for each of the UE-requested APN or DNN received in the “Create Session Request” from the MME or S-GW.
5	When a new configuration ‘authorization local’ under the selected DNN profile is present: • PGW-C skips the UDM interaction for fetch subscription and uses the values received in the ‘Create Session Request’ message from the MME. • PGW-C skips the UDM interaction to ‘Subscribe-for-Notification’ from the UDM.
6	When the ‘Secondary Authentication Radius’ under the selected DNN profile is not present, the PGW-C rejects the RADIUS-based secondary authentication.
7	When ‘failure handling’ for charging interaction is set as ‘action continue’: • PGW-C continues the call if converged charging is not configured. • PGW-C falls back to offline charging and continues the call.
8	During handover from 4G to 5G using N26, if the emergency PDN gets handed over, the SMF checks the DNN profile and if ‘authentication local’ is present, it skips the UDM interactions for registration and deregistration.

Emergency Services Fallback to LTE Call Flow

Figure 26: Emergency Services Fallback to LTE



Step	Description
1	UE camps on E-UTRA or NR cell in the 5GS (in either CM_IDLE or CM_CONNECTED state).
2	UE has a pending IMS emergency session request (example, voice) from the upper layers.
3	If the AMF has indicated support for emergency services using fallback via the "Registration Accept" message for the current RAT, the UE sends a "Service Request" message indicating that it requires an emergency services fallback.
4	The 5GC executes an NG-AP procedure in which it indicates to the NG-RAN that this is a fallback for emergency services. This procedure triggers the "Emergency Services Fallback" request. Currently the Cisco SMF and PGW-C supports Emergency Services in the EPC core Network (LTE). The AMF includes the EPC as a target CN to trigger inter-RAT fallback. When the AMF initiates the redirection for UEs that are successfully authenticated, AMF includes the security context in the request to trigger fallback towards the NG-RAN.
5	The NG-RAN initiates the handover or redirection to the E-UTRAN connected to the EPS (N26 interface based handover or redirection procedure). The NG-RAN uses the security context that the AMF to secure the redirection procedure. If the redirection procedure is used, the target CN is also conveyed to the UE to enable it to perform the S1 mode NAS procedures. The UE uses the emergency indication in the RRC message and E-UTRAN provides the emergency indication to the MME during the "Tracking Area Update".
6	After handover to the target cell, the UE establishes a PDU session or PDN connection for IMS emergency services and performs the IMS procedures for establishment of an IMS emergency session (example, voice).

Configuring Emergency SoS Support

This section describes how to configure the Emergency SoS Support feature.

Configuring the Emergency SoS Support involves the following steps:

- Local authorization configuration under DNN profile
- Secondary authentication configuration under DNN profile
- Charging failure handling configuration under Charging profile

Configuring Local Authorization

Use the following sample configuration to configure local authorization under the DNN profile, use the following commands:

```
config
  profile dnn pool_name
     [ no ] authorization local
     end
```

NOTES:

- **profile dnn**: Specifies the DNN profile name. *profile_name* must be an alphanumeric string.

- **no**: Disables the local authorization under the DNN profile.

Configuring Secondary Authentication

Use the following sample configuration to configure secondary authentication under the DNN profile:

```
config
  profile dnn pool_name
     [ no ] secondary authentication radius
     end
```

NOTES:

- **no**: Disables the secondary authentication under the DNN profile.
- **secondary authentication**: Enables secondary-authentication under the DNN profile and sets method as RADIUS.
- **radius**: Specifies RADIUS for secondary authentication.

Configuring Charging Failure Handling

To configure failure handling action for both converged charging and offline charging failure cases under the charging profile, use the following sample configuration:

```
config
  profile network-element chf charging_profile_name
     nf-client-profile offline_charging_profile_name
     failure-handling-profile failure_handling_profile_name
     end
```

NOTES:

- **profile network-element chf** *charging_profile_name*: Specify the charging function (CHF) as the network element profile. *charging_profile_name* must an alphanumeric string representing the corresponding network element profile name.
- **nf-client-profile** *offline_charging_profile_name*: Specify the local NF client profile.*offline_charging_profile_name* must an alphanumeric string representing the corresponding NF client profile name.
- **failure-handling-profile** *failure_handling_profile_name*: Specify the NRF failure handling network profile for the configured NF type. *failure_handling_profile-name* must an alphanumeric string representing the corresponding NRF failure handling network profile name.

Configuration Example

The following is an example configuration of the failure handling action for converged charging:

```
profile nf-client-failure nf-type chf
profile failure-handling fh1
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
```

Emergency Services Support

Feature Description

Emergency Services refer to functionalities provided by the serving network when the network is configured to support Emergency Services. Emergency Services are provided to support IMS emergency sessions.

To implement IMS emergency services in 4G and 5G, the SMF performs the following functions:

- Identifies 5G emergency session based on Request Type in SmContextCreate message or emergency configuration in DNN.
- Identifies 4G emergency session based on emergency configuration in DNN.
- Interacts with UDM if SUPI/IMSI is authenticated and **authorization local** command is not configured in the DNN profile. Else, skips the interaction with UDM.
- Enables PDU session establishment for Emergency Services with PEI or IMEI.
- Employs a new configuration to classify DNN as an Emergency DNN.
- Configures P-CSCF profile for Emergency Services
- Configures UPF for Emergency Services
- Configures default QoS profile for Emergency Services and flow-only timer used during tear down of dedicated bearer from PCF.

How it Works

Identification of Emergency Service Sessions

5G

SMF identifies the emergency session based on request type "Initial Emergency Request" or "Existing Emergency PDU Session" received in SmContextCreate Message from AMF or if the DNN is configured as an Emergency DNN.

4G

SMF identifies the emergency session based on the authentication status of IMSI. If the IMSI is unauthenticated (UIMSI is set to 1), the session is considered as an emergency session.

If IMSI is authenticated (UIMSI is set to 0), and DNN is configured as an emergency DNN (using new CLI) in SMF, the session is identified as an emergency session.

- For non-emergency session, SUPI or IMSI is mandatory.
- For emergency session:
  - For an authenticated SUPI or IMSI, SUPI or IMSI is used as the session-key based on the current implementation.
  - For an unauthenticated SUPI or IMSI, PEI or IMEI is always used as the session-key, If PEI or IMEI is not present, then the call is rejected.

UDM Interaction for Emergency Sessions

1. SMF skips UDM interaction if SUPI or IMSI is unauthenticated.
2. SMF skips UDM interaction if SUPI/IMSI is authenticated and if “authorization” in DNN configuration is set to “local”.
3. SMF interacts with UDM if SUPI or IMSI is authenticated and if “authorization” in DNN configuration is not set to local.
   - If UDM rejects, then the call will be rejected.
   - If UDM exchanges fail, further handling is done based on UDM failure handling template provisioning.

Important SMF does not consider whether “authorization local” is configured in DNN profile or not.

Configuring Emergency Sessions

1. Existing DNN, P-CSCF, UPF, and QoS Profile configuration works for emergency sessions.
2. Use CLI classify a DNN as Emergency DNN.
3. If "**authorization**" is set (using CLI) to local under DNN, UDM interaction is not required.
4. Use default Flow Only timer configuration to retain the default bearer to enable PSAP Callback session.

Support for Emergency Services if Request Type is “Existing Emergency PDU Session”

1. If the request type indicates "Existing Emergency PDU Session", the SMF determines that the request is HO from EPS (4G and WiFi). Current implementation supports emergency sessions mobility in WiFi to 5G HO using request type as “Existing Emergency PDU Session” and in 4G to 5G HO using N26 interface.
2. The SMF identifies the existing PDU session based on the PDU Session ID.
3. SMF updates the existing SM context to provide the representation of the updated SM context to the AMF in the response instead of creating new SM, which is equivalent to handling of “Existing PDU Session”.

Default Flow Only Timer for an Emergency Service (Dedicated Bearer)

At reception of an HTTP POST message that removes one or several PCC Rules from a PDU Session restricted to emergency services:

- When all PCC Rules bound to a QoS flow are removed, SMF initiates a QoS flow termination procedure.
- When not all PCC Rules bound to a QoS flow are removed, SMF initiates QoS flow modification procedure.

In addition, the SMF initiates a default flow only if timer if all PCC Rules with a 5QI other than the 5QI of the default QoS flow or the 5QI used for IMS signalling are removed from the PDU session restricted to Emergency Services (example - to enable public safety answering point (PSAP) Callback session). When the default flow only timer expires, the SMF initiates a PDU session termination procedure.

1. The SMF initiates default flow only timer when a PCF initiated modify procedure removes a dedicated bearer(voice/video). The main intension of this timer is to hold the emergency session for some more time to facilitate a PSAP callback.
2. When default flow only timer expires, the PCEF initiates termination of the IMS Emergency session.
3. The SMF stops the default flow only timer on receiving a PCF-initiated modification request for creating a new bearer.

EPS FB

If gNB rejects the QFI and EPS fall back is armed. SMf performs the EPS fallback as a it is done for a normal non-emergency session.

Use of PEI as Session Key

SMF uses PEI as session key if SUPI is not present or it is not authenticated. Following conditions must be met for PduContext on SMF:

1. The REST-EP, when the message is received, checks affinity based on SUPI and PEI. First lookup will be done with SUPI. If it fails, checks with the PEI.

   Or

   Both SUPI and PEI keys can be looked up.
2. When Smf-Service chooses PEI as key, it sets affinity in cache-pod using PEI.
3. When Smf-Service inserts CDL record using PEI as key, PEI will be added as Primary Key type. Either Primary key is SUPI+PduSessionid or PEI+PduSessionID.
4. After first transaction, CDL lookup will happen both with SUPI or PEI which ever is available.
5. SEID is generated using PEI hashing.

Configuring Emergency Service Support

This section describes how to configure Emergency Service Support.

Configuring Default Flow Only Timer in DNN Profile

Use the following sample configuration to configure Default Flow Only Timer:

```
config
   profile dnn profile_name
      timeout default-flow-only flow_only_timer
     end
```

NOTES:

- **timeout default-flow-only** *flow_only_timer* : Maximum allowed idle duration for a PDU/PDN session before system automatically terminates it. *flow_only_timer* must be an integer between 0 and 2147483647 milli seconds. Default is 0, which indicates the function is disabled.

Configuring Emergency DNN

Use the following sample configuration to configure Emergency DNN:

```
config
   profile dnn profile_name
     emergency { false | true }
     end
```

NOTES:

- **emergency {** *false* | *true* **}**: indicates whether dnn is emergency DNN or not, *false* | *true* must be false or true, default is false.

Verifying Emergency DNN

Use the following show command to verify Emergency DNN configuration:

```
show subscriber all
```

The following is an example output of the **show subscriber all** command.

```
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-9999988888",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "udm-uecm:209.165.202.131",
      "udm-sdm:209.165.202.151",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.225",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.225",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ],
    [
      "gpsi:msisdn-9999988888",
      "pei:imei-352099001761480",
      "psid:6",
      "dnn:intershat",
      "emergency:true",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "pcfGroupId:PCF-dnn=;",
      "pcf:209.165.202.151",
      "policy:2",
      "upf:209.165.202.151",
```

```
      "upfEpKey:209.165.202.151:209.165.202.150",
      "ipv4-addr:poolv4/209.165.200.234",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.200.225",
      "ipv4-startrange:poolv4/209.165.200.234",
      "amf:209.165.202.151",
      "peerGtpuEpKey:209.165.202.151:209.165.202.158"
    ]
  ]
}
```

Use the value of "emergency" to determine if the emergency services feature is enabled or disabled for the subscriber.

OAM Support for Emergency Services

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The following statistics are supported for the Emergency SoS Support feature.

- smf_session_counters: Indicates that the gauge is updated to show the number of current active sessions.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

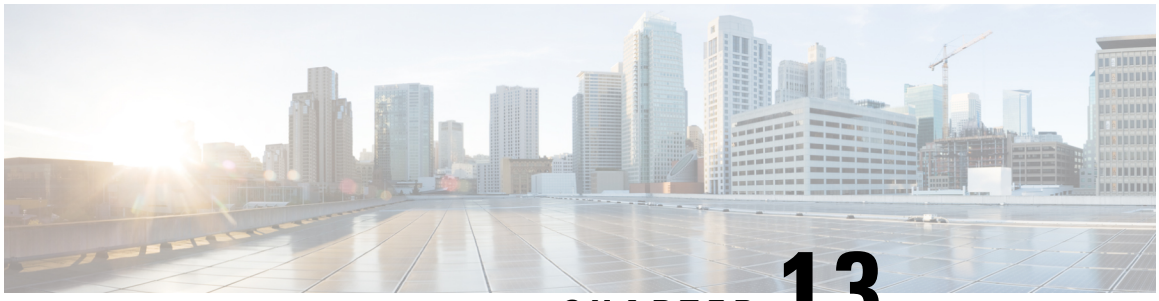
- smf_service_stats: Indicates the SMF call flow procedure counters.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

- smf_service_resource_mgmt_stats: Indicates the SMF Service Resource Management Statistics.

  This statistics includes "emergency_call" label. If the flag for this label is set to true, it indicates that it is an emergency call.

For information on bulk statistics support for SMF, see the *UCC 5G SMF Metrics Reference*.



CHAPTER 13

EPS Interworking

- Feature Summary and Revision History, on page 165
- Feature Description, on page 167
- Architecture, on page 168
- How it Works, on page 170
- Standards Compliance, on page 171
- Support for UE Initial Attach , on page 172
- Detach Procedure for EPS on SMF, on page 182
- Dedicated Bearer Activation and Deactivation, on page 191
- EPS Fallback, on page 198
- Indirect Data Forwarding Tunnel (IDFT) Timer Support, on page 201
- EPS Fallback Guard Timer Support, on page 206
- Generating EPS Fallback Report, on page 209
- Bearer Modification for EPS Session on SMF, on page 212
- Session Management Procedures for EPS and 5GC Interworking, on page 227
- 5G to EPS Handover Using N26 Interface, on page 251
- Create Dedicated Bearer Delay and Retry Support, on page 254
- Handling Dedicated Bearer Procedure Failures Caused by Timer Expiry, on page 257
- Handling GTP-U Error Indication for 4G Sessions, on page 265
- GTP Path Failure Handling, Restoration, and Recovery, on page 267
- Configuration Support for Rejecting 4G-only Devices, on page 273
- Change Notification Request Handling, on page 274
- Dynamic Configuration Change Support, on page 279
- Semantic and Syntactic Error Handling for 4G and 5G, on page 281

Feature Summary and Revision History

Summary Data

Table 41: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI

Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 42: Revision History

Revision Details	Release
Added the following support: • Receiving QoS rules and QoS descriptions with the ePCO length of two octets option in PDU session establishment. • Indication of local IP address in TFT in S1 node during the PDU session establishment in 5G for a PDU session supporting 5G-4G internetworking. • Semantic and syntactic error handling for the QoS rules and Qos description or for mapped EPS Bearer Contexts errors from the UE. • Handles CB or UB response with ePCO containing 5GSM cause. • Mandatory MFBR validation while receiving GBR flow creation or QoS Modification from PCF. • HSS-initiated QoS modification for 4G UE.	2023.04.0
Added the following support: • For the change notification request received with ULI for 4G calls with legacy interfaces. • The alternate RAT tunnel creation for 4G. • Added the Show command for 4G call for the change in output of RAT Type.	2023.03.0
Added support for: • E-UTRAN initial attach procedure with Diameter interfaces. • Network-initiated Detach Procedures with Diameter Interfaces • PCRF-initiated CCAU or RAR • Modify Bearer Request with or without S-GW Change • UE-Initiated Detach Procedure • Support for Context Replacement	2023.02.0
FB Call Continuity Cause Code Expansion	2021.02.2

Revision Details	Release
Added support for: • Configuring APN-AMBR action in Create Session Response • Container field—0005H (Selected Bearer Control Mode) for the PCO, ePCO, or aPCO IE in Create Session Response • GTP-C path failure detection and debugging improvements • GTP-C peer restart detection improvements • Handling the dedicated bearer procedure failures observed at the expiry of procedure SLA timer	2021.02.0
Introduced procedure to support dynamic configuration of the Access Profile configuration.	2020.03.0
New CLI command in the DNN profile configuration to reject calls from 4G-only UE devices.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

Important The PGW-C term used in this chapter denotes the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

EPS Interworking through 5G Core Network

The SMF implements the 3GPP recommendations for interworking of Evolved Packet System (EPS) and 5G Core Network (5GC).

The UEs capable of supporting both 4G and 5G NAS connect to the Evolved Terrestrial Radio Access Network (E-UTRAN) and the 5GC network. The SMF with the EPS interworking capability acts as a SMF and uses the S5 or S8 interface with S-GW to receive the 4G Session Creation Request. All the other interfaces involved in the 4G Session Creation (for example, Gx, Gy, Gz, and so on) are replaced by the corresponding 5GC Service Based Interfaces (for example, Npcf and Nchf).

After a PDU session is created on the SMF with E-UTRAN, Mobility Management Entity (MME) and Serving Gateway (S-GW), the UE can hand over E-UTRAN to 5G New Radio (NR) and conversely.

The SMF uses the N26 interface to interwork with EPS. This interface is an inter-CN interface between the MME and AMF and supports a subset of the functionalities over S10 interface to enable interworking.

The UE uses EPC NAS or 5GC NAS procedures depending on the core network by which it's served.

SMF Interworking with Diameter Interfaces

The Converged Core deployment allows signaling from a 4G subscriber. The SMF implements the 3GPP recommendations for interworking of Evolved Packet System (EPS) and Diameter Interfaces such as Gx for Policy, Gy for OCS, and Gz for offline charging. It also supports RADIUS authentication and accounting for

subscribers. The signaling call flows and Pod level communications along with communication over various 3GPP interfaces is limited with only E-UTRAN access types.

Following are the SMF Diameter Interface call flow procedures for E-UTRAN access types:

- Initial Attach on E-UTRAN with Diameter Interfaces , on page 175
- E-UTRAN PDN Modification with S-GW Change
- E-UTRAN PDN Modification without S-GW Change
- PCRF-Initiated RAR / CCAU
- Network-initiated Detach Procedures with Diameter Interfaces
- UE Initiated Detach Procedure

Note It should not be assumed that the Diameter interface features available on the SMF have full feature parity and functionality with StarOS or CUPS product.

Furthermore, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with StarOS legacy or CUPS products.

Please contact your Cisco Account or Support representative for any questions about parity between this product and any StarOS legacy or CUPS products.

Alternate RAT Tunnel Creation for 4G

SMF creates an alternate RAT tunnel during 4G sessions for 4G attach and dedicated bearer procedures. This tunnel is reused when a subscriber moves to another RAT during handover.

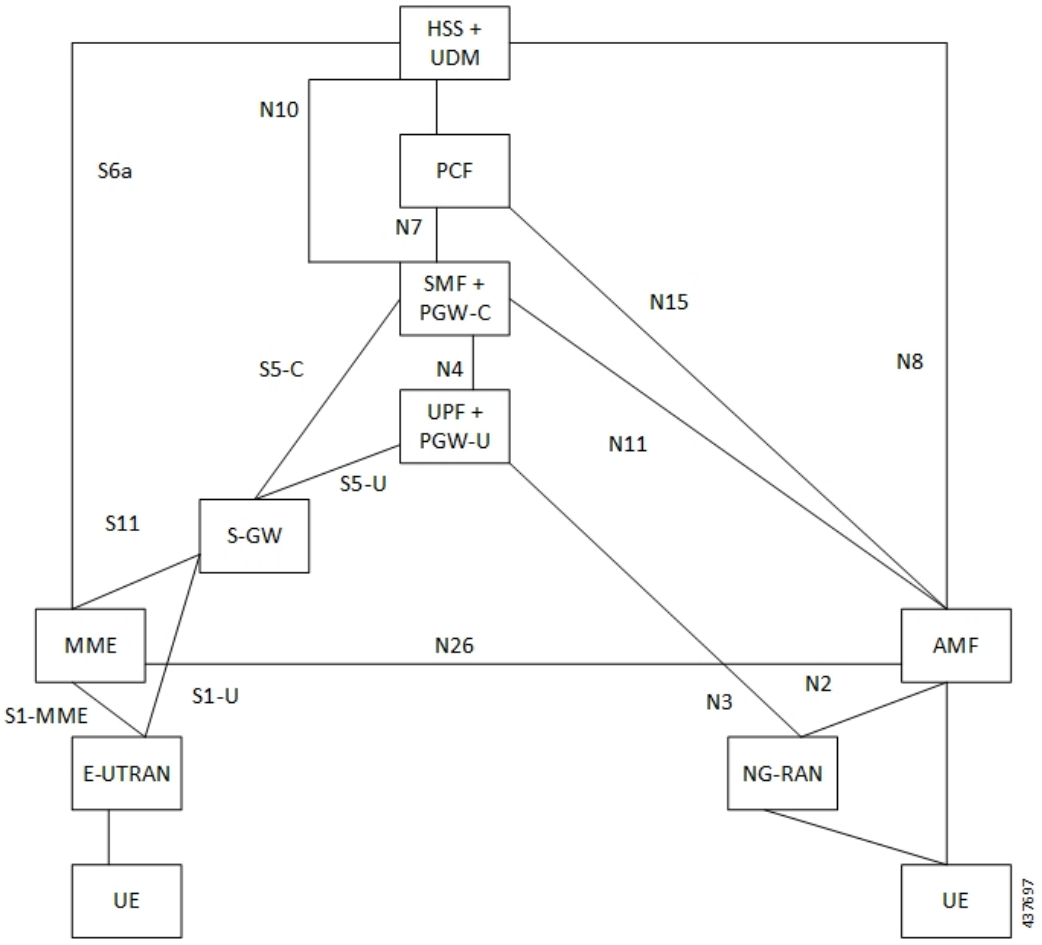
Note

- Creation of an alternate RAT tunnel is a prerequisite for the inter-PLMN handover support.
- SMF allocates an alternate RAT tunnel only if the EPS interworking is enabled.
- SMF doesn't allocate the alternate RAT tunnel for 4G only UEs during 4G attach.

Architecture

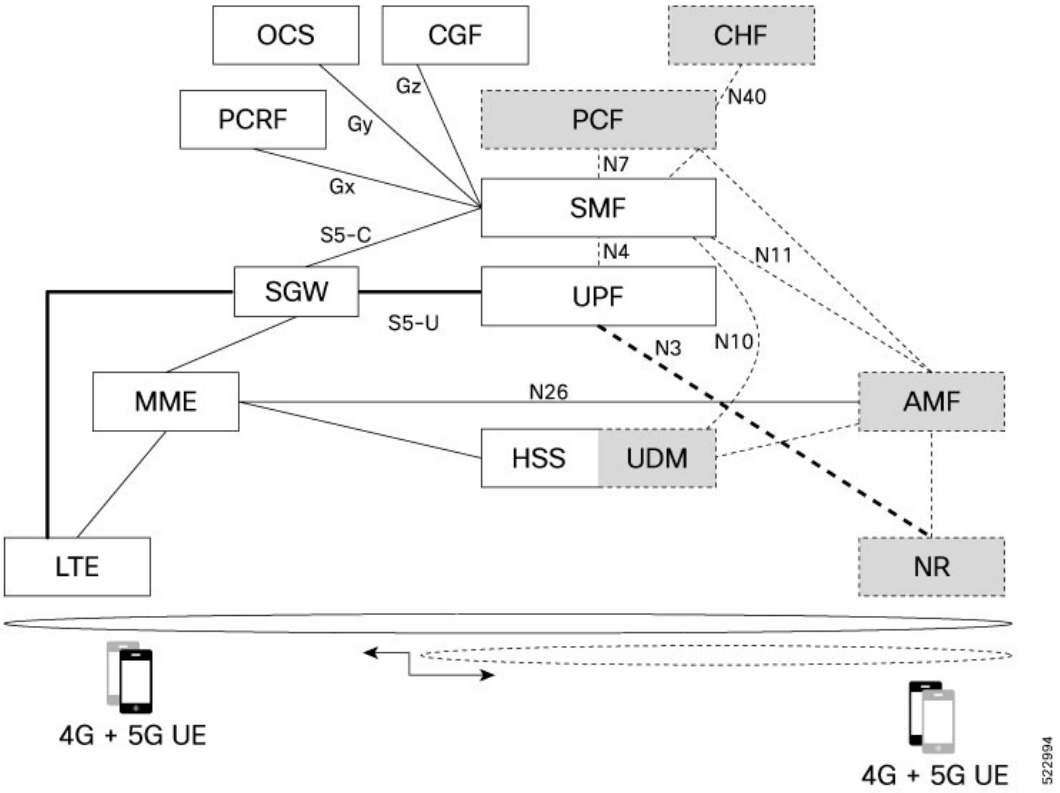
The following figure shows the network architecture for the EPS-5G Core and 4G interworking.

Figure 27: 3GPP Non-Roaming Architecture for EPS-5GC Interworking



The following architecture diagram shows that SMF using Diameter interfaces for Policy and online charging and the Gz for the offline charging. It uses the N4 interface towards the UPF. In this architecture diagram, the grayed element are the 5G nodes that are not used for the 4G only UE.

Figure 28: SMF Interworking with Diameter and GTPP Interfaces



How it Works

Table 43: Feature History

Feature Name	Release Information	Description
Support for ePCO length and Local IP in TFT	2023.04	SMF allows ePCO length with two octets for QoS rules and QoS descriptions and indicate local IP address in TFT. **Default Setting**: Enabled – Always-on

A UE that supports only EPS based Dual Connectivity with secondary RAT NR:

- Always performs initial access through E-UTRA (LTE-Uu) but never through NR.
- Performs EPS NAS procedures over E-UTRA (that is, Mobility Management, Session Management and so on) as defined in 3GPP TS 24.301.

A UE that supports camping on 5G Systems with 5GC NAS:

- Performs initial access either through E-UTRAN that connects to 5GC or through NR towards 5GC.

- Performs initial access through E-UTRAN towards EPS, if supported and needed.
- Performs EPS NAS or 5GC NAS procedures over E-UTRAN or NR respectively (that is, Mobility Management, Session Management, and so on) depending on whether the UE requests 5GC access or EPS access, if the UE also supports EPS NAS.

For interworking with EPS, the UE that supports both 5GC and EPS NAS can operate in one of the following modes:

- Single-registration mode: UE has only one active MM state (either RM state in 5GC or EMM state in EPS) and it is either in 5GC NAS mode or in EPS NAS mode (when connected to 5GC or EPS, respectively).
- Dual-registration mode: UE handles independent registrations for 5GC and EPS using separate RRC connections. In this mode, the UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

Networks that support interworking with EPS, may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface.

- Interworking procedures with N26 support provide IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPS NAS and that operate in single registration mode. Interworking procedures using the N26 interface, enables the exchange of MM and SM states between the source and target network.
- Networks that support interworking procedures without N26 support procedures to provide IP address continuity on inter-system mobility to UEs operating in both single-registration mode and dual-registration mode. For interworking without the N26 interface, IP address preservation is provided to the UEs on inter-system mobility by storing and fetching PGW-C+SMF and corresponding APN or DNN information via the HSS+UDM.
- The UE operating in the S1 mode in a network supporting N26 interface also indicates the support for local IP address in TFT during the PDU session establishment procedure in 5G for supporting interworking with EPS.

Important Interworking of SMF and EPS currently works only with the N26 interface.

Standards Compliance

The 5GC and EPS Interworking feature complies with the following standards:

- *3GPP TS 23.401, Version 15.6.0*
- *3GPP TS 23.501, Version 15.4.0*
- *3GPP TS 23.502, Version 15.4.0*
- *3GPP TS 29.502, Version 15.2.1*
- *3GPP TS 29.512, Version 15.2.0*
- *3GPP TS 23.401, Version 5.3.2.1*

Support for UE Initial Attach

Feature Description

The SMF supports the UE performing initial attach on E-UTRAN through MME and S-GW to create the default bearer.

Initial attach on E-UTRAN or EPS follows the procedure defined in 3GPP specification 23.401, Section 5.3.2.1. There are few deviations from the defined procedure to enable connectivity through the 5G core or Legacy GW. The deviations are as follows:

- The Packet Data Network Gateway (PGW-C) in the procedure is replaced by SMF.
- The IP-CAN Session establishment and modification is replaced by SM Policy Association Establishment procedure.
- The online and offline charging functionality using Gy and Gz interfaces is replaced by integrated charging over Nchf interface with Charging Function (CHF).
- The interface with the user-plane node is through N4 interface instead of Sxb interface.

SMF Interworking with Diameter Interfaces

The UE supports E-UTRAN Initial Attach procedures for Diameter interfaces as described in 5.3.2.1, 23.401 with following functions:

- Default EPS bearer establishment.
- Activate predefined PCEF rules with SMF as the Gx reference point is situated between the PCRF and the SMF. It is used for provisioning and removal of PCC rules. The Gx interface functions as a diameter connection. The Gx messages involve installing or removing dynamic rules and activating or deactivating predefined rules, APN-AMBR, and Default Bearer QoS.

How it Works

Call Flows

Initial Attach on E-UTRAN or EPS Procedure

The following figure shows the call flow derived from 3GPP reference for initial attach on E-UTRAN or EPS.

Figure 29: Call Flow for Initial Attach on E-UTRAN via 5G Core

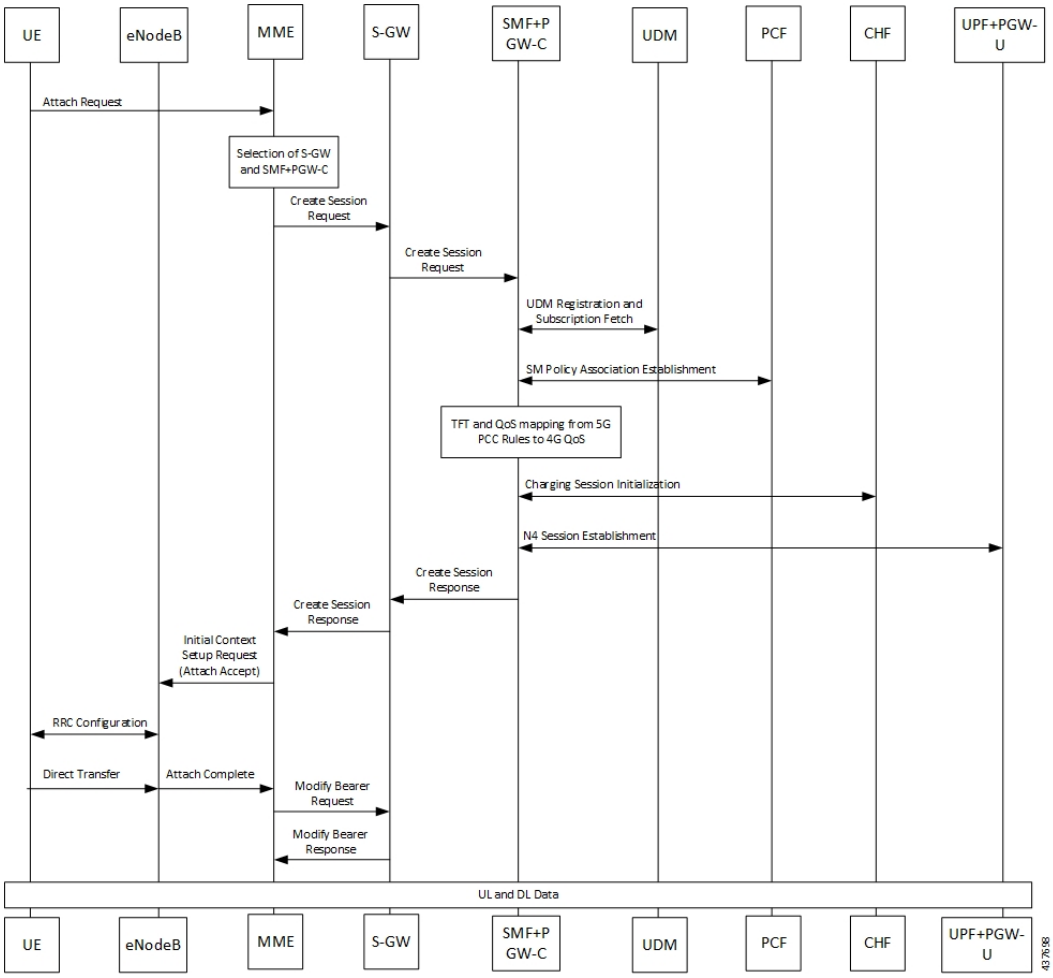


Table 44: Call Flow Description for Initial Attach on E-UTRAN via 5G Core

Step	Description
1	UE sends Attach Request to the MME through eNodeB.
2	The MME determines that the UE is capable and subscribed for handoff to NR. It selects an SMF node as the PGW-C for this PDU session.
3	The MME sends Create Session Request to the selected S-GW and includes the selected SMF address in it.
4	The S-GW initiates Create Session Request towards the SMF.
5	The SMF extracts the PDU Session ID sent by the UE in the Protocol Configuration Option (PCO) 001AH (PDU session ID) and saves it. It then performs a Unified Data Management (UDM) registration and sends PGW-C Fully Qualified Domain Name (FQDN) to the UDM. After registration, the SMF initiates subscription fetch from the UDM.

Step	Description
6	The SMF sends Npcf_SMPolicyControl_Create to the PCF to initiate SM policy Association Establishment. The SMF includes the information elements received in Create Session Request message into the Npcf_SMPolicyControl_Create Service as follows: • The SUPI contains the IMSI. • The DNN contains the APN. • The PEI contains the IMEI-SV. • The Session AMBR contains the APN-AMBR. • The default QoS information contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.
7	The SMF receives Policy Charging and Control (PCC) Rules and PDU Session Policy Information, 5G QoS information in PCC Rule and in PDU Session Policy Information which are mapped into EPS QoS information. The SMF creates Traffic Flow Template (TFT) from the Service Data Filters (SDFs) received in PCC rules and associates them with the corresponding default and dedicated bearers.
8	Based on the charging policies received from PCF, the SMF initiates Nchf_ConvergedCharging_Create operation towards the CHF. This procedure is similar to a 5G session and is based on the charging rules received from the PCF.
9	The SMF performs UPF+PGW-U selection and N4 Session Establishment. Since this is a 4G session connecting the SMF, a separate CN tunnel is created for each bearer and QoS Flow ID (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
10	The SMF sends Create Session Response to S-GW and includes the bearer information and Tunnel Endpoint Identifier (TEID) for the default bearer. The SMF also includes the 5G QoS parameters in PCO and ePCO options 001CH/0023H (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime) and 001FH/0024H (QoS flow descriptions) to the UE. The SMF populates the container identifier 0005H (Selected Bearer Control Mode) in PCO, ePCO, and aPCO IE in Create Session Response. The container identifier contents field with value 2 indicates that the MS/NW mode is selected.
11	The S-GW sends Create Session Response to the MME.
12	The MME sends Initial Context Setup Request to the eNodeB with N1 Attach Accept message.
13	The eNodeB and UE perform Radio Resource Control (RRC) configuration.
14	The UE sends Direct transfer message to the eNodeB.
15	The eNodeB sends Attach Complete message in Initial Context Setup Response to the MME along with the TEID of eNodeB.
16	The MME sends a Modify Bearer Request to the S-GW with eNodeB TEID.
17	The SMF sends the Modify Bearer Response to the S-GW.
18	The S-GW sends Modify Bearer Response to the MME.

Initial Attach on E-UTRAN with Diameter Interfaces

A UE needs to register with the network to receive services that require registration.

The following figure shows the call flow derived from the 3GPP reference for initial attach on E-UTRAN with Diameter interfaces Gx and Gy.

Figure 30: Call Flow for E-UTRAN Initial Attach

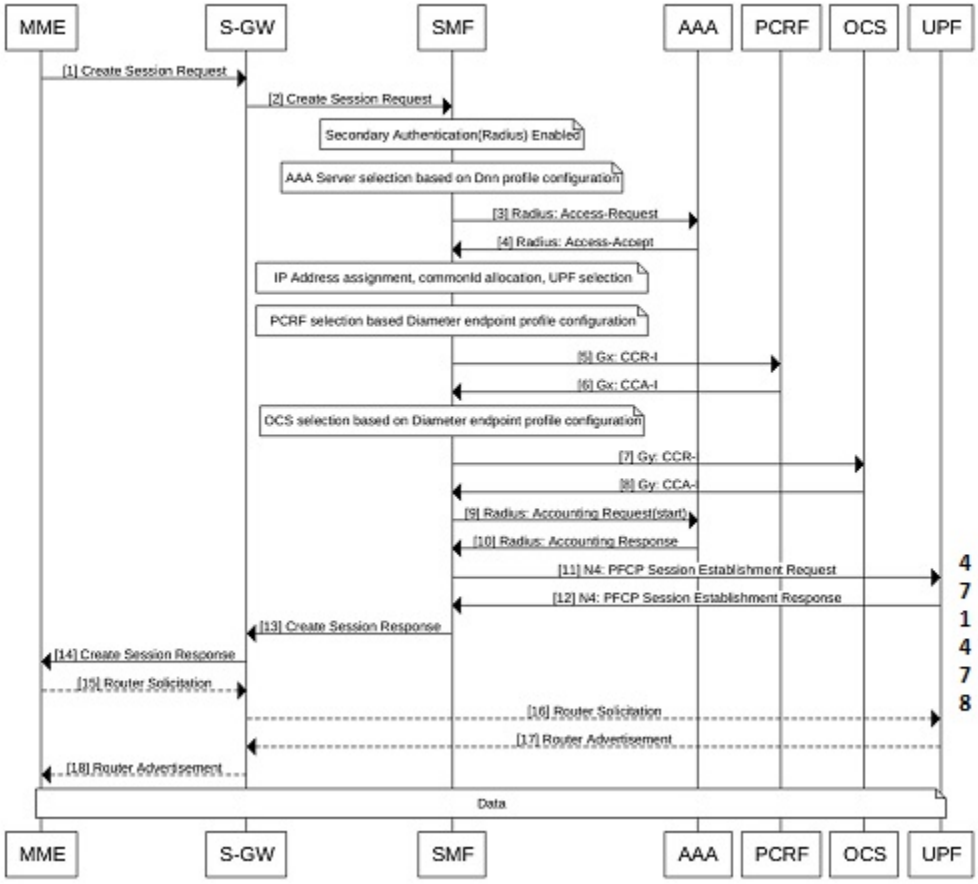


Table 45: Call Flow Description for E-UTRAN Initial Attach

Step	Description
1	MME sends Create Session Request to S-GW.
2	S-GW sends Create Session Request to SMF.
Note	As part of this call flow, Secondary Authentication using RADIUS gets enabled in a DNN profile, and the AAA server is selected based on the RADIUS profile configuration.
3	SMF sends RADIUS Access-Request to AAA server for authentication.
4	AAA Server sends Access-Accept to SMF.

Step	Description
Note	SMF assigns IP Address, commonId allocation, and UPF selection. SMF selects PCRF server based on Diameter endpoint profile configuration.
5	SMF sends Gx Credit Control Request Initial to PCRF server requesting for policy.
6	PCRF Server sends Gx Credit Control Answer Initial to SMF.
Note	SMF selects the Online Charging System (OCS) server based on the Diameter endpoint profile configuration.
7	SMF sends Gy Credit Control Request Initial to the OCS server requesting for quota. **Note** If the *diameter send- ccri traffic-start* is not configured, CCR-I is sent to OCS without any quota request after the Gx response for the default bearer. A successful response from OCS results in continuation of the Initial Attach procedure.
8	OCS server sends Gy Credit Control Answer Initial to SMF.
9	SMF sends Radius Accounting request start to AAA Server.
10	AAA Server sends Radius Accounting Response to SMF.
11	SMF sends N4 PFCP Session Establishment Request to UPF to create PDRs/FARs/QERs/URRs.
12	UPF sends N4 PFCP Session Establishment response to SMF.
13	SMF sends Create Session Response to S-GW.
14	S-GW sends Create Session Response to MME
15	MME sends Router solicitation to S-GW for IPv6 call.
16	S-GW sends Router Solicitation to UPF for IPv6 call.
17	UPF sends Router Advertisement to S-GW for IPv6 call.
18	S-GW sends Router Advertisement to MME for IPv6 call.

Context Replacement Call Flow

The SMF supports the context replacement procedure, when it receives a Create Session Request (CSReq) with the existing IMSI and EBI combination for which there's an existing subscriber.

The SMF can receive a CSReq for an already existing session. When the new CSReq is received, the existing session gets replaced with the new session, based on the new request. The context replacement procedure also referred as the create-over-create procedure.

As a first step in this process, the disconnect procedure for an existing session gets initiated. Later, it establishes a session based on the new request.

The following image describes the context replacement procedure call flow.

Figure 31: Call Flow for the Context Replacement Procedure

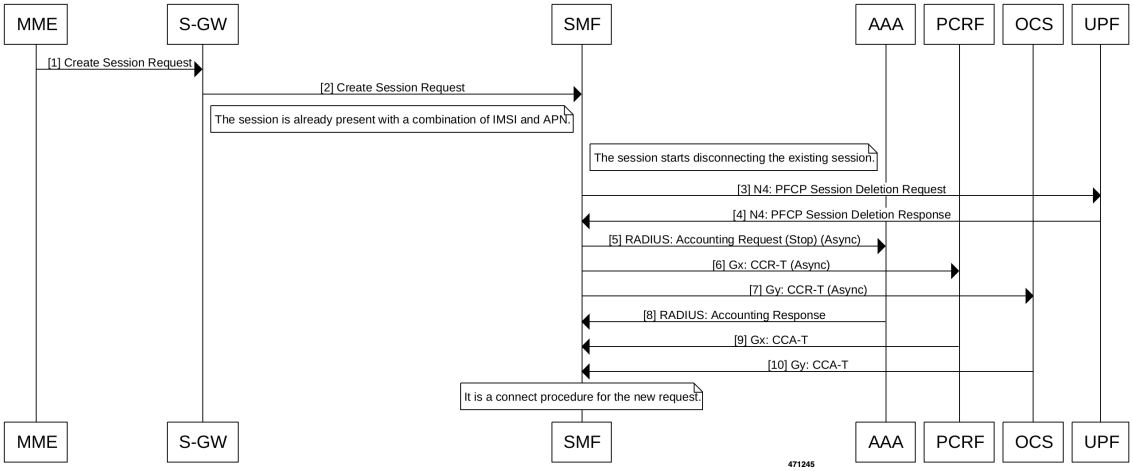


Table 46: Call Flow Description for the Context Replacement Procedure

Step	Description
1	The MME sends a Create Session Request to the S-GW.
2	The S-GW sends a Create Session Request to the SMF. **Note** A stale session was already present for this IMSI and EBI combination. The disconnect procedure gets started for the existing session.
3	The SMF sends a PFCP Session Deletion Request to the UPF.
4	The UPF sends a PFCP Session Deletion Response to the UPF.
5	The SMF sends an Async RADIUS Accounting-Request Stop to the AAA server.
6	The SMF sends an Async Gx CCR-T to the PCRF.
7	The SMF sends an Async Gy CCR-T to the OCS.
8	The AAA server sends a RADIUS Accounting-Response to the SMF.
9	The PCRF sends a Gx CCA-T to the SMF.
10	The OCS sends a Gy CCA-T to the SMF. **Note** After this action, the connect procedure continues for the new request.

Note The order in which the response messages outlined in Steps 8–10 is subject to change depending on the availability.

Configuring UE Initial Attach

This section describes how to configure the UE Initial Attach .

Configuring the UE Initial Attach involves the following steps:

1. Define FQDN in SMF Profile Configuration
2. Configure S5 Binding Address in SMF Service Configuration
3. Enable Kubernetes Configuration for SMF GTP Endpoint PODs

Define FQDN in SMF Profile Configuration

Use the following configuration to specify the FQDN of SMF. The configured FQDN is sent to the UDM during registration.

```
config
   profile smf smf_profile_name
   instances instance_id fqdn fqdn_name
      end
```

NOTES:

- **instances** *instance_id* **fqdn** *fqdn_name*: Configures the PGW-C FQDN corresponding to the local or remote instances. *fqdn_name* must be an alphanumeric string.

Configure S5 Binding Address

To define the S5 binding address at which the SMF listens for GTP messages from S-GW (S5 interface), use the following sample configuration:

```
config
  instance instance-id instance_id
    endpoint gtp
      replicas replica_count
      nodes node_id
      enable-cpu-optimization true
      interface s5
      vip-ip vip_ip_address
      exit
    interface s5e
      echo
      vip-ip vip_ip_address
      exit
    interface s2b
      vip-ip vip_ip_address
      end
```

NOTES:

- **interface s5**: Configure the S5 interface through which the messsges are sent from S-GW to SMF.

- **vip-ip** *vip_ip_address*: Enter the IP address at which SMF listens for GTP messages from S-GW through S5 interface. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

Configuring GTP Endpoint Parameters

Use the following sample configuration to define the GTP endpoint parameters.

```
config
   instance instance-id gr_instance_id
      endpoint gtp
         replicas replica_count
         vip-ip ipv4_address
         vip-ipv6 ipv6_address
         end
```

NOTES:

- **endpoint gtp**: Enter the GTP endpoint configuration.
- **replicas** *replica_count*: Enter the number of replicas to be created per node. The default value is 1.
- **vip-ip**: Specify the IPv4 address for the GTP endpoint.
- **vip-ipv6**: Specify the IPv6 address for the GTP endpoint.

Configuring APN-AMBR in CSR

The SMF sends APN-AMBR in Create Session Response if it is not received in Create Session Request or if the value has changed as part of PCF negotiation. The configuration under access profile overrides this behaviour.

Use the following sample configuration to configure the APN-AMBR action in Create Session Response.

```
config
  profile access access_profile_name
     gtpc message-handling create-session-response action apn-ambr
     exit
```

NOTES:

- **action apn-ambr**: Specifies the APN-AMBR action for the GTPC message.

Configuring PCRF, PCF, and OCS Interfaces

You can add Policy profiles under a dnnprofile to have configurations for 5G subscribers (N7 or N40 interface) and 4G subscribers (Gx, or Gy/Gz).

Important If the Gx (PCRF), Gy (OCS), Gz (CGF), or N40 (CHF) is not enabled, SMF will not interact with these interfaces.

Configure PCRF Interfaces

Use the following commands to configure a PCRF interface.

```
config
  profile dnn dnnprofile-ims
  network-element-profiles pcrf pcrf pcrf1
    exit
```

NOTES

- **network-element-profiles pcrf** *pcrf1*: Specifices the PCRF message handling profile configuration.

Configure PCF Interfaces

Use the following commands to configure a PCF interface.

```
config
  profile dnn dnnprofile-ims
  network-element-profiles pcf pcf nfprf-pcf1
    exit
```

NOTES

- **network-element-profiles pcf** *pcf nfprf-pcf1* : Specifies the PCF message handling profile configuration.

Configure OCS Interfaces

Use the following commands to configure an OCS interface.

```
config
  profile dnn dnnprofile-ims
  network-element-profiles ocs  ocs1
    exit
```

NOTES

- **network-element-profiles ocs***ocs1* : Specifies the OCS message handling profile configuration.

Verifying the UE Initial Attach Configuration

This section describes how to verify the UE Initial Attach configuration.

The following configuration is a sample output of the **show running-config** command:

```
show running-config
.
.
.
profile smf smf1
 node-id          ABC123
 bind-address ipv4 209.165.200.230
 bind-port        8008
instances 1  allowed-nssai  [ slice1 ]
 plmn-id mcc 123
 plmn-id mnc 456
 fqdn ciscosmf1
 service name nsmf-pdu
```

```
  type               pdu-session
  .
  .
  .
  n4 bind-address ipv4 209.165.200.240
  s5 bind-address ipv4 209.165.200.240
  http-endpoint base-url http://smf-service
.
.
.
k8 smf local redis-endpoint redis-primary:6379
k8 smf local service no-of-replicas 1
k8 smf local nodemgr no-of-replicas 1

.
.
.
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Show Command Support

Use the **show subscriber supi imsi** *imsi_value* **nf-service smf full** command to view the configuration related to the subscriber details for a 4G call.

The following is an example output.

```
smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-123456789012345",
        "pei": "imeisv-1122334455667788",
        "pduSessionId": 69,
        "pduSesstype": "Ipv4V6PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "765"
        },
        "sScMode": 1,
        "allocatedIp": "12.0.0.4",
        "allocatedIpv6": "2001:db0:0:2003::",
        "allocatedIntfid": "tG1H//5HR0c=",
        "eUtranLocation": {
          "ecgi": {
            "mcc": "214",
            "mnc": "365",
            "eutraCellId": "1234567"
          },
          "tai": {
            "mcc": "214",
            "mnc": "365",
            "tac": "6789"
          },
```

```
          "ueLocationTimestamp": "2022-08-08T13:16:09Z"
        },
        "alwaysOn": "None",
        "dcnr": "None",
        "wps": "Non-Wps Session",
        "ratType": "EUTRA",
        "ueType": "4G Capable UE",
        "sessTimeStamp": "2022-08-08 13:16:09.107469768 +0000 UTC",
        "callDuration": "3.531530696s",
        "ipPool": "poolv4",
        "ipv6Pool": "poolv6",
        "commonId": 2097156,
        "linkedEbi": 5,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        "authStatus": "Unauthenticated",
        "roamingStatus": "Roamer",
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        },
      }
    }
  ]
}
```


Note In the preceding output example, for a 4G call, the RAT Type appears as "EUTRA".

Detach Procedure for EPS on SMF

Feature Description

EPS Interworking through 5G Core Network

The SMF supports the default bearer deletion procedures for a UE attached through E-UTRAN, MME, and S-GW.

SMF Interworking with Diameter Interfaces

When the UE is attached to the E-UTRAN, SMF supports the following Network-initiated detach procedures with Diameter interfaces:

- SMF-initiated detach procedure
- UPF-initiated detach procedure
- PCRF-initiated detach procedure
- UE-initiated detach procedure
- RADIUS-initiated detach procedure

How it Works

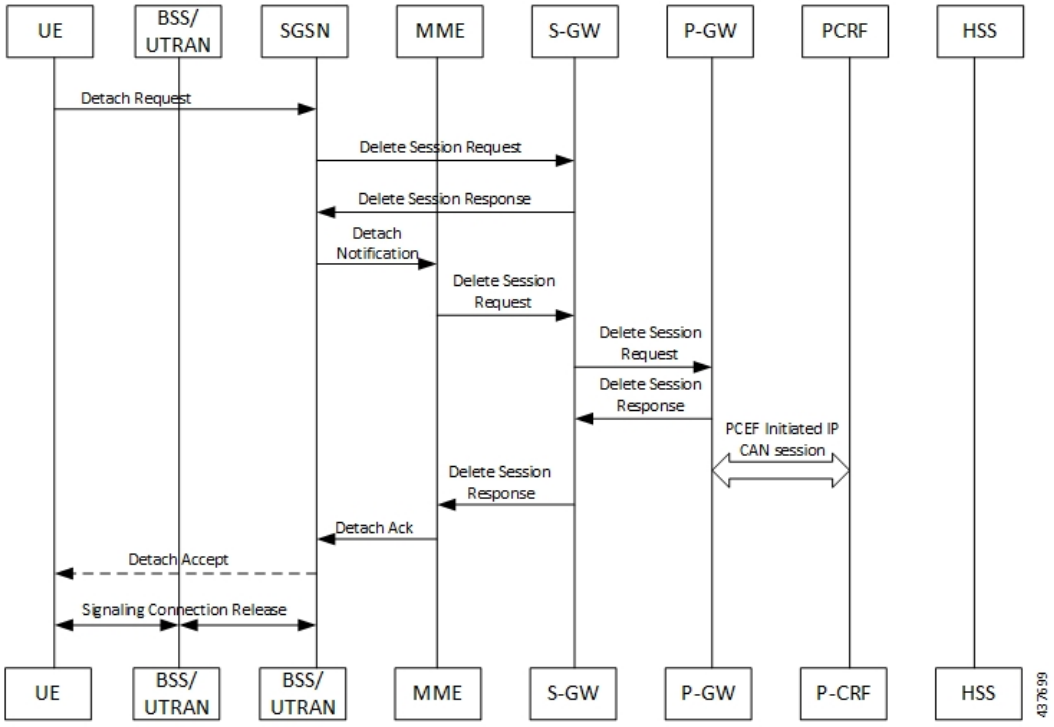
Call Flows

This section describes the call flows associated with this feature.

UE-initiated EPS Call Release Procedure

The following figure shows the call flow for UE-initiated release of EPS call.

Figure 32: UE-initiated EPS Call Release Flow



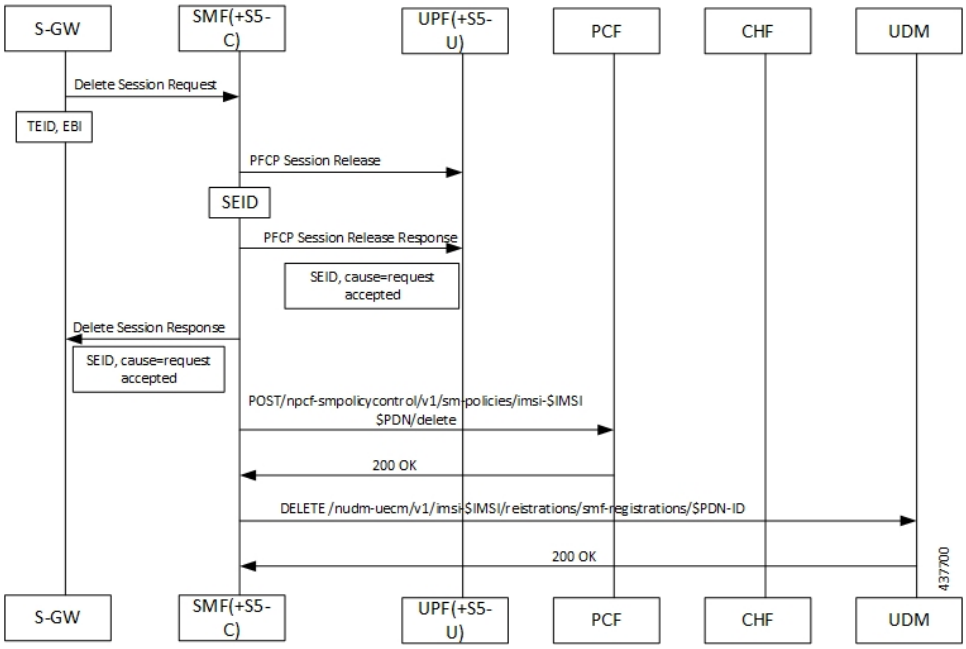
The detach procedures for the EPS are defined in 3GPP 23.401, Section 5.3.8. When the UE is attached to E-UTRAN, the detach procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

- Any interaction towards PCRF (CCR-T), that is PCEF-initiated IP-CAN session between PGW-C and PCRF, is replaced by Npcf_SMPolicyControl_Update Request from the SMF to the PCF. The parameters sent in this message follow a mapping from Delete Session Request contents in a way similar to the Create Session Request message for initial attach.
- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Release service operations.
- The user plane resources are removed using the N4 Session Release procedure towards the UPF.

UE-initiated Call Release Detail Procedure

The following figure shows the detailed procedure of UE-initiated release of EPS call.

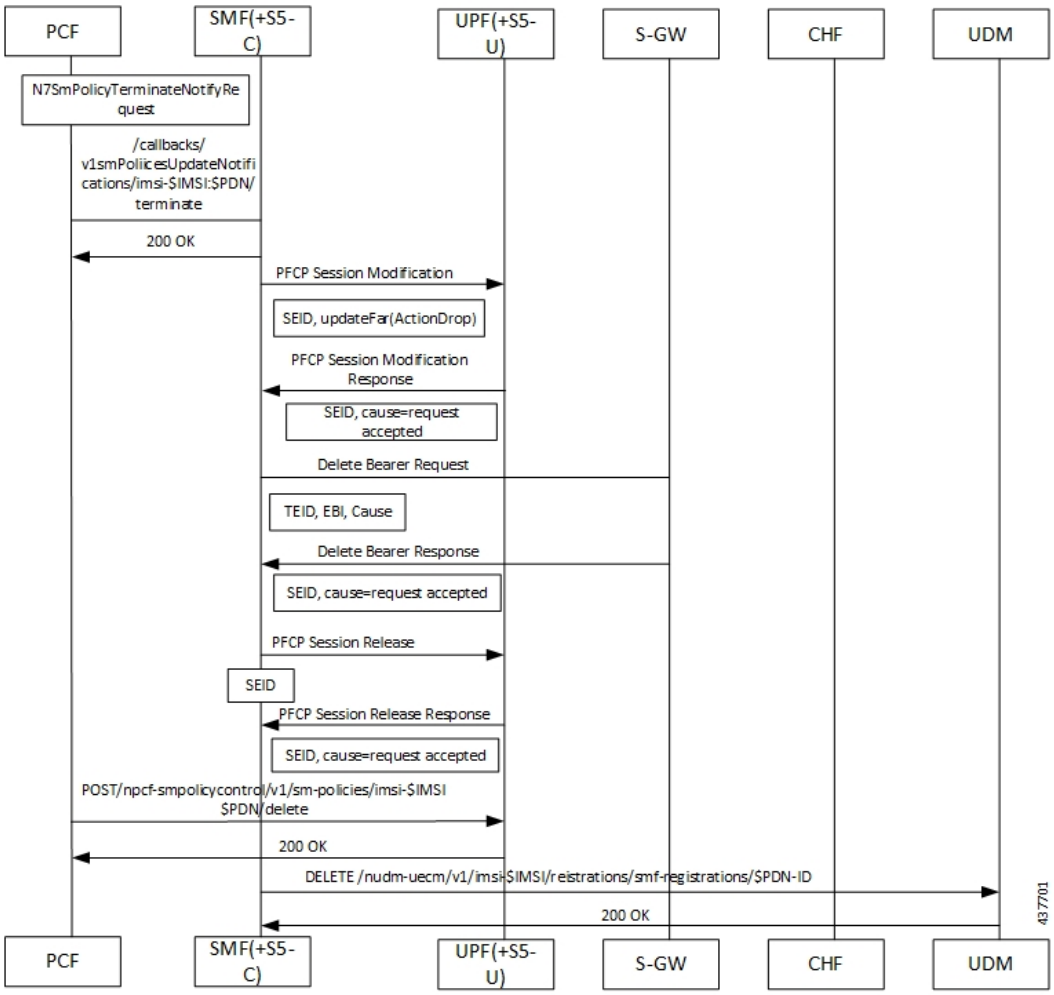
Figure 33: Detailed Call Flow of UE-initiated EPS Call Release



PCF-initiated Call Release Detail Procedure

The following figure shows the detailed procedure of PCF-initiated release of EPS call.

Figure 34: Detailed Call Flow of PCF-initiated EPS Call Release



Network-initiated Detach Procedures with Diameter Interfaces

This section describes Network-initiated Detach call flows and procedures.

SMF Initiated Detach Procedure

SMF receives a request for session release through one of the following methods:

- Clear Subscriber
- GTP Path Failure
- Peer Restart
- Absolute Session Timeout
- Cp-idle Timeout

The following call flow illustrates the procedure of an E-UTRAN network (SMF) initiated detach.

Figure 35: Call Flow for SMF-initiated Detach

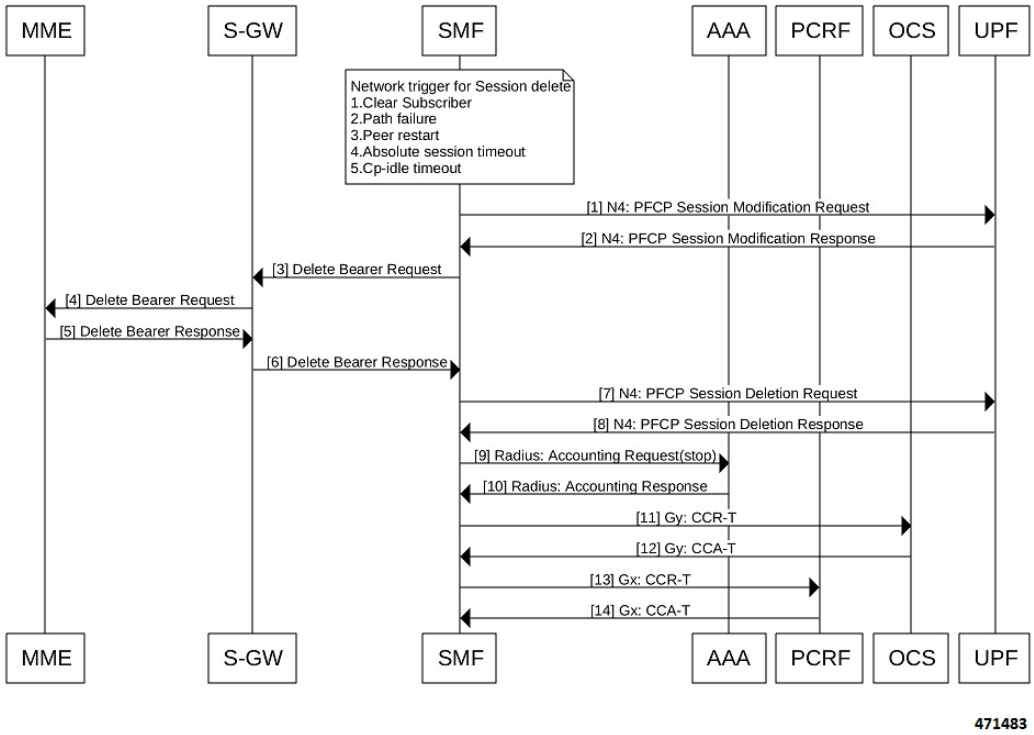


Table 47: Call Flow Description for SMF Initiated Detach

Step	Description
1	SMF sends N4 PFCP Session Modification Request to UPF with FARs having apply action set to Drop.
2	UPF sends N4 PFCP Session Modification Response to SMF.
3	SMF sends Delete Bearer Request to S-GW.
4	S-GW sends Delete Bearer Request to MME.
5	MME sends Delete Bearer Response to S-GW.
6	S-GW sends Delete Bearer Response to SMF.
7	SMF sends N4 PFCP Session Deletion Request to UPF to release N4 session.
8	UPF sends N4 PFCP Session Deletion Response to SMF.
9	SMF sends Radius Accounting Request Stop to AAA server to release the accounting session.
10	AAA server sends Radius Accounting Response to SMF.
11	SMF sends Gx Credit Control Request Terminate to OCS to release the Gy session.
12	OCS sends Gx Credit Control Answer Terminate to SMF.

Step	Description
13	SMF sends Gx Credit Control Request Terminate to PCRF to release the Gx session.
14	PCRF sends Gx Credit Control Answer Terminate to SMF.

UPF-initiated Detach Procedure

The following call flow illustrates an E-UTRAN network (UPF) initiated detach.

Figure 36: Call Flow for UPF-initiated Detach

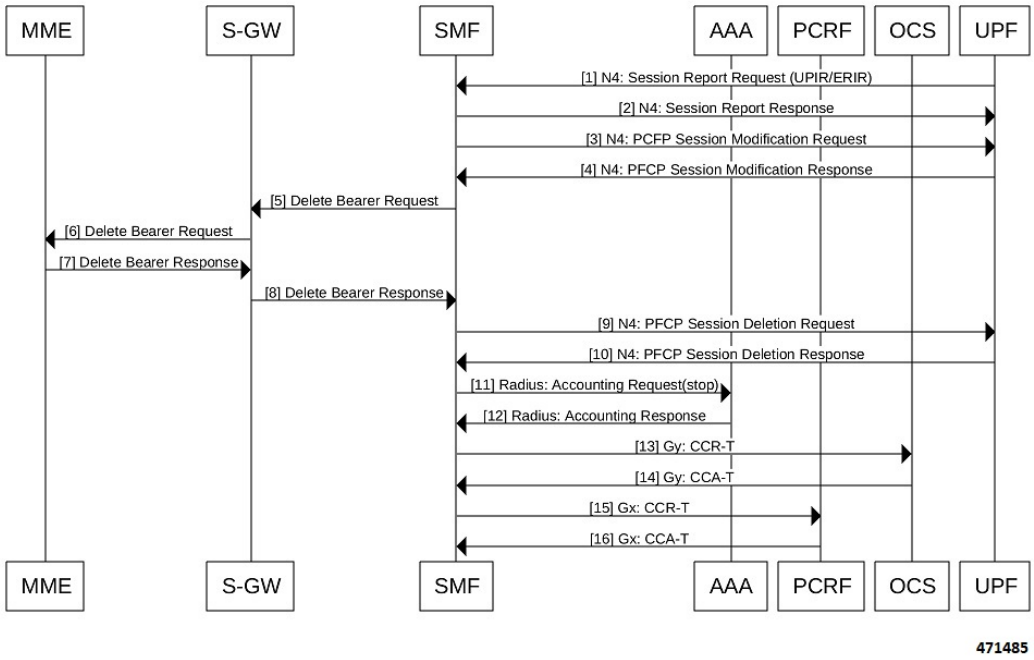


Table 48: Call Flow Description for UPF-initiated Detach

Step	Description
1	UPF sends N4 Session Report Request (ERIR[default bearer]/UPIR) to SMF.
Note	Session Report Request of type ERIR is received when GTP-U Error Indication is received at UPF. Session Report Request of type UPIR is received when the UPF inactivity timer is expired on UPF. Both of these (In case, ERIR is received on default bearer) lead to session termination.
2	SMF sends N4 Session Report Response to UPF.
3	SMF sends N4 PFCP Session Modification Request to UPF with FARs having apply action set to drop
4	UPF sends N4 PFCP Session Modification Response to SMF.
5	SMF sends Delete Bearer Request to S-GW.
6	S-GW sends Delete Bearer Request to MME.

Step	Description
7	MME sends Delete Bearer Response to S-GW.
8	S-GW sends Delete Bearer Response to SMF.
9	SMF sends N4 PFCP Session Deletion Request to UPF to release N4 session.
10	UPF sends N4 PFCP Session Deletion Response to SMF.
11	SMF sends Radius Accounting Request Stop to AAA server to release the accounting session.
12	AAA server sends Radius Accounting Response to SMF.
13	SMF sends Gy Credit Control Request Terminate to OCS to release the Gy session.
14	OCS sends Gy Credit Control Answer Terminate to SMF.
15	SMF sends Gx Credit Control Request Terminate to PCRF to release the Gx session.
16	PCRF sends Gx Credit Control Answer Terminate to SMF.

PCRF-initiated Detach Procedure

The following call flow illustrates the procedure in which the E-UTRAN network (PCRF) initiated detach.

Figure 37: Call Flow for PCRF-initiated Detach

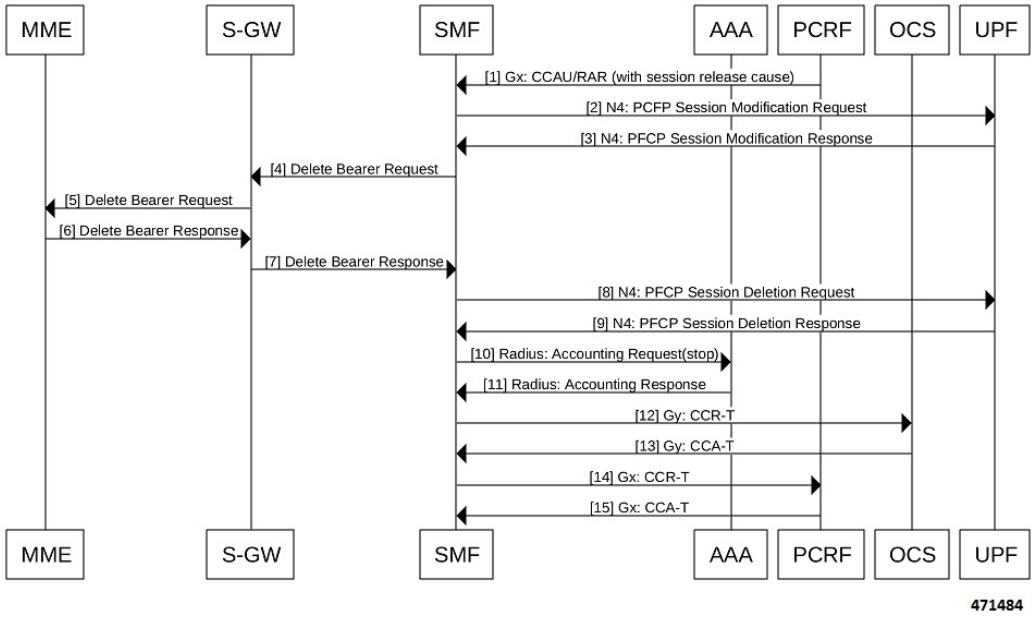


Table 49: Call Flow Description for PCRF-initiated Detach

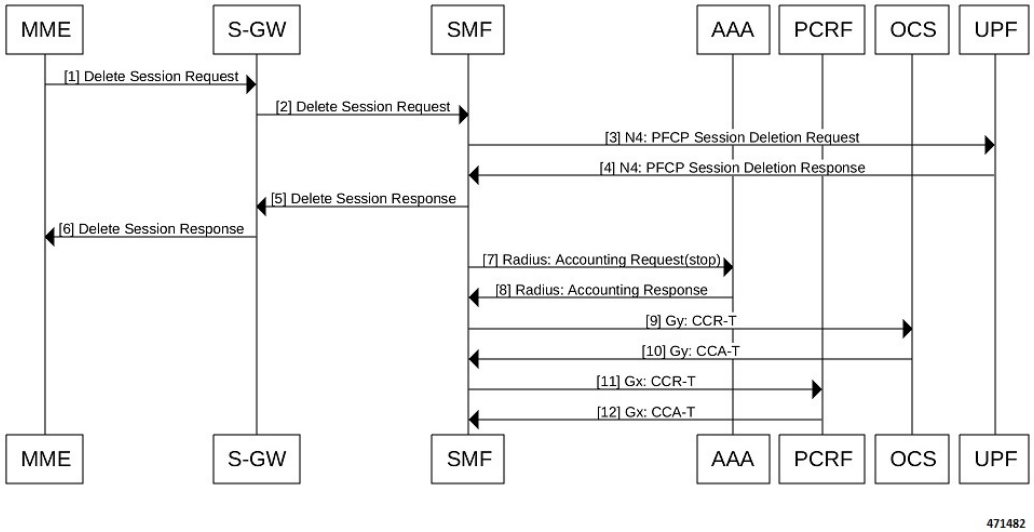
Step	Description
1	PCRF sends Gx Credit Control Answer or RAR with session release cause to SMF.

Step	Description
2	SMF sends N4 PFCP Session Modification Request to UPF with FARs having apply action set to Drop
3	UPF sends N4 PFCP Session Modification Response to SMF.
4	SMF sends Delete Bearer Request to S-GW.
5	S-GW sends Delete Bearer Request to MME.
6	MME sends Delete Bearer Response to S-GW.
7	S-GW sends Delete Bearer Response to SMF.
8	SMF sends N4 PFCP Session Deletion Request to UPF to release N4 session.
9	UPF sends N4 PFCP Session Deletion Response to SMF.
10	SMF sends Radius Accounting Request Stop to AAA server to release radius session.
11	AAA server sends RADIUS Accounting Response to SMF.
12	SMF sends Gx Credit Control Request Terminate to OCS to release Gy session.
13	OCS sends Gx Credit Control Answer Terminate to SMF.
14	SMF sends Gx Credit Control Request Terminate to PCRF to release Gx session.
15	PCRF sends Gx Credit Control Answer Terminate to SMF.

UE Initiated Detach Procedure

The following figure shows the call flow for an UE-initiated release with Diameter interfaces.

Figure 38: Call Flow for UE Initiated Release with Diameter Interfaces



The following table describes the detailed procedure of an E-UTRAN UE-initiated detach.

Table 50: Call Flow Description for UE Initiated Release with Diameter Interfaces

Step	Description
1	MME sends Delete Session Request to S-GW.
2	S-GW sends Delete Session Request to SMF.
3	SMF sends N4 PFCP Session Deletion Request to UPF to release N4 session.
4	UPF sends N4 PFCP Session Deletion Response to SMF.
5	SMF sends Delete Session Response to S-GW.
6	S-GW sends Delete Session Response to MME.
7	SMF sends Radius Accounting Request Stop AAA server to release the accounting session.
8	AAA server sends RADIUS Accounting Response to SMF.
9	SMF sends Gy Credit Control Request Terminate to OCS to release the Gy session.
10	OCS sends Gy Credit Control Answer Terminate to SMF.
11	SMF sends Gx Credit Control Request Terminate to PCRF.
12	PCRF sends Gx Credit Control Answer Terminate to SMF to release the Gx session.

RADIUS-initiated Detach Procedure

The following figure shows the call flow for E-UTRAN RADIUS disconnect messages.

Figure 39: Call Flow for RADIUS-initiated Detach

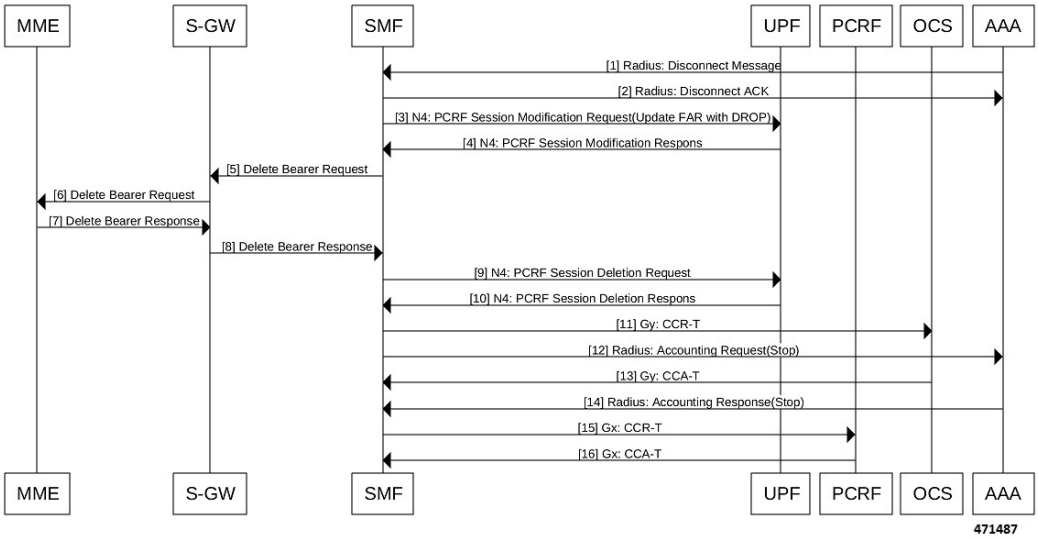


Table 51: Call Flow Description for RADIUS-initiated Detach

Step	Description
1	AAA Radius Disconnect Message to SMF.
2	SMF sends back Radius Disconnect acknowledgment.
3	SMF sends PCRF Session Modification Request (Update FAR with DROP) to UPF.
4	UPF responds to SMF with PCRF Session Modification Response.
5	SMF sends Delete Bearer Request to S-GW
6	S-GW forwards Delete Bearer Request to MME.
7	MME responds to S-GW with Delete Bearer Response.
8	S-GW forwards Delete Bearer Response to SMF.
9	SMF sends PCRF Session Deletion Request to UPF.
10	UPF responds to SMF with PCRF Session Deletion Response.
11	SMF sends CCR-T to OCS.
12	SMF sends Accounting Request(Stop) to AAA.
13	OCS responds to SMF with CCA-T.
14	SMF responds to AAA with Accounting Response(Stop).
14	SMF sends CCR-T to PCRF.
15	PCRF responds to SMF with CCA-T.

Dedicated Bearer Activation and Deactivation

Feature Description

SMF supports the PCF-initiated dedicated bearer creation and dedicated bearer deletion procedures for a UE attached via E-UTRAN, MME, and S-GW.

How it Works

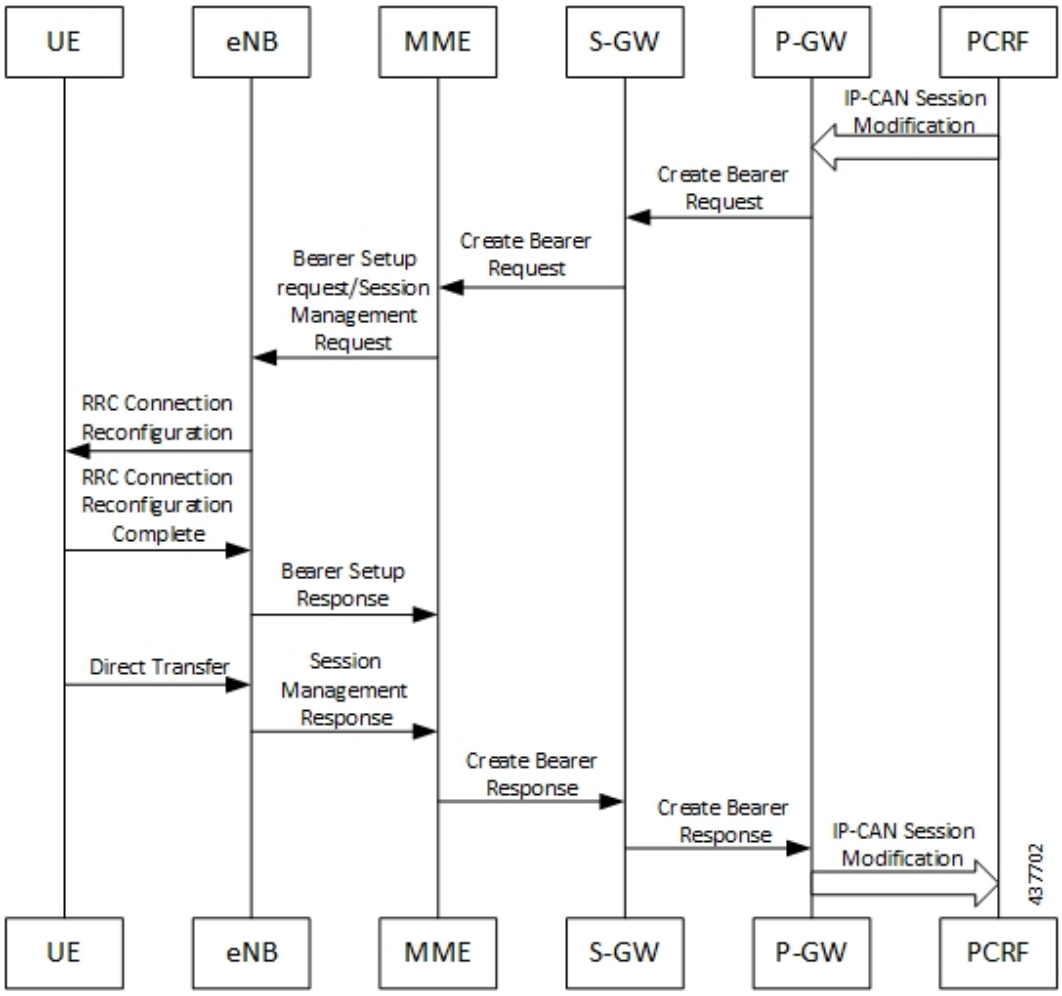
Call Flows

This section describes the call flows associated with this feature.

Dedicated Bearer Creation Call Flow

The following figure describes the Dedicated Bearer Creation procedure.

Figure 40: Dedicated Bearer Creation Call Flow

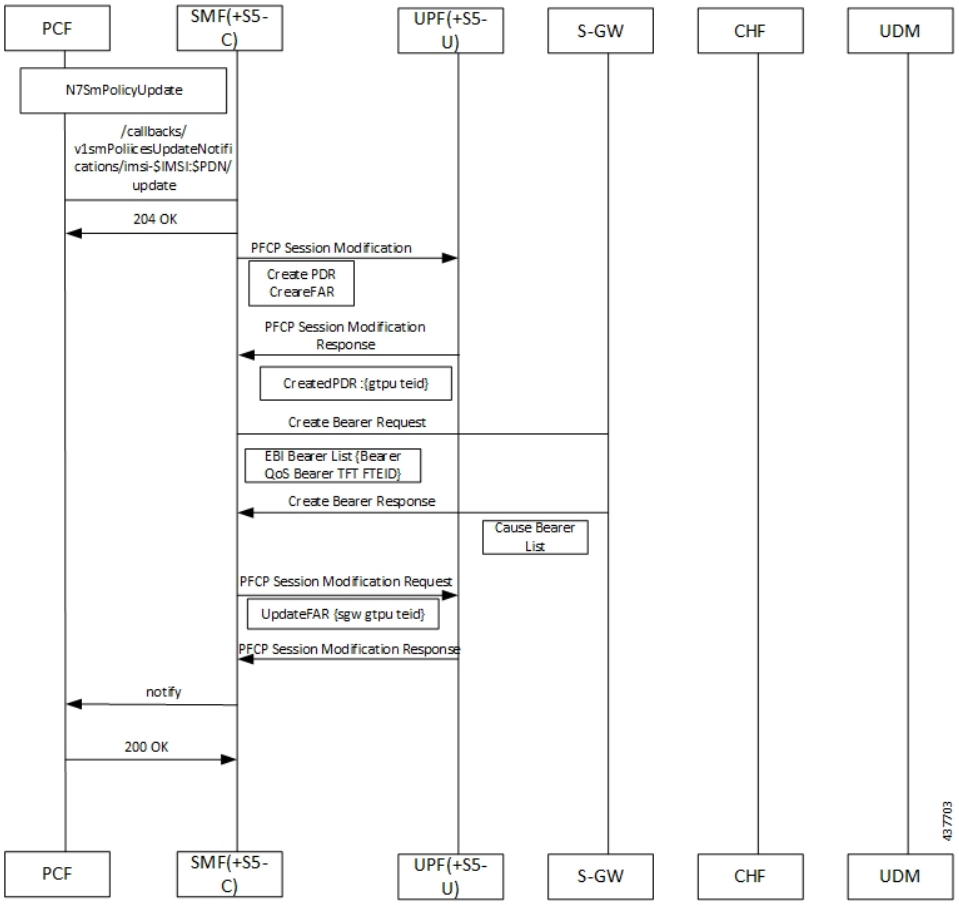


The dedicated bearer creation or activation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.1. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

- Any interaction towards the PCRF (RAR from the PCRF or CCR-U to the PCRF) are replaced by Npcf_SMPolicyControl_UpdateNotify request from the PCF to the SMF and Npcf_SMPolicyControl_Update Request from the SMF to the PCF respectively.
- The PCC rules provided by PCF are mapped to TFTs for the new dedicated bearer and the associated QoS is mapped to 4G QoS as defined in the Generating EPS PDN Connection Parameters from 5G PDU Session Parameters, on page 250.
- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Update service operations.
- The user plane resources for dedicated bearers are added using the N4 Session Modification procedure towards UPF where PDRs, QERs and FARs are added for the SDF filters for the new dedicated bearer.
- The SMF saves the EBI for the dedicated bearer as received in Create Bearer response.

The following figure describes the PCF-initiated Dedicated Bearer Activation procedure.

Figure 41: PCF-initiated Dedicated Bearer Activation



Non-roaming 4G PDN Attach with N4 Optimization Call Flow

This section describes the call flow of the non-roaming 4G PDN attach with the N4 optimization.

Figure 42: Non-roaming 4G PDN Attach with N4 Optimization Call Flow

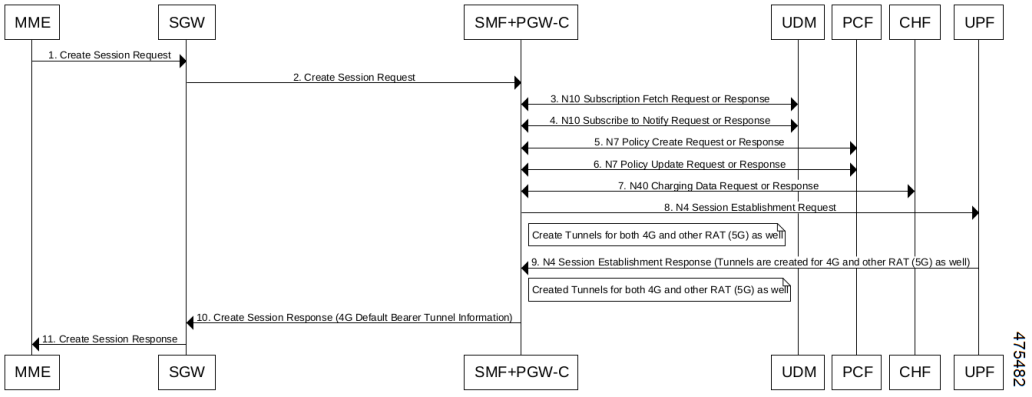


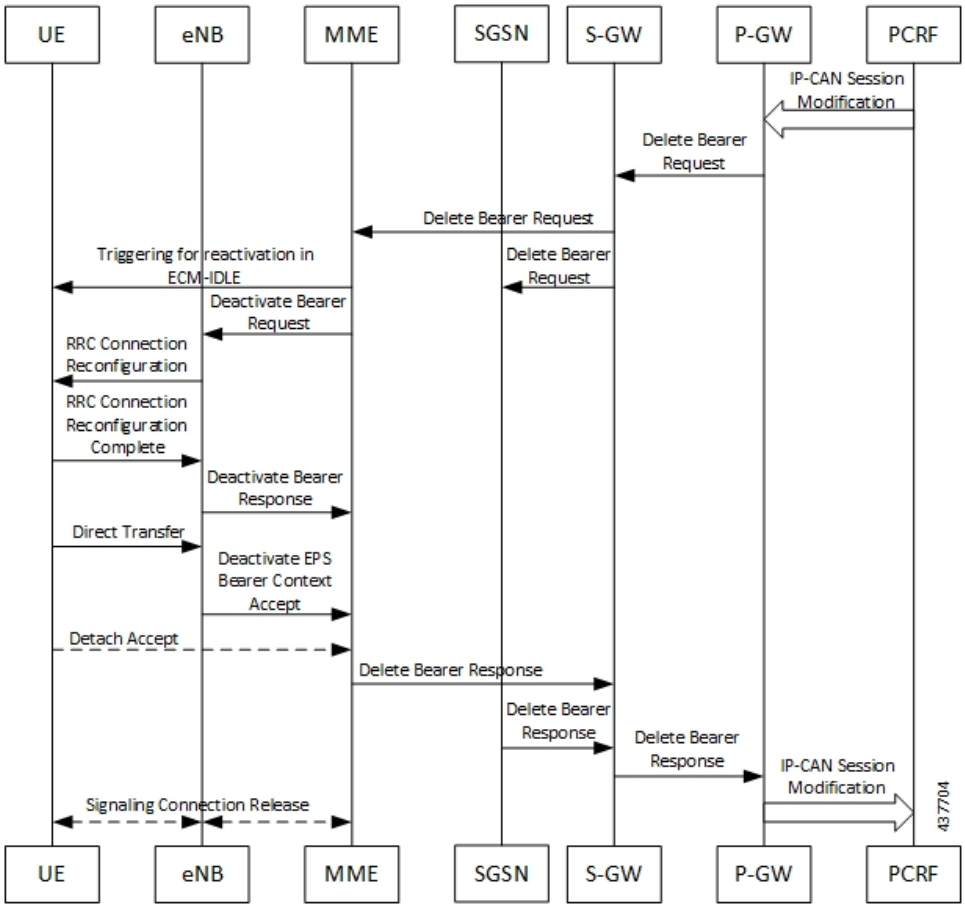
Table 52: Non-roaming 4G PDN Attach with N4 Optimization Call Flow Description

Step	Description
1	MME sends the Create Session Request to S-GW.
2	S-GW sends the Create Session Request to SMF+PGW-C.
3	SMF+PGW-C sends the N10 Subscription Fetch Request to UDM. Then, UDM sends the N10 Subscription Fetch Response to SMF+PGW-C.
4	SMF+PGW-C sends the N10 Subscribe to Notify Request to UDM. Then, UDM sends the N10 Subscribe to Notify Response to SMF+PGW-C.
5	SMF+PGW-C sends the N7 Policy Create Request to PCF. Then, PCF sends the N7 Policy Create Response to SMF+PGW-C.
6	SMF+PGW-C sends the N7 Policy Update Request to PCF. Then, PCF sends the N7 Policy Update Response to SMF+PGW-C.
7	SMF+PGW-C sends the N40 Charging Data Request to CHF. Then, CHF sends the N40 Charging Data Response to SMF+PGW-C.
8	SMF+PGW-C sends the N4 Session Establishment Request to UPF. SMF creates tunnel for both 5G and other RAT (4G).
9	After the creation of the tunnel, UPF sends the N4 Session Establishment Response to SMF+PGW-C.
10	SMF+PGW-C sends the Create Session Response to S-GW. This response includes the 4G default bearer tunnel information.
11	S-GW sends the Create Session Response to MME.

Dedicated Bearer Deactivation Call Flow

The following figure describes the Dedicated Bearer Deactivation procedure.

Figure 43: Dedicated Bearer Deactivation Call Flow



The dedicated bearer deactivation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.4. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

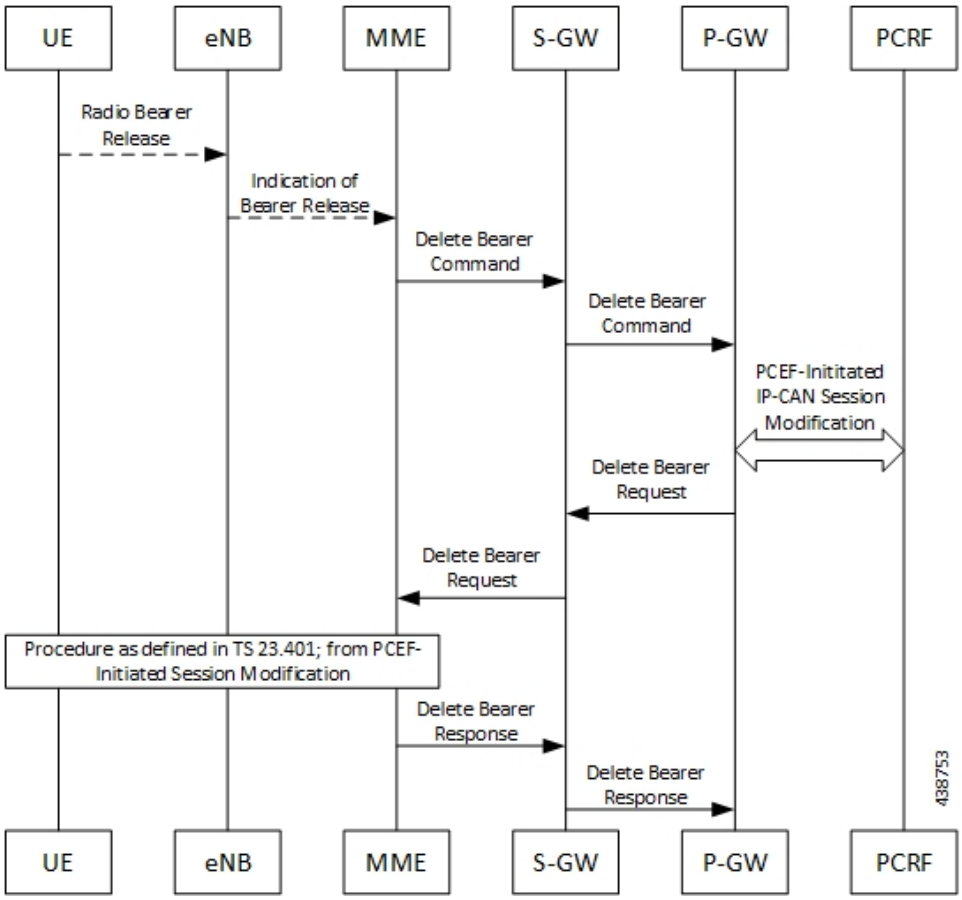
- Any interaction towards PCRF (RAR from the PCRF/CCR-U to the PCRF) are replaced by Npcf_SMPolicyControl_UpdateNotify request from PCF to the SMF and Npcf_SMPolicyControl_Update Request from the SMF to the PCF respectively.
- The PCC rules removed by PCF are mapped to the corresponding dedicated bearers and the bearer deactivation is triggered for these bearers.
- All Gy and Gz interface messages are replaced by Nchf_ConvergedCharging_Update service operations.
- The user plane resources for dedicated bearers are removed using the N4 Session Modification procedure towards UPF where PDRs, QERs and Forward Action Rule (FARs) are removed for the SDF filters for the deleted dedicated bearer.

MME-initiated Dedicated Bearer Deactivation

The MME uses the UE or MME-requested PDN Disconnection procedure to initiate the release of PDN connections. The following call flow illustrates the procedure in which the dedicated bearers are deactivated.

Note The default bearers are not affected during the disconnection process.

Figure 44: MME-initiated Dedicated Bearer Deactivation



Step	Description
1	The release of Radio bearers for the UE in the ECM-CONNECTED state occurs due to local reasons such as abnormal resource limitation. The UE deletes the bearer contexts related to the released radio bearers.
2	When the eNodeB releases radio bearers, it sends an indication of bearer release to the MME. This indication could either be the Bearer Release Request (EPS Bearer Identity) message to the MME, or Initial Context Setup Complete, Handover Request Ack and UE Context Response. Path Switch Request can also indicate the release of a bearer. The eNodeB includes the ECGI and TAI in the indication sent to the MME.
3	The MME sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN or NAS Release Cause, if available) message per PDN connection to the S-GW to deactivate the selected dedicated bearer. RAN or NAS Release Cause indicates the RAN release cause or the NAS release cause. RAN or NAS Release Cause is only sent by the MME to the PGW-C, if permitted according to the MME operator policy.

Step	Description
4	The S-GW sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN/NAS Release Cause) message per PDN connection to the PGW-C.
5	If the PCC infrastructure is deployed, the PGW-C informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure as defined in 3GPP TS 23.203 and provides the User Location Information, UE Time Zone and RAN or NAS Release cause, if available, received in the Delete Bearer Command from the S-GW if requested by the PCRF as defined in 3GPP TS 23.203. The PCRF sends an updated PCC decision to the PGW-C. **Note** User Location Information and UE Time Zone may be unavailable if the MME or the S-GW are of a previous release and did not provide this information.
6	The PGW-C sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
7	The S-GW sends the Delete Bearer Request (EPS Bearer Identity) message to the MME.
8	This step involves invoking Step 5 through Step 8. Note that these steps are omitted if the bearer deactivation was triggered by the eNodeB in Step 1 and Step 2. Also, these steps are omitted if the MME initiated bearer release due to failed bearer set up during handover, the UE and the MME deactivate the failed contexts locally without peer-to peer ESM signaling.
9	The MME deletes the bearer contexts related to the deactivated EPS bearer and acknowledges the bearer deactivation to the S-GW by sending a Delete Bearer Response (EPS Bearer Identity, User Location Information (ECGI)) message.
10	The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the PGW-C by sending a Delete Bearer Response (EPS Bearer Identity) message.

SMF-initiated Dedicated Bearer Deactivation

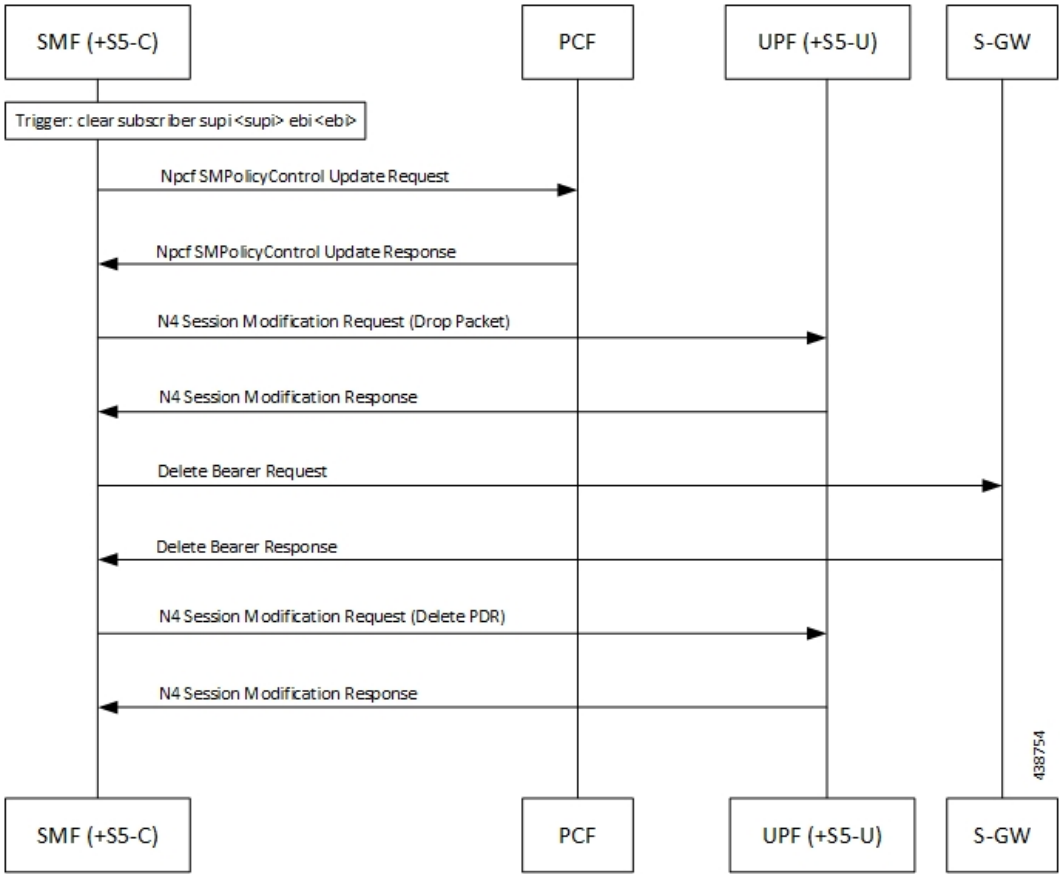
The following procedure describes the SMF-initiated dedicated bearer deactivation process as defined in 3GPP TS 23.203.

Note Default bearers are not affected during the dedicated bearer deactivation process.

- The SMF-initiated delete bearer is triggered using the **clear subscriber** command.
- If the PCC infrastructure is deployed, the PGW-C informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure and provides the User Location Information, UE Time Zone and RAN or NAS Release cause, if available, received in the **clear subscriber** command if requested by the PCRF. The PCRF sends an updated PCC decision to the PGW-C.
- The PGW-C sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
- The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the PGW-C by sending a Delete Bearer Response (EPS Bearer Identity) message.

The following call flow illustrates the SMF-initiated dedicated bearer deactivation.

Figure 45: SMF-initiated Dedicated Bearer Deactivation



EPS Fallback

Feature Description

SMF supports fallback to EPS from 5GC for IMS sessions if gNB rejects the dedicated bearer creation with ims-voice-eps-fallback or rat-fallback triggered.

For the UE devices not supporting VoNR, the SMF performs a fallback to EPS for voice calls. This includes 5G to EPS handover and dedicated bearer creation in 4G for voice call.

How it Works

Call Flows

The following call flow depicts the EPS Fallback procedure.

Figure 46: EPS Fallback Call Flow

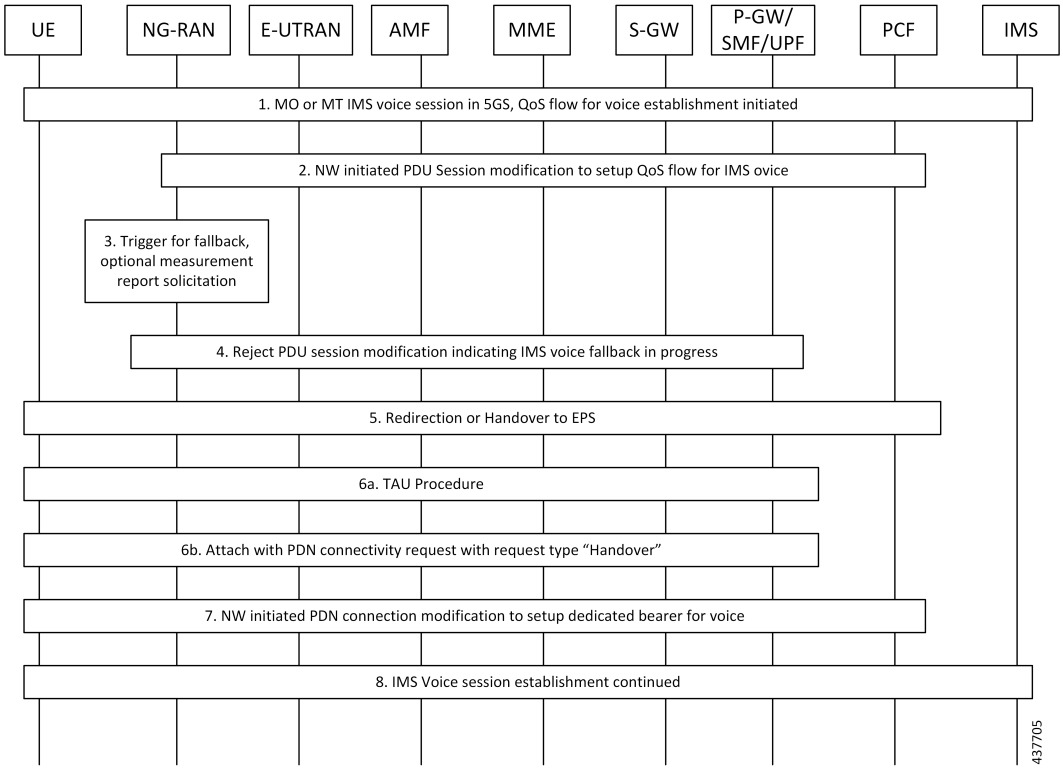


Table 53: EPS Fallback Call Flow Description

Step	Description
1	The UE initiates Mobile-Originated (MO) or a Mobile-Terminated (MT) IMS voice establishment procedure with NG-RAN in 5GS.
2	The Network-initiated PDU Session modification request to set up QoS flow for voice reaches the NG-RAN.
3	The NG-RAN is configured to support the EPS fallback for IMS voice. Based on the UE functionalities, indication from the AMF to redirect EPS fallback for voice, network configuration, and radio conditions, the NG-RAN triggers fallback to EPS. If the NG-RAN determines not to trigger the fallback to EPS, then the procedure stops, and the following steps are not performed. The NG-RAN initiates measurement report solicitation from the UE including E-UTRAN as target.

Step	Description
4	The NG-RAN rejects the PDU Session modification request received in Step 2 with an indication that mobility due to fallback for IMS voice is ongoing. The NG-RAN indicates the rejection of the PDU session modification to configure QoS flow for IMS voice that is received in Step 2 as PDU Session Response message toward the SMF through the AMF. This message includes the details on the ongoing mobility due to fallback for IMS voice. The SMF maintains the PCC rules that are associated with the QoS flows. For a roaming scenario, the PDU Session Response message is sent toward H-SMF through V-SMF. Or NG-RAN responds with configured cause which it might trigger fallback to EPS. If the cause sent by gNB matches with EPS Fallback causes configured at SMF, it continues to behave as mentioned in steps from step. 5 onwards. **Note** If configuration at SMF always checks for the configured cause even if gNB rejects N2 message with cause “IMS voice EPS fallback or RAT fallback triggered”.
5	Based on the UE functionalities, the NG-RAN initiates handover to the EPS. The SMF reports change of the RAT type, if the PCF is subscribed for it. A timer starts to track failure in the EPS fallback. After the timer expires, the SMF notifies the PCF about the dedicated bearer creation failure and new statistics, with the “smf_eps_fb” and “timeout” labels, is incremented.
6a	For 5GS to EPS handover, the UE initiates TAU procedure.
6b	The UE attaches the PDN connectivity request with the “handover” request type.
7	After the completion of the 5GS to EPS handover procedure, the SMF or PGW-C reinitiates the configuration of the dedicated bearer for IMS voice and mapping the 5G QoS to EPC QoS parameters. The SMF notifies about the Successful Resource Allocation and Access Network Information, if the PCF is subscribed for it.
8	The IMS voice session establishment continues.

EPS Fallback Trigger Cause Configuration

Use the following sample configuration to configure EPS fallback trigger cause.

```
config
  profile access access_profile_name
    eps-fallback trigger-cause group radioNetwork value radioNetwork_value
    exit
```

NOTES:

- **trigger-cause** : Indicates cause to trigger EPSFallback.
- **group** : Indicates cause group.

```
[smf] smf(config-access-access1)# eps-fallback trigger-cause group
Possible completions:
misc nas protocol radioNetwork transport
[smf] smf(config-access-access1)# eps-fallback trigger-cause group radioNetwork value
Possible completions:
unsignedInt, 0 .. 46
```

Verifying EPS Fallback Trigger Cause Configuration

This section describes how to verify the EPS fallback trigger cause configuration in SMF.

Use the following sample configuration to verify EPS fallback trigger cause radio network value configuration:

```
smf# show running-config profile access access1
 eps-fallback trigger-cause group radioNetwork
 value [ 22 36 ]
 exit
 eps-fallback trigger-cause group transport
 value [ 0 ]
 exit
 eps-fallback trigger-cause group nas
 value [ 0 ]
 exit
 eps-fallback trigger-cause group misc
 value [ 1 ]
 exit
exit
```

Indirect Data Forwarding Tunnel (IDFT) Timer Support

Feature Description

SMF supports the Indirect Data Forwarding Tunnel (IDFT) timer during the IDFT procedures for 5G to a 4G handover. During the handover, the IDFT tunnels of 5G are released. SMF receives the NSMF PDU Session Update SM Context Request to release the forwarding tunnels from AMF. When SMF does not receive this request, the IDFT timer ensures the release of unused tunnels.

How it Works

Call Flows

This section includes the following call flow.

5G to EPS Handover with IDFT Timer Call Flow

This section describes the 5G to EPS handover with IDFT timer call flow.

Figure 47: 5G to EPS Handover with IDFT Timer Call Flow

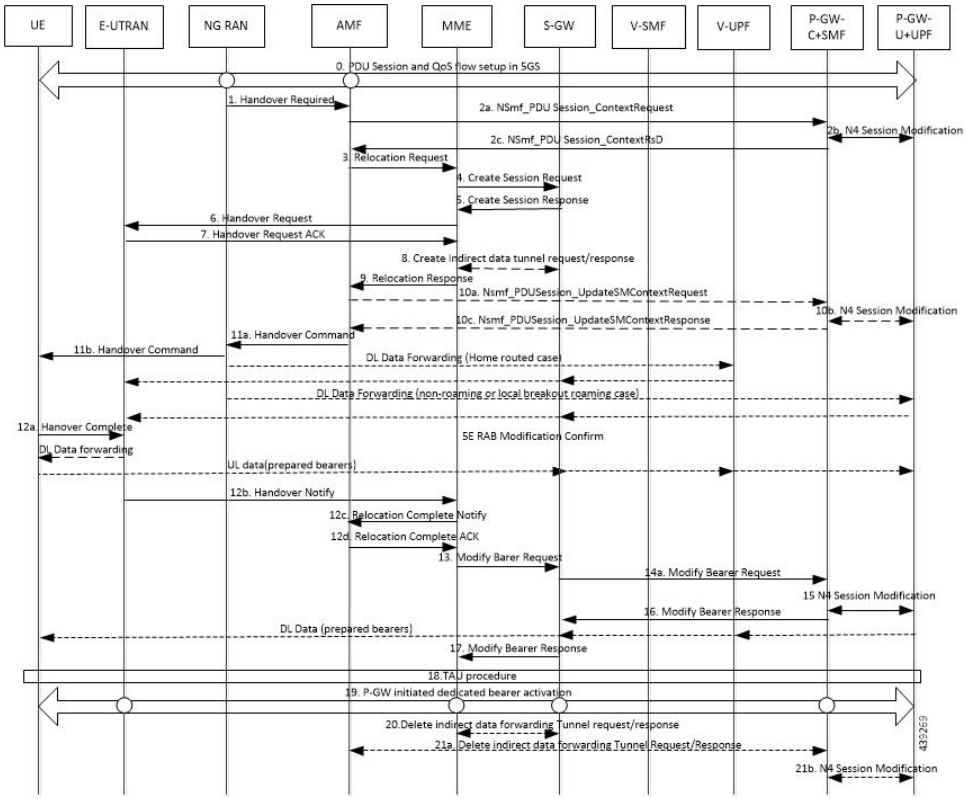


Table 54: Call Flow Description for 5G to EPS Handover with IDFT Timer

Step	Description
1	NG-RAN determines to handover UE to E-UTRAN. If NG-RAN is configured to perform inter-RAT mobility due to the IMS voice fallback that is triggered by QoS flow setup and request to set up QoS flow for IMS voice is received, then NG-RAN indicates the rejection of the QoS flow establishment. This indication is because of mobility due to fallback for the IMS voice through N2 SM information and triggers the handover to E-UTRAN. The NG-RAN sends a Handover Required message to the AMF. This message includes the details on target eNB ID, direct forwarding path availability, source to target transparent container, and inter-system handover indication. NG-RAN uses the source to target transparent container to indicate bearers for the corresponding 5G QoS flows for data forwarding.
2a	AMF sends the NSMF PDU Session Context Request to the SMF+PGW-C to provide SM Context.

Step	Description
2b	SMF+PGW-C sends the N4 session modification to PGW-U+UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules, which PCC sends, are available in the SMF. The SMF also has the bearer IDs that are received from the bearer ID allocation procedure. The SMF+PGW-C creates new PDRs for the N4 session and gets the TEID allocated for each bearer as required by the 4G system. The timer in SMF+PGW-C starts in this step. This timer monitors the resources for indirect data forwarding in UPF that are to be released. Following are the cases for the IDFT timer expiry: • Step 21a does not happen and the timer expires—The PDRs and FARs that are not required for the indirect tunnels, are removed before Step 21a. • The timer expires before or during the Steps 14a and 16—The PDRs and FARs that are not required for the indirect tunnels, are removed and the call flow continues independently. • Step 21a happens after the timer expiry—The SMF does not send the N4 Modification Request to UPF+PGW-U as the resources are released on the timer expiry.
2c	SMF+PGW-C sends the EPS bearer contexts to AMF. The bearer context is a string with the byte format, which is the base64-encoded characters, encoding the UE EPS PDN Connection IE. The SMF+PGW-C also provides the CN tunnel information to AMF for all the bearers for the uplink traffic from E-UTRAN.
3	AMF sends a Forward Relocation Request to MME. The AMF includes the mapped SM EPS UE Contexts for the PDU Sessions with and without active UP connections.
4	MME sends the Create Session Request to SGW. See S1-based handover in the normal case section in *3GPP TS 23.401, clause 5.5.1.2.2* for details.
5	SGW sends the Create Session Response to MME. See S1-based handover in the normal case section in *3GPP TS 23.401, clause 5.5.1.2.2* for details.
6	MME sends the handover request to E-UTRAN.
7	E-UTRAN sends the handover request acknowledgment to MME.
8	MME and SGW send and receive the indirect data forwarding request and response to each other.
9	MME sends the Relocation Response to AMF.
10a	In case of indirect data forwarding, AMF sends the NSMF PDU Session Update SM Context Request to PGW-C+SMF. This request is for SGW addresses and SGW DL TEIDs for data forwarding and for creating the indirect data forwarding tunnel.
10b	PGW-C+SMF sends the N4 Modification Request to UPF+PGW-U to create more PDRs and FARs. The PDRs and FARs are created to receive the redirected DL data over the indirect tunnel from NG RAN and to forward them to eNodeB. The UL PDRs have the QFI to match the forwarded DL data from NG RAN. The associated QER has the QFI to forward the data to eNodeB. Also, the FAR redirects the received data to eNodeB over the appropriate tunnel based on the QFI.

Step	Description
10c	PGW-C+SMF sends the NSMF PDU Session Update SM Context Response to AMF. This response includes details on cause, CN tunnel information for data forwarding, and QoS flows for data forwarding. PGW-C+SMF sends this response to create indirect data forwarding. Based on the correlation between QFIs and SGW addresses and TEIDs for data forwarding, the PGW-U+UPF maps the QoS flows into the data forwarding tunnels in EPC.
11a	AMF sends the Handover Command to the source NG-RAN.
11b	The source NG-RAN sends the Handover Command to UE to handover to the target access network. The UE correlates the ongoing QoS Flows with the indicated EPS Bearer IDs (EBI) that are to be set up in the handover command. If the QoS Flow associated with the default QoS rule in the PDU Session has an unassigned EBI, the UE deletes the PDU Session locally. If the QoS Flow that is associatedthat is with the default QoS rule has an assigned EBI, the UE retains the PDU session. For the QoS Flow with unassigned EBIs, the UE deletes the QoS rules and the QoS Flow level QoS parameters locally if any associated with those QoS Flows. Then, the UE notifies the impacted applications that the dedicated QoS resource has been released. The UE deletes any UE-derived QoS rules. The EBI that was assigned for the QoS Flow of the default QoS rule in the PDU Session becomes the EBI of the default bearer in the corresponding PDN connection.
12a	UE sends the notification of handover completion to E-UTRAN.
12b	E-UTRAN sends the Handover Notify request to MME.
12c	MME sends the Relocation Complete Notification to AMF.
12d	AMF sends the Relocation Complete Notification acknowledgment to MME.
13	MME sends the Modify Bearer Request to SGW.
14a	SGW sends the Modify Bearer Request to SMF+PGW-C. This request includes the information on DL TEIDs on SMF for the bearers.
15	PGW-C+SMF initiates a N4 Session Modification procedure toward the UPF+PGW-U to update the User Plane path, which implies that DL User Plane for the indicated PDU Session is switched to E-UTRAN. The PGW-C+SMF releases the resource of the CN tunnel for PDU Session in UPF+PGW-U.
16	PGW-C+SMF sends Modify Bearer Response to SGW. At this stage, the User Plane path is established for the default bearer and the dedicated EPS bearers between the UE, target eNodeB, SGW, and the PGW-U+UPF. The PGW-C+SMF uses the EPS QoS parameters as assigned for the dedicated EPS bearers during the QoS Flow establishment. PGW-C+SMF maps all the other IP flows to the default EPS bearer. If indirect forwarding tunnels are established, the PGW-C+SMF starts a timer to release the resources that are used for indirect data forwarding.
17	SGW sends Modify Bearer Response to MME.

Step	Description
18	UE initiates a Tracking Area Update procedure. See the S1-based handover in the normal case section in *3GPP TS 23.401, clause 5.5.1.2.2* for details. This procedure deregisters the old AMF for 3GPP access from HSS+UDM. Any registration that is associated with the non-3GPP access in the old AMF is not removed. It implies that an AMF that is serving the UE over both the 3GPP and non-3GPP accesses does not consider the UE as deregistered over non-3GPP access and remains registered and subscribed to subscription data updates in UDM.
19	If PCC is deployed, then PCF determines to provide the earlier removed PCC rules to the PGW-C+SMF again. With these PCC rules, the PGW-C+SMF initiates the dedicated bearer activation procedure.
20	SGW sends the Delete Indirect Data Forwarding Tunnel Request to MME. The MME sends the Delete Indirect Data Forwarding Tunnel Response to SGW.
21a	AMF initiates NSMF PDU Session Update SM Context Request service operation with an indication to release the forwarding tunnels.
21b	SMF sends the N4 Modification Request to UPF+PGW-U to delete the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed. The IDFT timer that started in Step 2b stops.

Standards Compliance

The IDFT timer support feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*
- *3GPP TS 23.401 version 12.6.0 Release 12*

Configuring the IDFT Timer

This section describes how to configure the IDFT timer.

```
config
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard enable timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
    end
exit
```

NOTES:

- **profile access**: Accesses the profile configuration.
- **test**: Accesses the profile instance.
- **eps-fallback**: Enters the EPS fallback configuration.
- **n26**: Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration
- **n2**: Enters the N2 interface, which is the NG-RAN configuration.

- **idft enable timeout**: Enters the value from 15 to 60 for the IDFT timer to expire.

EPS Fallback Guard Timer Support

Feature Description

SMF supports the guard timer to track failure in the EPS fallback. After the timer starts, it waits for the EPS fallback to happen before the bearer creation failure information is communicated to PCF.

How It Works

The EPS fallback timer starts after receiving the notification for dedicated bearer creation failure with the EPS fallback cause from gNB through AMF. In this case, SMF does not send the failure notification to PCF and waits for 5G to 4G handover to complete. Then, SMF triggers the bearer creation in 4G. The EPS fallback timer stops on the completion of the 5G to 4G handover.

In case the timer expires before the completion of the 5G to 4G handover, SMF sends a notification for dedicated bearer creation failure to PCF. Then, the new statistics counter, with the “smf_eps_fb” and “timeout” labels, is incremented. However, the 5G to 4G handover procedure continues.

Call Flows

This section includes the following call flow.

EPS Fallback Guard Timer Call Flow

This section describes the 5G to EPS fallback guard timer call flow.

Figure 48: EPS Fallback Guard Timer Call Flow

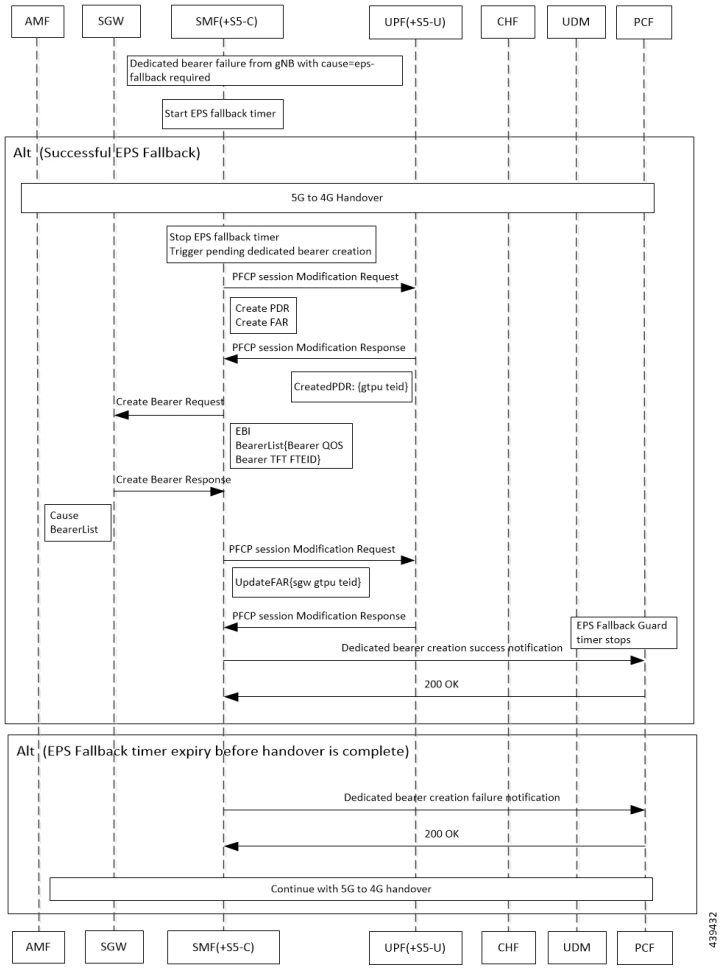


Table 55: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
In the successful EPS fallback with 5G to 4G handover scenario, Steps 3 –12 happen.	
3	EPS fallback timer stops and triggers pending dedicated bearer creation.
4	SMF(+S5-C) sends the PFCP session modification request to UPF(+S5-U).
5	PDR and FAR are created.
6	UPF(+S5-U) sends the PFCP session modification response to SMF(+S5-C).
7	The information on the created PDR with the GTP-U TEID is available.
8	SMF(+S5-C) sends the Create Bearer Request to SGW.
9	SGW sends the Create Bearer Response to SMF(+S5-C).

Step	Description
10	SMF(+S5-C) sends the PFCP Session Modification Request to UPF(+S5-U).
11	UPF(+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
12	EPS fallback guard timer stops.
13	PCF sends the “200 OK” acknowledgment to SMF(+S5-C)
In the EPS fallback timer expiry before handover completion scenario, Steps 14–16 happen.	
14	SMF(+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
15	PCF sends the “200 OK” acknowledgment to SMF(+S5-C).
16	The 5G to 4G handover procedure continues.

Standards Compliance

The EPS fallback guard timer support feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*

Configuring the EPS Fallback Guard Timer

This section describes how to configure the EPS Fallback Guard Timer feature.

```
config
  profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
  end
```

NOTES:

- **profile access**: Accesses the profile configuration.
- **test**: Accesses the profile instance.
- **eps-fallback**: Enters the EPS fallback configuration.
- **eps-fallback guard timeout**: Enters the value for the EPS fallback timer from the range of 500 to 15000 milliseconds.
- **n26**: Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration.
- **n2**: Enters the N2 interface, which is the NG-RAN configuration.
- **idft enable timeout**: Enters the value from 15 to 60 for the IDFT timer to expire.

Generating EPS Fallback Report

Table 56: Feature History

Feature Name	Release Information	Description
EPS Fallback Reporting	2024.01	SMF supports EPS Fallback Reporting functionality for PCC rules for which the EPS_FALLBACK trigger was sent by the PCF. **Default Setting**: Enabled when the compliance version 16.10.0 is set for npcf-smpolicycontrol.

Feature Description

SMF allows EPS_FALLBACK Policy Control Request trigger from PCF for EPS Fallback Reporting for PCC rules. The following functions occur:

- When the **EPSFallbackReport** is enabled in the **supported-features** list and if the PCF has armed trigger " policyCtrlReqTriggers" with the value "EPS_FALLBACK" then, SMF notifies the PCF of EPS fallback for the PCC rule referred in the "lastReqRuleData" attribute with "reqData" attribute value as EPS_FALLBACK".
- SMF includes the following in the SmPolicyUpdateContextData to indicate EPS Fallback to the PCF:
  - The "EPS_FALLBACK" value within the "repPolicyCtrlReqTriggers" attribute.
  - The affected PCC rules within the "pccRuleIds" attribute included in the "ruleReports" attribute, where the "ruleStatus" attribute is set to ACTIVE.

Important To enable the EPS Fallback Report, ensure to configure the compliance version for npcf-smpolicycontrol to 16.10. 0

How It Works

The EPS Fallback Reporting is done post the EPS Fallback. The reporting procedure is done only for pccRules for which the EPS_FALLBACK trigger was sent by PCF and resource setup is also successful post EPS Fallback.

Call Flows

The following call flow depicts the EPS Fallback Report handling procedure.

Figure 49: EPS Fallback Reporting Call Flow

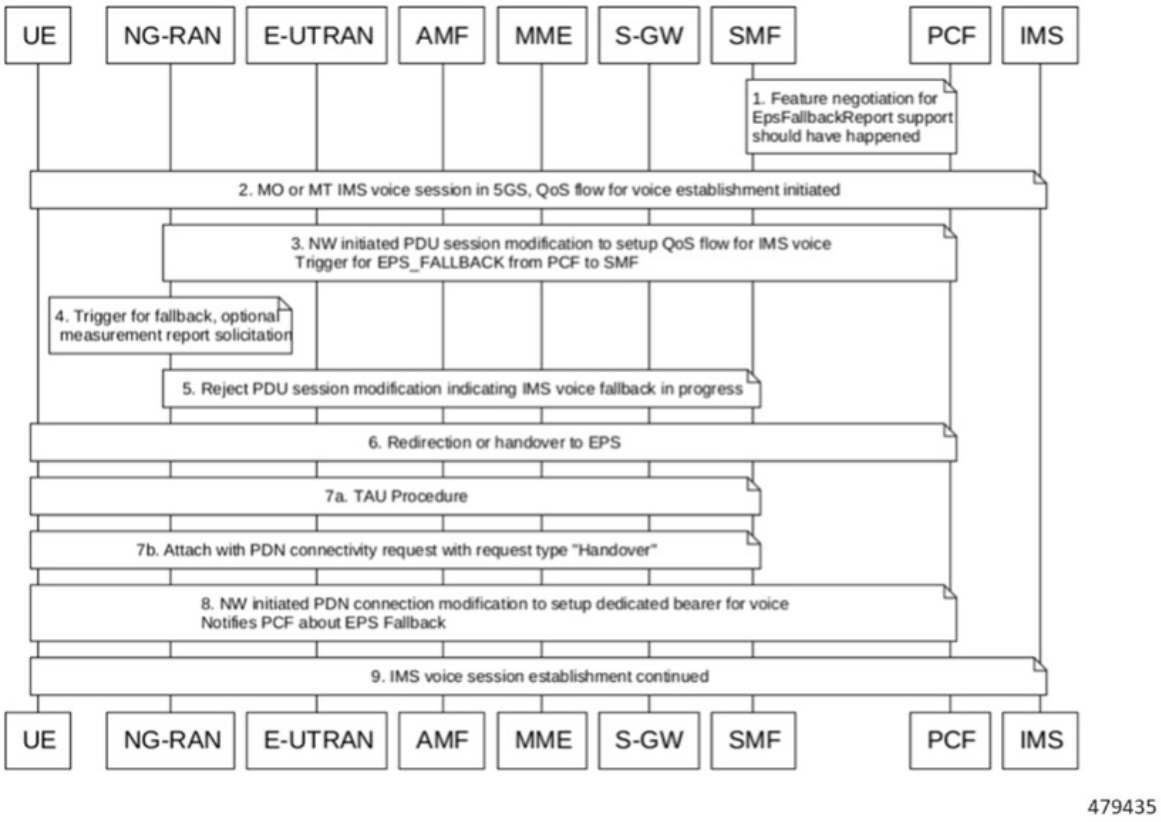


Table 57: EPS Fallback Reporting Call Flow Description

Step	Description
1	The feature negotiation for EPSFallbackReport support should have happened between SMF and PCF during session establishment.
2	The UE initiates Mobile-Originated (MO) or a Mobile-Terminated (MT) IMS Voice establishment procedure with NG-RAN in 5GS.
3	The Network-initiated PDU Session modification request to set up QoS flow for Voice reaches the NG-RAN. PCF also arm SMF with an EPS_FALLBACK trigger for EpsFallbackReport.
4	The NG-RAN is configured to support the EPS fallback for IMS Voice. Based on the UE functionalities, indication from the AMF to redirect EPS fallback for voice, network configuration, and radio conditions, the NG-RAN triggers fallback to EPS. The NG-RAN initiates measurement report solicitation from the UE including E-UTRAN as target.

Step	Description
5	The NG-RAN rejects the PDU Session modification request that is received in Step 3 with an indication that mobility due to fallback for IMS voice is ongoing. The NG-RAN indicates the rejection of the PDU session modification to configure QoS flow for IMS voice that is received in Step 3 as PDU Session Response message toward the SMF through the AMF. This message includes the details on the ongoing mobility due to fallback for IMS voice. The SMF maintains the PCC rules that are associated with the QoS flows. For a roaming scenario, the PDU Session Response message is sent toward H-SMF through V-SMF. Or NG-RAN responds with a configured cause which it might trigger fallback to EPS. If the cause sent by gNB matches with EPS Fallback causes configured at SMF, it continues to behave as mentioned in steps from step. 6 onwards. **Note** If configuration at SMF always checks for the configured cause even if gNB rejects the N2 message with cause “IMS voice EPS fallback or RAT fallback triggered”.
6	Based on the UE functionalities, the NG-RAN initiates handover to the EPS. The SMF reports change of the RAT type, if the PCF is subscribed for it. A timer starts to track failure in the EPS fallback. After the timer expires, the SMF notifies the PCF about the dedicated bearer creation failure.
7a	For 5GS to EPS handover, the UE initiates the TAU procedure.
7b	The UE attaches the PDN connectivity request with the “handover” request type.
8	After the completion of the 5GS to EPS handover procedure, the SMF or PGW-C reinitiates the configuration of the dedicated bearer for IMS voice and mapping the 5G QoS to EPC QoS parameters. The SMF notifies about the EPS fallback, Successful Resource Allocation, and Access Network Information, if the PCF is subscribed for it.
9	The IMS voice session establishment continues.

Note In case where the feature is enabled on SMF but is not mentioned by PCF in the supported-features list during initial negotiation but the PCF still sends PolicyControlRequestTrigger as EPS_FALLBACK, even then SMF will be armed with this trigger and EPS Fallback Report will be sent to PCF in case of EPS Fallback.

Bearer Modification for EPS Session on SMF

Table 58: Feature History

Feature Name	Release Information	Description
HSS-Initiated Bearer QoS Modification	2023.04	SMF supports the HSS Initiated Bearer QoS Modification procedure to modify APN-AMBR and optionally one or more of the EPS Bearer QoS parameters. **Default Setting**: Enabled – Always-on

Feature Description

EPS Interworking through 5G Core Network

SMF supports modification of EPS bearer that a PCF or an MME initiates. The SMF+PGW handles the following triggers for this feature:

- QoS modifications.
- RAT, ULI, and SGW modifications.
- UE time zone modifications.

SMF Interworking with Diameter Interfaces

SMF supports modification of EPS bearer for the tracking area update information through the following features:

- PCRF-initiated RAR
- E-UTRAN PDN modification with S-GW change
- E-UTRAN PDN modification without S-GW change
- HSS-initiated QoS modification

How it Works

The bearer modification for an EPS session on SMF works with the following modifications:

- PCF and MME-Initiated Bearer Modifications for EPS session on SMF—These procedures are used either when one or multiple EPS Bearer QoS parameters QCI, GBR, MBR, or ARP are modified or to modify the APN-AMBR. The PCF-initiated or the MME-initiated bearer modification procedures do not support the modification from a QCI of non-GBR resource type to a GBR resource type QCI and vice versa.

- X2 and S1 Based Handover for EPS Session Connected to SMF—The X2-based handover procedure is used to hand over a UE from a source eNodeB to a target eNodeB using X2. In this procedure, the MME is unchanged and the MME determines to relocate the SGW.

  The S1-based handover procedure is used when the X2-based handover cannot be used. The source eNodeB initiates a handover by sending the Handover Required message over the S1-MME reference point. This procedure may relocate the MME or the SGW.

Call Flows

This section includes the following call flows:

- PCF-Initiated Bearer Modification for EPS session on SMF call flow
- MME-Initiated Bearer Modification for EPS session on SMF call flow
- X2 and S1 Based Handover for EPS Session Connected to SMF call flow

PCF-initiated Bearer Modification for EPS session on SMF

This section describes the PCF-Initiated Bearer Modification for EPS session on SMF call flow.

Figure 50: Call Flow for PCF-Initiated Bearer Modification

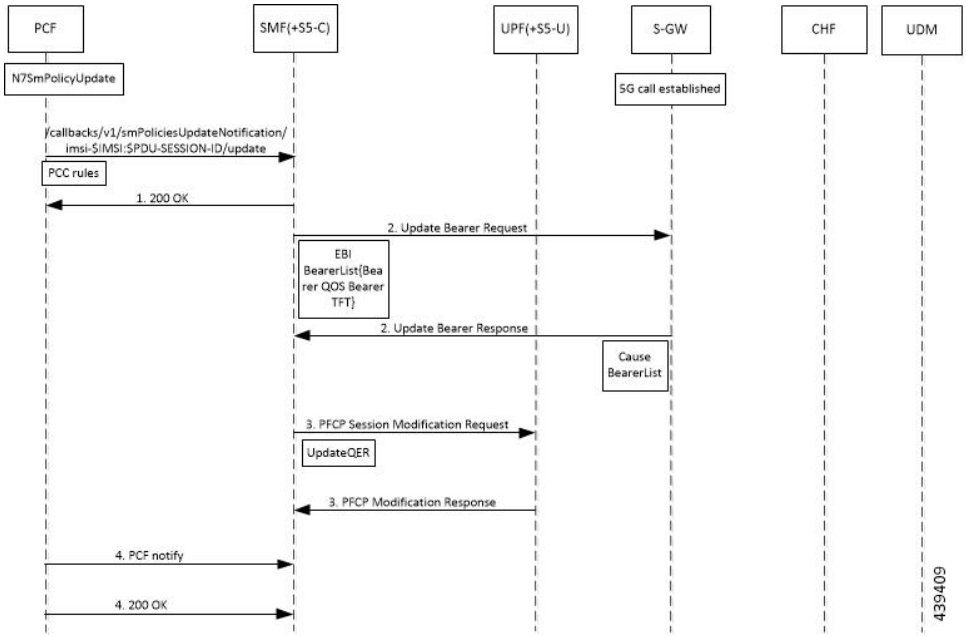


Table 59: Call Flow Description for PCF-Initiated Bearer Modification

Step	Description
1	PCF initiates the N7 Policy Update Notify with the updated parameters of QoS or TFT toward SMF.
2	SMF sends the “200 OK” acknowledgment to PCF. The PCC rules that the PCF provides are mapped to TFTs for the modified dedicated bearer. The associated QoS is mapped to 4G QoS.
3	SMF sends the Update Bearer Request to SGW.

Step	Description
4	SGW sends the Update Bearer Response to SMF with EPS Bearer ID and the modified QoS or TFT for the associated bearer.
5	SMF initiates the PFCP Modification request toward UPF.
6	UPF sends the PFCP Modification Response to SMF with updated QER.
7	SMF sends the PCF Notify message to PCF.
8	PCF sends the “200 OK” acknowledgment to SMF.

MME-initiated Bearer Modification for EPS session

This section describes the MME-Initiated Dedicated Bearer Modification for EPS session on SMF call flow.

Figure 51: Call Flow for MME-Initiated Bearer Modification

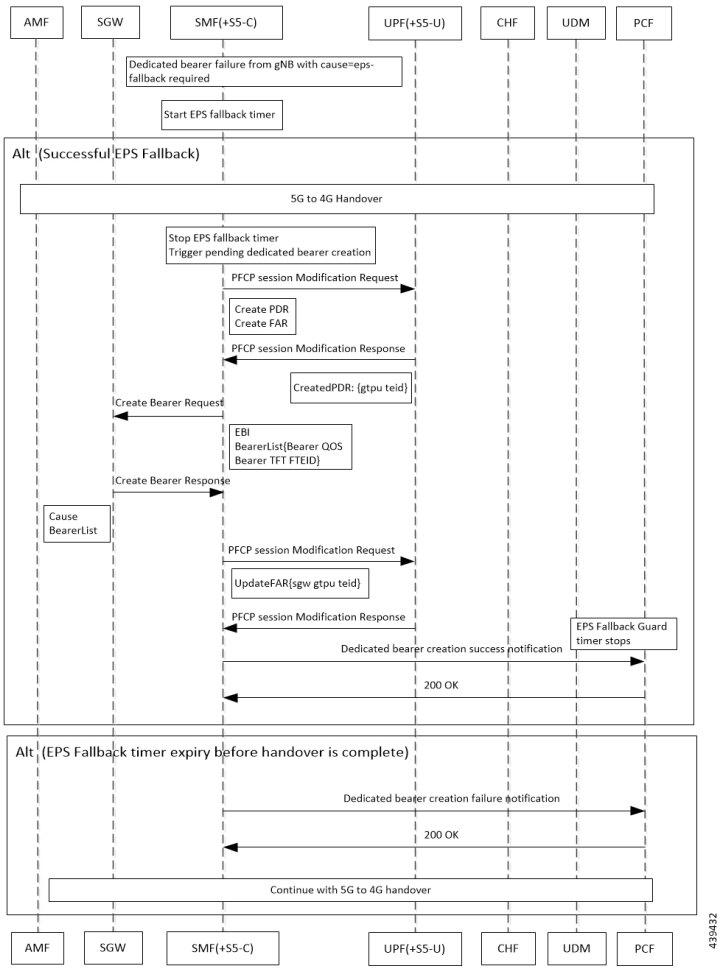


Table 60: Call Flow Description for MME-Initiated Bearer Modification

Step	Description
1	HSS sends an Insert Subscriber Data message to the MME. The subscription data includes the details on IMSI, EPS subscribed QoS (QCI and ARP), and the subscribed UE-AMBR and APN-AMBR.
2	If the subscribed UE-AMBR is modified, the MME calculates a new UE-AMBR value and sends the Modify Bearer Command to SGW.
3	SGW sends the Modify Bearer Command message to the SMF or PDN GW. This message includes the details on EPS Bearer Identity, EPS Bearer QoS, and APN-AMBR.
4	SMF or PDN GW sends the updated APN-AMBR to PCF.
5	PCF sends the updated PCC decision to the SMF or PDN GW. The PCF modifies the APN-AMBR that is associated with the default bearer in response to the SMF or PDN GW.
6	SMF sends the Update Bearer Request to SGW.
7	SGW sends the Update Bearer Request to MME. This request message includes the details on EBI, EPS Bearer QoS, TFT, and APN-AMBR.
8	MME sends the Update Bearer Response to SGW.
9	SGW sends the Update Bearer Response as acknowledgment for the bearer modification to the SMF or PDN GW. The response message includes the details on EBI and user location information.
10	UPF sends the PFCP Session Modification Response to SMF. Based on the PCC decision provision message (QoS policy) that is received from the PCF, the SMF or PDN GW initiates the dedicated bearer modification procedure. SMF or PDN GW uses the QoS policy to determine if a service data flow is to be added or removed from an active bearer or if the authorized QoS of a service data flow is changed.
11	UPF updates the PFCP parameters and sends a PFCP Session Modification Response to the SMF or PDN GW. UPF confirms the successful modification of the PFCP session.
12	SMF or PDN GW notifies PCF on the requested PCC decision whether it was enforced or not.
13	PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

X2 and S1 based Handover for EPS Session Connected to SMF

This section describes the X2 and S1-based handover for EPS session connected to SMF.

Figure 52: Call Flow for X2 and S1 based Handover for EPS Session Connected to SMF

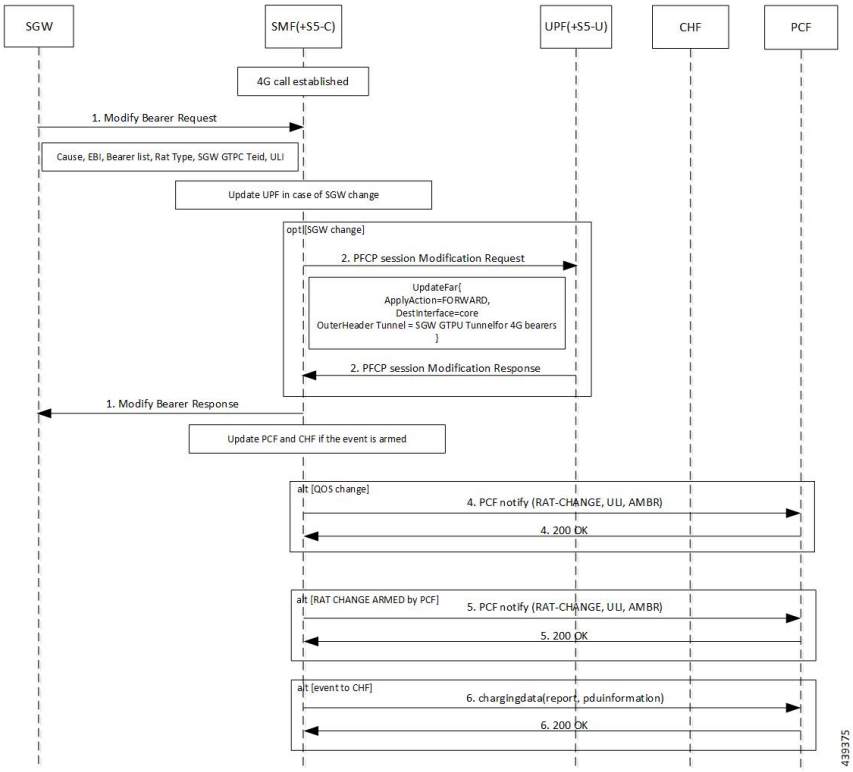


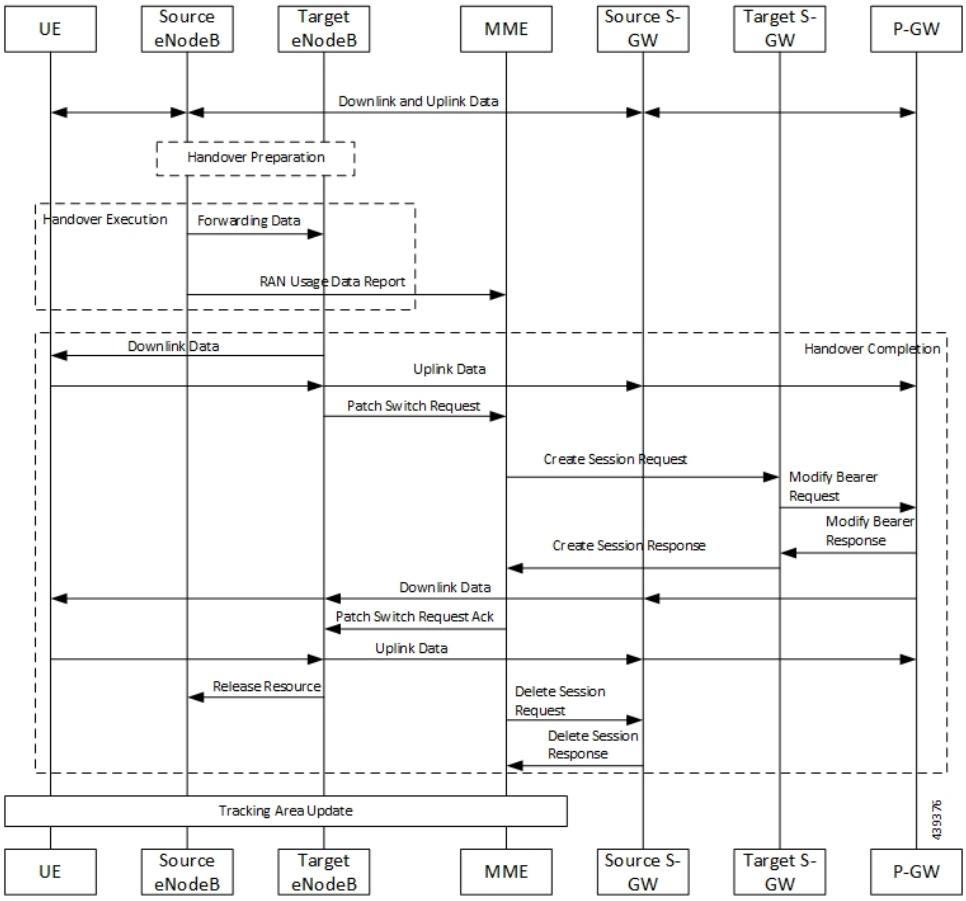
Table 61: Call Flow Description for X2 and S1 based Handover

Step	Description
1	The SGW sends the Modify Bearer Request to the SMF. This request includes the user location information IE, UE time zone IE, and the serving network IE per PDN connection to the associated PDN GWs information that is received from the MME.
2	In case of change in S-GW, SMF or PGW-C sends the PFCP Session Modification Request to the UPF.
3	If Step 2 occurs, the UPF sends the PFCP Session Modification Response to SMF or PDN GW.
4	After receiving the response from the UPF, the SMF or PGW-C sends the Modify Bearer Response to S-GW.
5	If PCF has armed notification for QoS modification, the SMF or PGW-C sends a notification to the PCF.
6	If Step 5 occurs, the PCF sends the “200 OK” acknowledgment to the SMF or PGW-C.
7	If PCF has armed notification for ULI or RAT modifications, SMF or PDN GW sends a notification to PCF.
8	If Step 7 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.
9	If CHF has armed notification for QoS, ULI, or RAT modifications, SMF or PDN GW sends a notification to PCF.

Step	Description
10	If Step 9 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

The following call flow shows the X2-based handover with S-GW relocation:

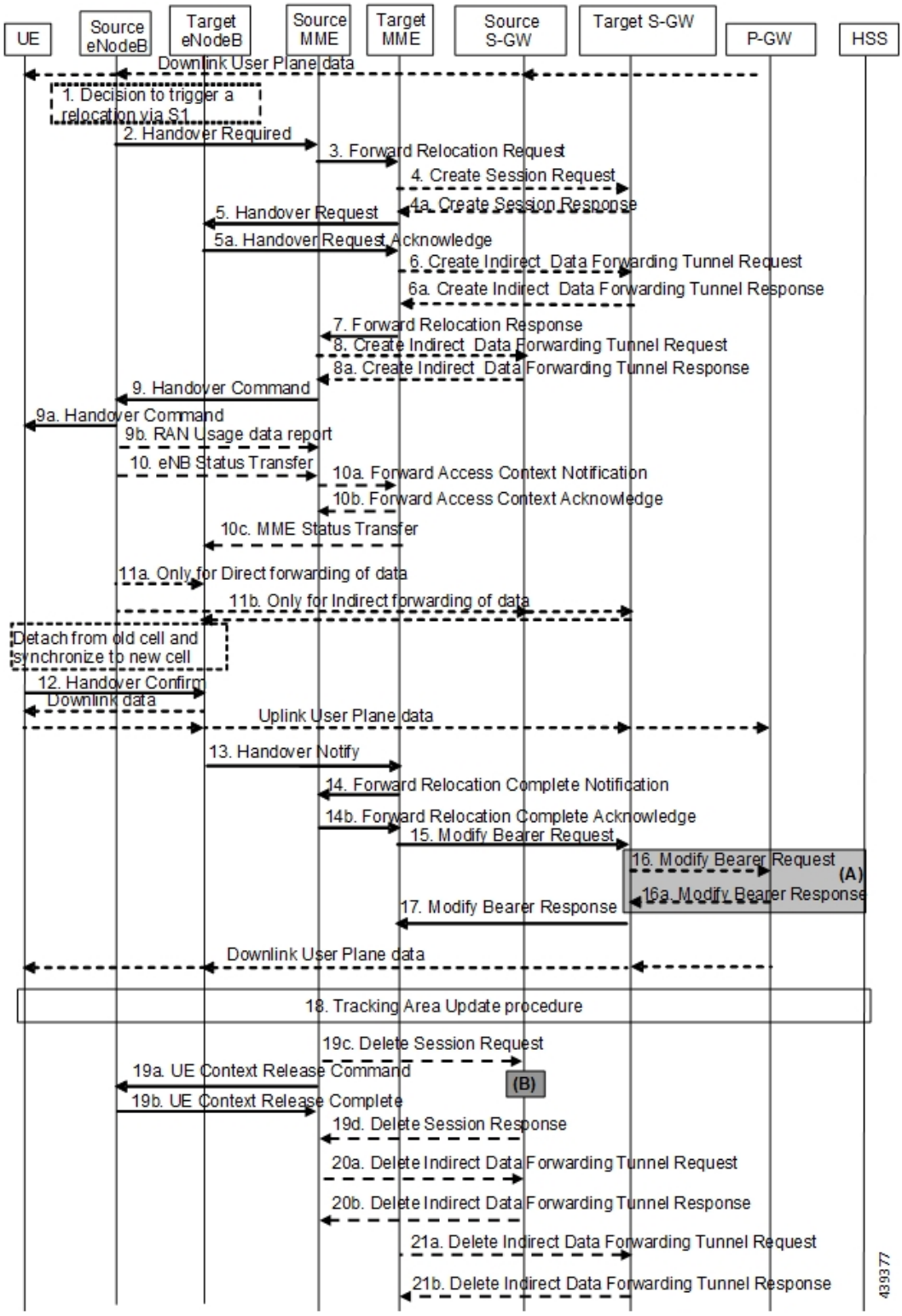
Figure 53: X2-Based Handover with SGW Relocation Call Flow



For call flow description, see the section 5.5.1.1.3 "X2-based handover with Serving GW relocation" from *3GPP TS 23.401*.

The following call flow shows the S1-based handover:

Figure 54: S1-based Handover Call Flow



For call flow description, see section 5.5.1.2.2 "S1-based handover, normal" from *3GPP TS 23.401, version 15.8.0*.

PCRF-Initiated RAR / CCAU

The following figure shows the call flow for E-UTRAN Network Credit Control Answer Update (CCAU) or Re-Authorization Request (RAR) initiated Update Bearer Request (UBR).

Figure 55: Call Flow for E-UTRAN Network (PCRF) CCAU/RAR Initiated UBR

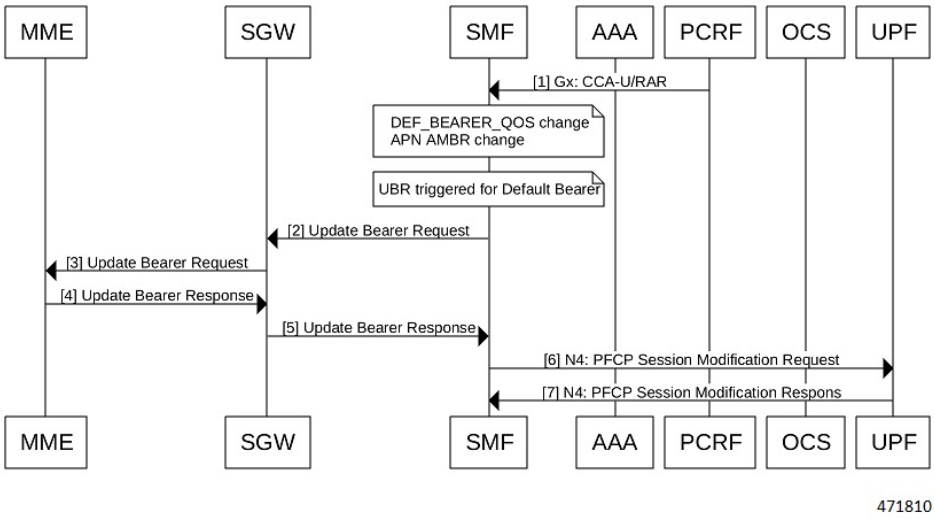


Table 62: Call Flow Description for PCRF-initiated CCAU or RAR

Step	Description
1	PCRF sends RAR to SMF or CCAU to SMF with modified Default Bearer Qos and/or APN AMBR change.
Note UBR is triggered for the default bearer as there's change in either Default Bearer Qos and/or APN AMBR.	
2	SMF sends Update Bearer Request to S-GW with updated Default Bearer Qos and/or updated APN AMBR.
3	SGW sends the Update Bearer Request to MME.
4	MME sends the Update Bearer Response to S-GW.
5	SGW sends the Update Bearer Response to SMF.
6	SMF sends N4 PFCP Session Modification Request to the UPF to update the Bearer level information (if default bearer Qos is changed) and/or APN AMBR QER (if APN AMBR is changed).
7	UPF sends N4 PFCP Session Modification response to SMF.

E-UTRAN PDN Modification with S-GW Change

The following figure shows the call flow for PDN modification with S-GW change.

Figure 56: Call Flow for PDN Modification with S-GW Change

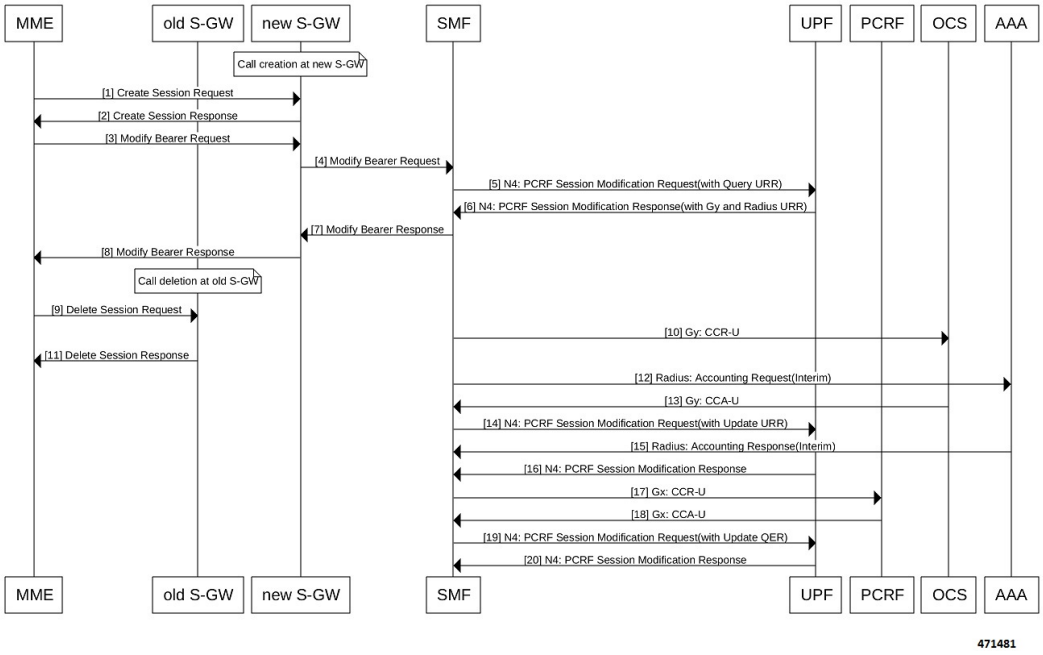


Table 63: Call Flow Description for PDN Modification with S-GW Change

Step	Description
1	As part of the call creation at the new S-GW, the MME sends the Create Session Request to the new S-GW.
2	The new S-GW responds with the Create Session Response to MME.
3	MME sends Modify Bearer Request to new S-GW.
4	The new S-GW forwards Modify Bearer Request to SMF.
5	SMF sends Session Modification Request with Query URR to UPF based on event triggers. **Note** serv-node-change event triggers for S-GW change.
6	UPF responds with the N4: PCRF Session Modification Response with Gy and RADIUS URR to SMF based on the Gy and RADIUS configuration, which can be enabled or disabled.
7	SMF responds with Modify Bearer Response to new S-GW.
8	New S-GW forwards Modify Bearer Response to MME.
9	As part of Call deletion at the old S-GW, MME sends Delete Session Request to the new S-GW.
10	SMF sends CCR-U to OCS and Accounting Request (Interim) to AAA.

Step	Description
11	Old S-GW sends Delete Session Response to MME.
12	OCS and AAA respond to SMF with CCA-U and interim Accounting Response respectively.
13	SMF sends PCRF Session Modification Request with update URR to UPF.
14	UPF responds to SMF with PCRF Session Modification Response.
15	SMF sends CCR-U towards PCRF if event trigger is armed. **Note** AN_GW_CHANGE event triggers for S-GW change.
16	PCRF responds to SMF with CCA-U.
17	SMF sends PCRF Session Modification Request with Update QER to UPF.
18	SMF sends PCRF Session Modification Response to UPF.

E-UTRAN PDN Modification without S-GW Change

The following figure shows the call flow derived from the 3GPP reference for PDN modification without S-GW change.

Figure 57: Call Flow for PDN Modification without S-GW Change

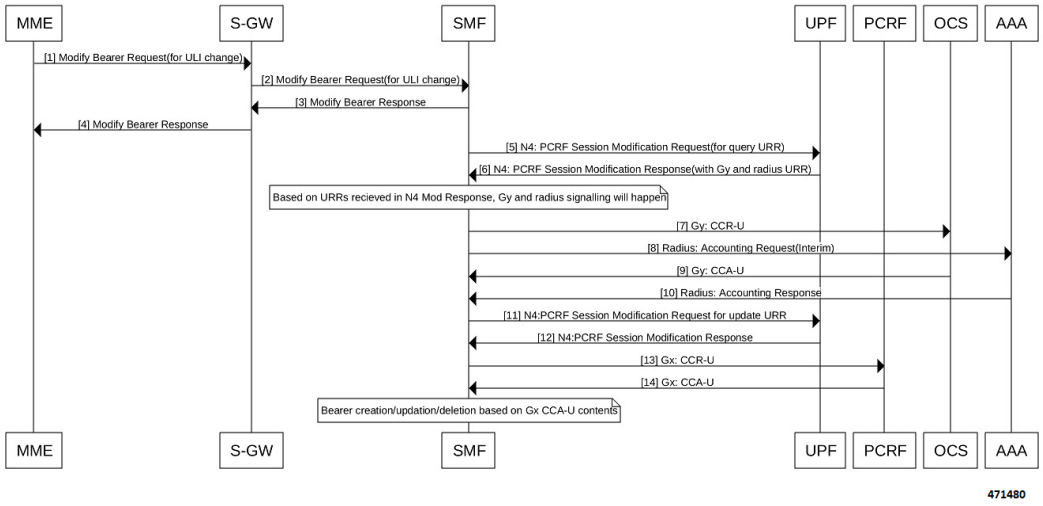


Table 64: Call Flow Description for PDN Modification without S-GW Change

Step	Description
1	MME sends Modify Bearer Request (for ULI change) to S-GW.
2	S-GW forwards Modify Bearer Request to SMF. **Note** If a session is present and not in disconnecting state, SMF sends success and does further processing.

Step	Description
3	SMF sends Modify Bearer Response to S-GW.
4	S-GW forwards Modify Bearer Response to MME.
5	SMF sends the N4 Session Modification Request for query Usage Reporting Rule (URR) to UPF based on event triggers. **Note** user-loc-change event triggers for ULI change
6	UPF responds with the N4 Session Modification Response with Gy and RADIUS URR, SMF based on Gy, and RADIUS configuration, which can be enabled or disabled.
7	Based on URRs received in N4 Session Modification Response, Gy, and RADIUS signaling happens.
8	SMF sends CCR-U to OCS and RADIUSs Accounting Request to AAA.
9	OCS responds with CCA-U and AAA with RADIUS Accounting Response.
10	SMF sends N4 Session Modification Request for update URR to UPF.
11	UPF sends N4 Session Modification Response to SMF.
12	If an event trigger is armed, SMF sends CCR-U to PCRF. **Note** USER_LOCATION_CHANGE event trigger for ULI change.
13	PCRF then sends CCA-U to SMF.
14	Bearer creation, update, or deletion happens based on Gx CCA-U contents.

HSS Initiated Bearer QoS Modification for SMF with Diameter Interfaces

The HSS Initiated Bearer QoS Modification procedure is used to modify APN-AMBR and optionally one or more of the EPS Bearer QoS parameters. For example, the EPS Bearer QoS parameters can be QCI or the ARP of the default EPS Bearer. If the HSS changes the default Bearer QCI or the ARP and APN-AMBR, the HSS initiates such message to the MME, which then generates the Modify Bearer Command (MBC) toward the P-GW through S-GW.

The following call flow illustrates the procedure for HSS Initiated Bearer QoS Modification.

Figure 58: Call Flow for HSS Initiated Bearer QoS Modification

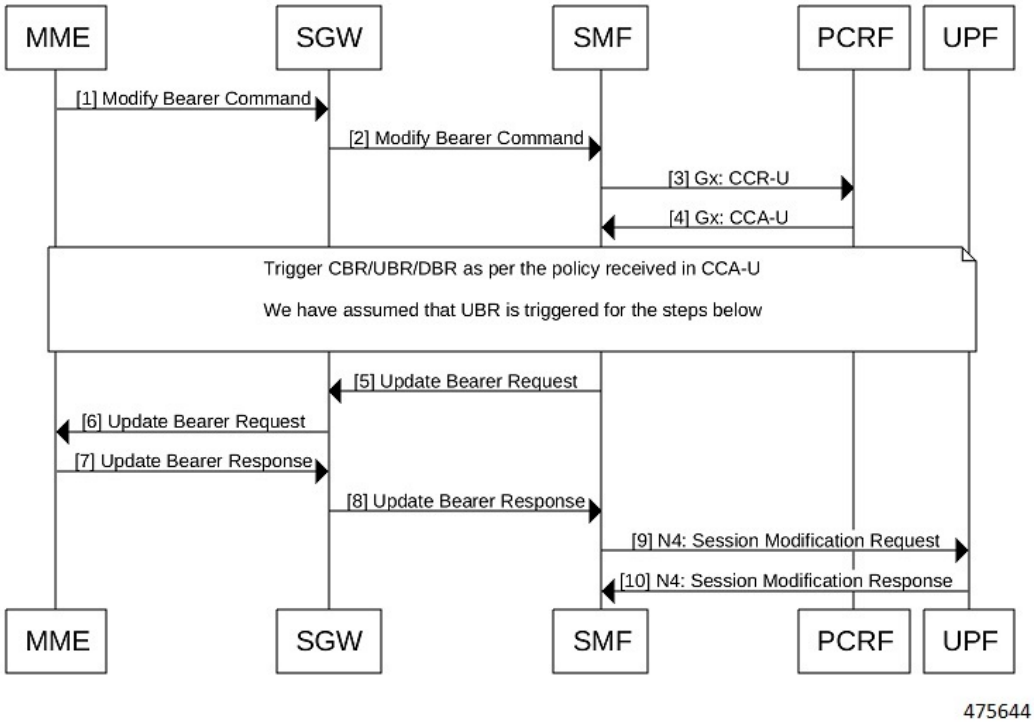


Table 65: Call Flow Description for HSS Initiated Bearer QoS Modification

Step	Description
1	MME sends Modify Bearer Command to S-GW as part of the HSS Initiated Subscribed QoS Modification procedure.
2	S-GW sends the Modify Bearer Command to SMF.
3	SMF sends Gx CCR-U to PCRF with associated event triggers of APN AMBR change and optionally default bearer qos change if they are subscriber by PCRF. The requested Default Bearer QoS, APN-AMBR are sent to the PCRF, and the authorized values from the PCRF is applied on the subscriber along with the other policies. For example, Dynamic Rules gets applied. and optionally default Bearer QoS change if they are subscriber by PCRF.
4	PCRF sends the Gx CCA-U to SMF. **Note** All the charging support applicable as part of CCA-U and N4 communication continues through Gy/RADIUS triggers.
Note	Based on the policy received from PCRF, either CBR, UBR, or DBR procedure gets triggered.
5	SMF sends the Update Bearer Request to the S-GW with a new APN AMBR and default bearer QoS values.

Step	Description
6	SGW sends the Update Bearer Request to MME with a new APN AMBR and default bearer QoS values.
7	MME sends the Update Bearer Response to the S-GW.
8	S-GW sends the Update Bearer Response to the SMF.
9	SMF sends PFCP Session Modification Request to UPF to update APN AMBR QER and Bearer Level Information if APN AMBR and Default Bearer QoS are respectively updated by PCRF.
Note	Along with the Update QER, when there is a default bearer QoS change through CCA-U or with Modify Bearer Command when PCRF is disabled, PFCP Session Modification Request to UPF have Update PDRs, which is generic for other procedures.
10	UPF sends PFCP Session Modification Response to SMF.

Modify Bearer Command with Rulebase Change

The following call flow illustrates the procedure for modification of Bearer command with Rulebase change that is received from Policy Server in Gx CCA-U.

Figure 59: Call Flow for Bearer Command with Rulebase Change Modification

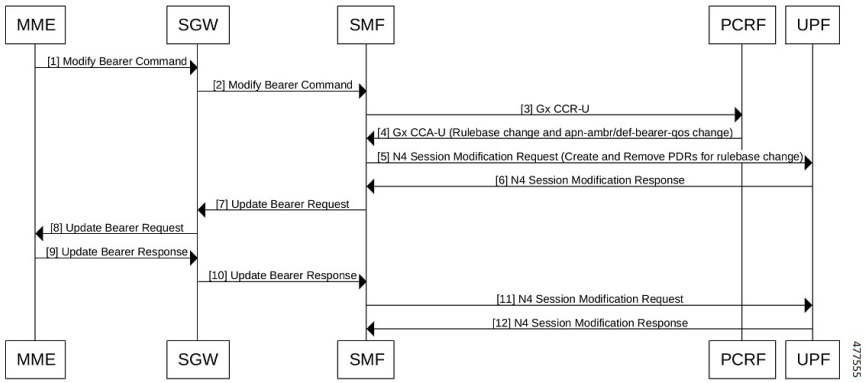


Table 66: Call Flow Description for Bearer Command with Rulebase Change Modification

Step	Description
1	MME sends Modify Bearer Command to S-GW as part of HSS Initiated Subscribed QoS Modification procedure.
2	S-GW sends Modify Bearer Command to SMF.
3	SMF sends Gx CCR-U to PCRF with associated event triggers of APN AMBR change and optionally default bearer QoS change if they are subscriber by PCRF.
4	PCRF sends Gx CCA-U to SMF with Rulebase change as well as APN-AMBR and default Bearer QoS change.

Step	Description
5	SMF sends N4 Session Modification Request to UPF with Create and Remove PDRs for Rulebase change.
6	UPF sends N4 Session Modification Response
7	SMF sends Update Bearer Request to SGW with new APN AMBR and default Bearer QoS values.
8	S-GW sends Update Bearer Request to MME with new APN-AMBR and default Bearer QoS values.
9	MME sends Update Bearer Response to S-GW.
10	S-GW sends Update Bearer Response to SMF.
11	SMF sends PFCP Session Modification Request to UPF to update APN-AMBR QER and Bearer Level Information if APN AMBR and Default Bearer QoS are respectively updated by PCRF.
Note	Along with Update QER, when there is a default bearer QOS change through CCA-U or with MBC when PCRF is disabled, PFCP Session Modification Request to UPF also has Update PDRs which is generic for other procedures
12	UPF sends PFCP Session Modification Response to SMF.

Modify Bearer Command Failure

The following call flow illustrates the procedure for failure of modify Bearer command.

Figure 60: Call Flow for Modify Bearer Command Failure

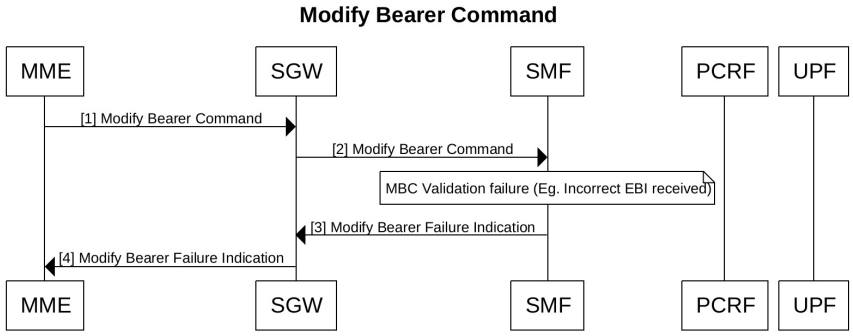


Table 67: Call Flow Description for Modify Bearer Command Failure

Step	Description
1	MME sends Modify Bearer Command to S-GW as part of HSS Initiated Subscribed QoS Modification procedure.
2	S-GW sends Modify Bearer Command to SMF.
Note	MBC validation failure oocurs. For example, Incorrect EBI is received in Modify Bearer Command
3	SMF sends Modify Bearer Failure Indication to S-GW.

Step	Description
4	S-GW sends Modify Bearer Failure Indication to MME.

Modify Bearer Command Retransmission Handling

MBC retransmissions are handled as following in these scenarios:

- If retransmission is received when MBC is still in progress or MBC is processed successfully, the retransmission is dropped with appropriate logs and statistics.
- If retransmission is received when MBC has result in MB Failure Indication, SMF responds with the cached MB Failure Indication.
- If retransmission is received after affinity is lost at smf-service, it is treated as a new MBC.

Modify Bearer Command Scenarios and Associated UBReq Values

In the standard MBC scenarios with policy servers the values of **APN-AMBR** and **Def-bearer-QOS** authorized from PCRF are the final values to be sent in UBReq toward S-GW. However, for a few exceptional MBC scenarios the behavior is different. The following table describes these scenarios.

Scenario	Description
MBC with Empty Gx CCA-U	UBR is triggered with earlier PCRF authorized values.
Due to no Event trigger for APN-AMBR and def-bearer-qos change there is no Gx CCR-U for MBC	UBR is triggered with values that are received in MBC.
MBC with same APN-AMBR and def-bearer-qos values as the existing session values. Hence, no Gx CCR-U for MBC.	UBR is triggered with the existing session values. **Note** As there is no change to be communicated to the UPF, N4 modification is not required after UBR .
MBC with different APN-AMBR and def-bearer-qos values however values that are received from PCRF in Gx CCA-U are the same as the existing session values	UBR is triggered with values that are received from PCRF **Note** As there is no change to be communicated to the UPF, N4 modification is not required after UBR .
No Gx config: UBR triggered with values that are received in MBC	UBR is triggered with values that are received in MBC.
Gx CCA-I failure with action continue, followed by MBC: UBR triggered with values that are received in MBC	UBR is triggered with values that are received in MBC.
MBC's Gx CCA-U failure with action continue: UBR triggered with values that are received in MBC.	UBR is triggered with values that are received in MBC.

Standards Compliance

The Bearer Modification for EPS Session on SMF feature complies with the following standards:

- *3GPP TS 23.401*
- *3GPP TS 23.502 V16.1.1 (2019-06)*
- *3GPP TS 29.274, version 15.8.0*

Session Management Procedures for EPS and 5GC Interworking

Feature Description

The 5G Session Management procedures defined in *3GPP TS 23.502* ensure that the EPS interworking is successful when the UE moves to an LTE 4G radio after performing the initial attach to a 5G NR radio.

Support for Number of Packet Filters in NAS Message

The UE sends the Number of packet filter IE to the SMF in PDU Establishment and Modification request messages. By default, the UE sends a maximum of 16 packet filters.

The UE supports more than 16 packet filters in the following scenarios:

- When the UE is attaching to the SMF in N1 mode.
- When the initial attach to the SMF in S1 mode is complete and the 4G to 5G handover is ongoing.

The SMF sends the maximum filters to the PCF in PolicyCreateControl in "NumOfPackFilter" field. If the Number of packet filter IE is received from the UE in N1 mode, then the SMF uses the “Maximum number of supported filters” field in PDU establishment request. If this IE is not received from the UE in N1 mode or if the received value is lesser than 16, the SMF sends the max filters as 16. If the UE attaches to the SMF in S1 mode and the 4G to 5G or 5G to 4G handover is ongoing, the SMF sends the default value, that is, 16 packet filters.

If there is any change in the packet filter value, then the SMF sends the new value to the PCF through PolicyUpdate message along with NUM_OF_PACKET_FILTER trigger.

The SMF controls the maximum filters allowed per PDU session based on the numOfPackFilter IE. If the number of packet filters crosses the maximum allowed by the UE, the SMF caps the packet filters. This means that the SMF drops the PCC rules when the limit crosses and sends the rule report with INCOR_FLOW_INFO failure code.

Note Currently, the 3GPP specification doesn't include appropriate failure code for INCOR_FLOW_INFO. When it is available in the 3GPP specification, the failure code will be updated accordingly.

Maximum supported filters are only valid for dynamic rules and not for static and predefined rules.

The "pcc_rule_report_max_supported_filter" statistics is introduced under the policy_pcc_rule_report category. This statistics is incremented if the PCC rule report is generated upon reaching the maximum supported filters.

Support for PCF ID in SmContextCreate

The AMF includes the PCF ID in the Nsmf_PDUSession_CreateSMContext Request. The PCF ID identifies the Home Policy Control Function (H-PCF) in the non-roaming case and the Visited Policy Control Function (V-PCF) in the local breakout roaming case. See the 3GPP specification 23.501, section 6.3.7.1 for more details on when the AMF forwards the PCF ID to the SMF.

When the SMF receives the PCF ID, use the following CLI configuration in the PCF network profile to control the SMF behaviour in using the PCF ID.

UseAmfProvidedPCF [True/False]

The default behaviour is to use the PCF ID provided by AMF in SmContextCreate.

If the PCF ID provided by AMF is not reachable, the SMF behaves as per the configured failure handling template. In this case, it uses the static configuration.

Support for DNN Selection Mode in SmContextCreate

The SMF uses the DNN Selection Mode for deciding whether to accept or reject the UE request.

The SMF uses the DNN Selection Mode for deciding whether to retrieve the Session Management Subscription data. In case the DNN, S-NSSAI of the HPLMN is not explicitly subscribed, the SMF uses the local configuration instead of the Session Management Subscription data.

Note The preceding use case is not supported.

The SMF validates the IE present in SmContextCreate data. If there is a DnnSelectionMode failure due to the mismatch between DnnSelectionMode and the configured CLI, the SMF does not proceed with the registration. When the DnnSelectionMode failure is observed, the “disc_pdusetup_sm_cxt_unsupported_ie" is incremented as part of the disconnect reasons.

DnnSelectionMode Type	Description
Not Present	The SMF sends the subscription request to fetch the subscription data.
Verified	The SMF sends the subscription request to fetch the subscription data.
UE_DNN_NOT_VERIFIED	If the **dnn-selection-mode verified ue-provided** CLI command is configured as shown in the following configuration, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.
NW_DNN_NOT_VERIFIED	If the **dnn-selection-mode verified network-provided**CLI is configured, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.

The SMF uses the following sample configuration to configure the DnnSelectionMode:

```
config
  profile smf profile_name
    dnn-selection-mode [ verified ue-provided | network-provided ]
    end
```

One or more DnnSelectionMode types can be configured. By default, the DnnSelectionMode is verified.

Post the subscription request, if no subscription data is fetched from UDM, the SMF falls back to the local DNN profile for subscription data. Neither the subscription data is fetched from the UDM nor the local configuration is present, the SMF sends the SmContextCreateError with subscription failure.

How it Works

Call Flows

This section describes the 5G Session Management procedures to support EPS and 5GC interworking.

PDU Session Creation Call Flow

This section describes the PDU Session Creation procedure as specified in *3GPP TS 23.502, section 4.3.2.2.1*.

Figure 61: PDU Session Creation Call Flow

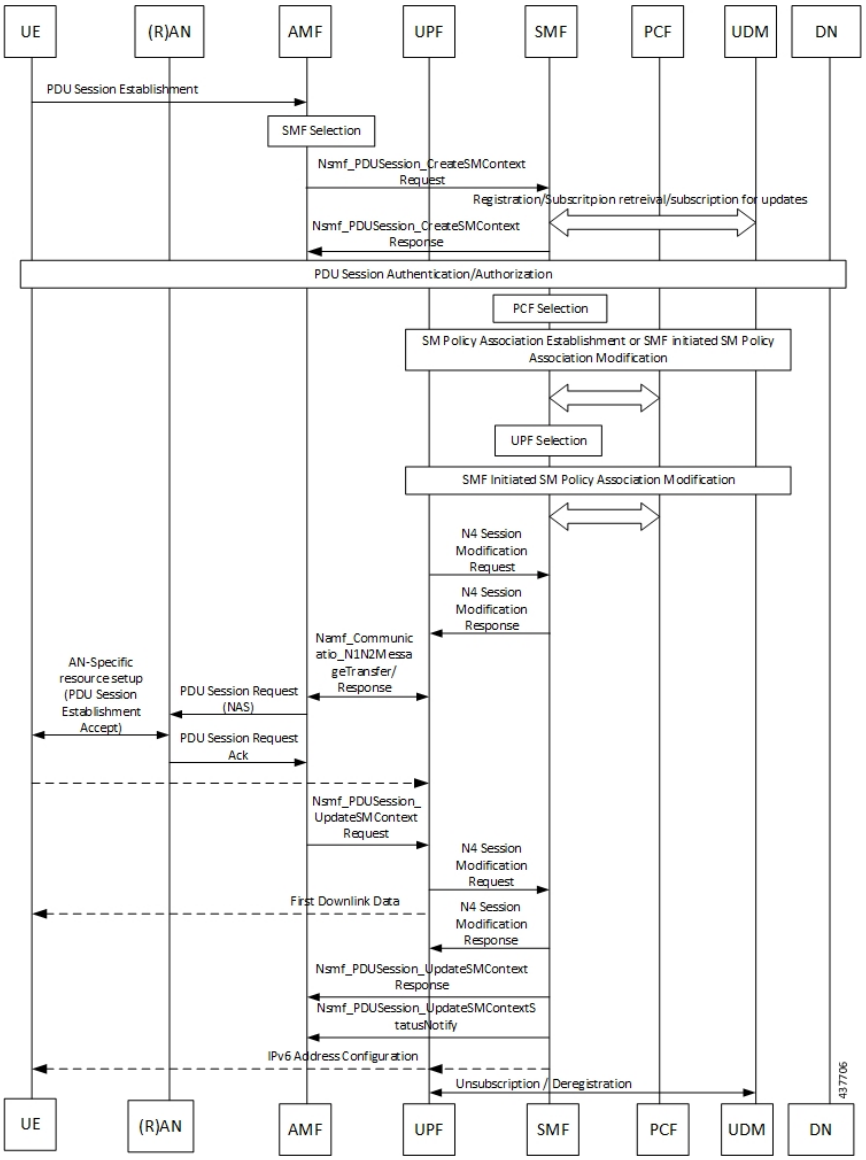


Table 68: PDU Session Creation Call Flow Description

Step	Description
1	The UE initiates the UE Requested PDU Session Establishment procedure by transmitting a NAS message containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID, Requested PDU Session Type, a Requested SSC mode, 5GSM Capability PCO, SM PDU DN Request Container, Number of Packet Filters, and optionally Always-on PDU Session Requested.
2	The AMF performs SMF selection as described in 3GPP specification.

Step	Description
3	The AMF includes EPS Interworking Indication in the Nsmf_PDUSession_CreateSMContext Request message sent to the SMF. This parameter indicates whether the UE can perform 4G to 5G handover (and vice versa) and if it is allowed with or without the presence of the N26 interface between the AMF and MME.
4	If the EPS Interworking Indication received from the AMF indicates that the UE supports EPS interworking and the SMF determines (for example, if EPS interworking is allowed for this DNN and S-NSSAI based on UE subscription data) that the PDU session supports EPS interworking, the PGW-C+SMF FQDN for the S5/S8 interface is included in the Nudm_UECM_Registration Request message.
5	The SMF sends either Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause))) or an Nsmf_PDUSession_UpdateSMContext Response depending on the Request received in Step 3. If the SMF received Nsmf_PDUSession_CreateSMContext Request in Step 3 and the SMF can process the PDU Session Establishment Request, the SMF creates an SM context and responds to the AMF by providing an SM Context Identifier.
6	(Optional). If the Request Type in Step 3 indicates "Existing PDU Session", the SMF does not perform secondary authorization and authentication. If the Request Type received in Step 3 indicates "Emergency Request" or "Existing Emergency PDU Session", the SMF does not perform secondary authorization and authentication. If the SMF needs to perform secondary authorization and authentication during the establishment of the PDU Session by a DN-AAA server as described in *3GPP TS 23.501, section 5.6.6*, the SMF triggers the PDU session establishment authentication and authorization as described in *3GPP TS 23.501, section 4.3.2.3*.
7a	If dynamic PCC is to be used for the PDU Session, the SMF performs PCF selection as described in *3GPP TS 23.501, section 6.3.7.1*. If the Request Type indicates "Existing PDU Session" or "Existing Emergency PDU Session", the SMF uses the PCF already selected for the PDU Session. Otherwise, the SMF may apply local policy.
7b	The SMF performs the mapping of PCC rules and 5G QoS parameters to 4G TFTs and 4G QoS as described in the Generating EPS PDN Connection Parameters from 5G PDU Session Parameters section in this document. Based on the QoS flows, the SMF+PGW-C also determines the number of dedicated bearers required for the session when it hands off to EPS and the required flows (all non-GBR flows) in the default bearer. The SMF+PGW-C saves the mapping of 5G flows to 4G bearers.
8	If the Request Type in Step 3 indicates "Initial request", the SMF selects an SSC mode for the PDU Session as described in *3GPP TS 23.501, section 5.6.9.3*. The SMF also selects one or more UPFs as needed as described in *3GPP TS 23.501, section 6.3.3*.
9	The SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in *3GPP TS 23.502, section 4.16.5.1* to provide information on the Policy Control Request Trigger conditions that have been met. If Request Type is "initial request" and dynamic PCC is deployed and PDU Session Type is IPv4 or IPv6 or IPv4v6, the SMF notifies the PCF (if the Policy Control Request Trigger condition is met) with the allocated UE IP address/prefix(es). SMF+PGW-C initiates the EBI allocation procedure as defined in *3GPP TS 23.502, section 4.11.1.4*.

Step	Description
10	If the Request Type indicates "initial request", the SMF initiates an N4 Session Establishment procedure with the selected UPF. Otherwise, it initiates an N4 Session Modification procedure with the selected UPF. If multiple UPFs are selected for the PDU Session, the SMF initiates N4 Session Establishment/Modification procedure with each UPF of the PDU Session in this step.
11	In the non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS flow(s) to be sent to the UE in the N1 SM container. The PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. The PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF through the Namf_Communication_N1N2MessageTransfer message.
12	The AMF sends N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept))) to the (R)AN. The AMF sends the NAS message containing PDU Session ID and PDU Session Establishment Accept targeted to the UE and the N2 SM information received from the SMF within the N2 PDU Session Request to the (R)AN.
13	The (R)AN may issue AN-specific signaling exchange with the UE that is related with the information received from the SMF. For example, in case of an NG-RAN, an RRC Connection Reconfiguration may take place with the UE establishing the necessary NG-RAN resources related to the QoS rules for the PDU Session Request received in Step 12.
14	(R)AN issues N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification)) to the AMF.
15	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF. The AMF forwards the N2 SM information received from (R)AN to the SMF.
16a	The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Information and the corresponding forwarding rules to the UPF.
16b	The UPF provides an N4 Session Modification Response to the SMF. If multiple UPFs are used in the PDU session, the UPF in Step 16a refers to the UPF terminating N3. After this step, the UPF delivers any downlink packets to the UE that may have been buffered for this PDU session.
17	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (Cause) to the AMF.
18	(Conditional) The SMF sends Nsmf_PDUSession_SMContextStatusNotify (Release) to the AMF. If during the procedure, any time after Step 5, the PDU Session establishment is not successful, the SMF informs the AMF by invoking Nsmf_PDUSession_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU session address if allocated (for example, IP address) and releases the association with PCF, if any.

Step	Description
19	If the PDU Session Type is IPv6 or IPv4v6, the SMF generates an IPv6 Router Advertisement and sends it to the UE via N4 and the UPF.
20	If the PDU Session Establishment failed after Step 4, the SMF performs the following: • The SMF unsubscribes to the modifications of Session Management Subscription data for the corresponding (SUPI, DNN, S-NSSAI), using Nudm_SDM_Unsubscribe (SUPI, Session Management Subscription data, DNN, S-NSSAI), if the SMF is no more handling a PDU session of the UE for this (DNN, S-NSSAI). The UDM may unsubscribe to the modification notification from UDR by Nudr_DM_Unsubscribe (SUPI, Subscription Data, Session Management Subscription data, S-NSSAI, DNN). • The SMF deregisters for the given PDU session using Nudm_UECM_Deregistration (SUPI, DNN, PDU Session ID). The UDM may update corresponding UE context by Nudr_DM_Update (SUPI, Subscription Data, UE context in SMF data).

PDU Session Modification Call Flow

This section describes the PDU session modification procedure as specified in *3GPP TS 23.502, section 4.3.3.2*.

Figure 62: PDU Session Modification Call Flow

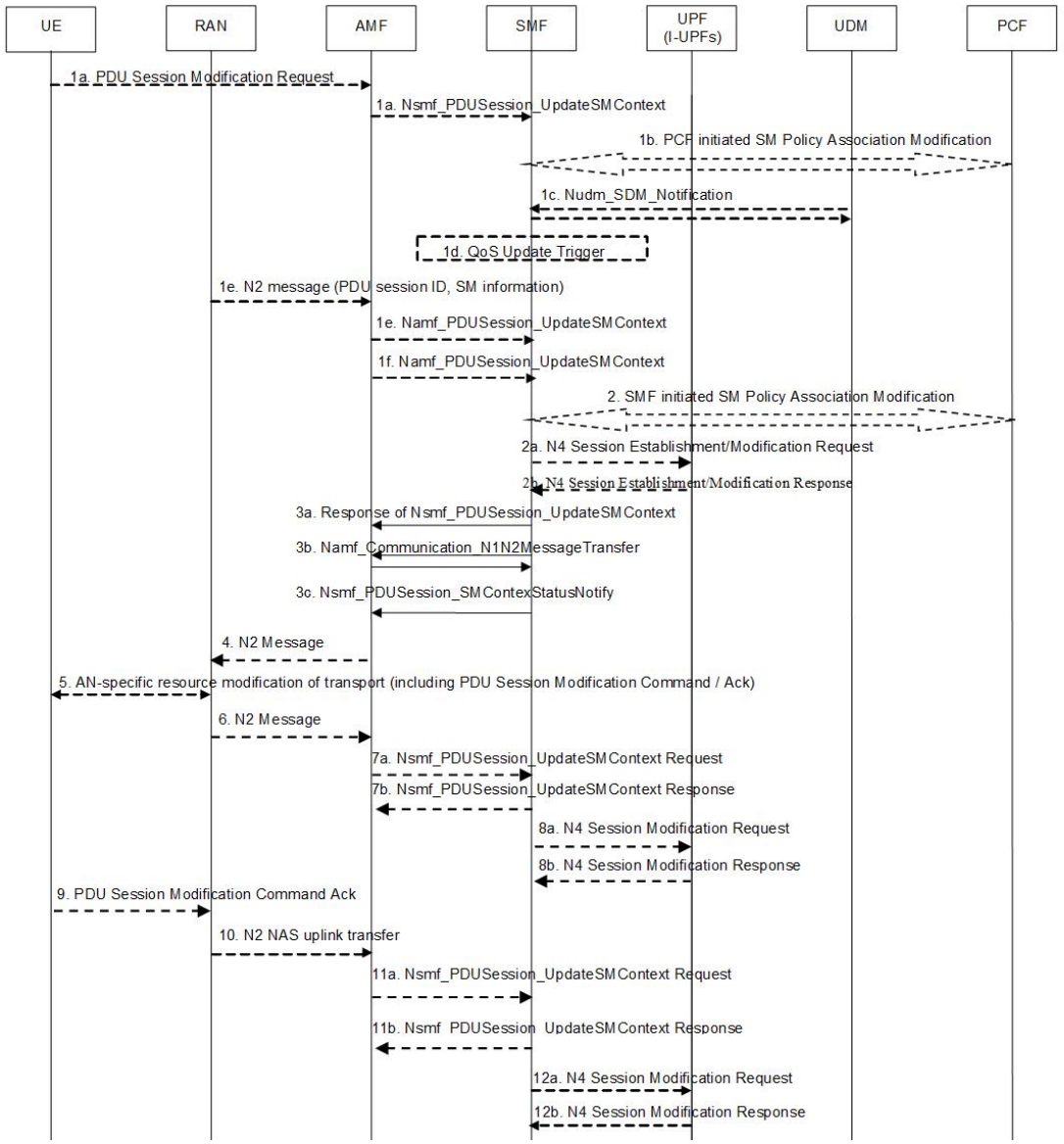


Table 69: PDU Session Modification Call Flow Description

Step	Description
1a	The UE initiates the UE Requested PDU Session Modification procedure by transmitting a NAS message containing a PDU Session Modification Request within the N1 SM container. The PDU Session Modification Request includes a PDU session ID, Packet Filters, Operation, Requested QoS, Segregation, and 5GSM Core Network Capability.
1b	(SMF-requested modification) The PCF performs a PCF-initiated SM Policy Association Modification procedure to notify the SMF about the modification of policies. The policy decision or upon AF requests, for example, Application Function influence on traffic routing, triggers this procedure.

Step	Description
1c	(SMF-requested modification) The UDM updates the subscription data of SMF by Nudm_SDM_Notification (SUPI, Session Management Subscription Data). The SMF updates the Session Management Subscription Data and acknowledges the UDM by returning an Ack with (SUPI).
1d	(SMF-requested modification) The SMF decides to modify PDU session. This procedure is also triggered based on locally configured policy or triggered from the (R)AN. If the SMF receives one of the triggers in step 1b to 1d, the SMF starts SMF-requested PDU Session Modification procedure.
1e	(AN-initiated modification) (R)AN indicates to the SMF when the AN resources onto which a QoS Flow is mapped are released irrespective of whether notification control is configured. (R)AN sends the N2 message (PDU Session ID, N2 SM information) to the AMF. The N2 SM information in the smf_PDU_Session_UpdateContext includes the following information: • QoS Flow Identifier (QFI) • User location Information • QoS Flow Release List IE - list of QoS flows which are released by NG-RAN node • QoS Flow Notify List IE and Notification Cause IE - list of GBR QoS flows that fulfilled a specific criteria, and the flows that missed fulfilling the criteria The SMF supports AN-initiated modification to release the QFI from RAN. For details on this support, see the following section.
2	The SMF reports the subscribed event to the PCF by performing an SMF-initiated SM Policy Association Modification procedure. The SMF skips this step if the PDU Session Modification procedure is triggered by step 1b or 1d. If the dynamic PCC is not deployed, the SMF may apply local policy to decide whether to change the QoS profile. The SMF does not invoke the steps 3 to 7 when the PDU Session Modification requires only action at a UPF (for example, gating).
3a	For UE or AN-initiated modification, the SMF responds to the AMF through Nsmf_PDUSession_UpdateSMContext including N2 SM information and N1 SM container. The N2 SM information carries information that the AMF provides to the (R)AN. It includes the QoS profiles and the corresponding QFIs to notify the (R)AN that one or more QoS flows were added, or modified. It includes only QFI(s) to notify the (R)AN that one or more QoS flows were removed. The N1 SM container carries the PDU Session Modification Command that the AMF provides to the UE. It includes the QoS rule(s), QoS rule operation, QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), and Session-AMBR.
3b	For SMF-requested modification, the SMF invokes Namf_Communication_N1N2MessageTransfer including N2 SM information and N1 SM container. If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer, and skips the steps 4, 5, 6 and 7. When the UE is reachable, that is, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.

Step	Description
4	The AMF sends N2 PDU Session Request (N2 SM information received from the SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) Message to the (R)AN.
5	The (R)AN issues AN-specific signalling exchange with the UE that is related with the information received from the SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
6	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session Ack Message to the AMF.
7	The AMF forwards the N2 SM information and the User location Information from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response. If the (R)AN rejects QFI(s), the SMF updates the QoS rules and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s) in the UE accordingly.
8	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request message to the UPF.
9	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command Ack)).
10	The (R)AN forwards the NAS message to the AMF.
11	The AMF forwards the N1 SM container (PDU Session Modification Command Ack) and User Location Information from the AN to the SMF through Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response.
12	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF. For a PDU Session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s).
13	If the SMF interacts with the PCF in step 1b or 2, the SMF notifies the PCF whether the PCC decision is enforced or not by performing an SMF-initiated SM Policy Association Modification procedure. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change. If the step 1b is triggered to perform Application Function influence on traffic routing, the SMF reconfigures the User Plane of the PDU session.

Releasing QFI During AN-initiated Modification Procedure

For the SMF to support AN-initiated modification to release the QFIs, perform the following steps:

1. If the EPS Interworking Indication is enabled for a given PDU session, the SMF initiates the EBI release towards the AMF.

2. The SMF sends N4 Modification to the UPF to delete the Packet Detection Rule (PDR), QoS Enforcement Rule (QER), and Usage Reporting Rule (URR) related to the flows being released.
3. The SMF initiates N1N2TransferMessage containing N1 PDU Session Modification command. This message includes information about the deleted flows, Mapped EPS Bearer Context.
4. Then, the SMF interacts with the PCF to report the flows released for the rules if “RES_RELEASE” trigger is set.

Note The "policy_pdu_flows_total" statistics is available to check the released flows.

EPS Interworking Indication in PDU Session Modification

The EpsInternetworkingIndication field denotes the possibility of handover between EPS and 5GC. This field holds the following values:

- NONE: The PDU session cannot be moved to EPS.
- WITH_N26: The PDU session is moved to EPS, with N26 interface supported during EPS interworking procedures.
- WITHOUT_N26: The PDU session is moved to EPS, without N26 interface supported during EPS interworking procedures.

The SMF allows the 4G to 5G handover and vice-versa only if the EpsInternetworkingIndication value is set to WITH_N26. For other values of EpsInternetworkingIndication, the SMF rejects the handovers.

During 4G and 5G PDU session establishment, if the EPS internetworking indication is received from the AMF, the SMF includes PGW-C+SMF FQDN for S5/S8 interface in the UDM Registration request.

With the EPS Interworking Indication Support Enabled:

If the EpsInternetworkingIndication value changes from NONE or WITHOUT_N26 to WITH_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The AMF invokes the Nsmf_PDUSession_UpdateSMContext request with the changed EpsInterworkingIndication value.
2. The SMF receives the Nsmf_PDUSession_UpdateSMContext request from the AMF, and initiates the Namf_Communication_EbiAssignmentRequest. This request includes the PDU Session ID and Allocation/Retention Priority (ARP) List.
3. The AMF sends Namf_Communication_EbiAssignmentResponse to the SMF. The AMF sends the following through the response:
   - assignedEbiList containing the successfully assigned EBIs.
   - failedArpList containing the failed ARPs for which the EBI assignment failed.
   - 4XX/5XX error along with AssignEbiError representing the EBI assignment failure.
4. The SMF sends N1N2MessageTransfer request message if the EBIs are created successfully. This request includes the following:

- N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Create])
- N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER (QoS Flow Add or Modify Request Item with EPS Radio Access Bearer (E-RAB) ID and QoS Flow ID)

Note If the UE is in Idle mode, the SMF skips sending the N2 message.

5. The SMF informs mapped EPS bearer context in the UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
6. The SMF informs EBI to QoS Flow Identifier (QFI) mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
7. The SMF completes the PDU Session Modification procedure.

With the EPS Interworking Indication Support Disabled:

If the EpsInternetworkingIndication value changes from WITH_N26 to NONE or WITHOUT_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The SMF receives the Nsmf_PDUSession_UpdateSMContext request with the changed EpsInterworkingIndication value from the AMF.
2. The SMF sends N1N2MessageTransfer request message. This request includes the following:
   - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Delete])
   - N2:N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER

Note If the UE is in Idle mode, the SMF skips sending the N2 message.

3. The SMF deletes Mapped EPS bearer context in UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
4. The SMF deletes EBI to QFI mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
5. The SMF completes the PDU Session Modification procedure.

Use the **show subscriber** command to determine the EPS interworking status of the PDU session, and the EBI mapping for the QoS flows.

PDU Session Release Call Flow

The PDU Session Release procedure is used to release all the resources associated with a PDU session, including:

- The IP address/prefixes allocated for an IP-based PDU session
- Any UPF resource that was used by the PDU session.

- Any access resource that was used by the PDU session.

The SMF notifies any entity associated with the PDU session: PCF, Data Network (DN) (for example, when DN authorization has taken place at PDU session establishment), and so on.

There are different ways to initiate the PDU session release. It can be from UE, network, AMF, or RAN.

UE-initiated PDU Session Release Call Flow

The UE-initiated PDU session release procedure allows the UE to request the release of the PDU session. In the case of Local Breakout (LBO), the procedure is as in the case of non-roaming with the difference that the AMF, the SMF, the UPF, and the PCF are located in the visited network.

The following figure depicts the UE-initiated PDU session release procedure to support EPS interworking on the SMF as specified in *3GPP TS 23.502, section 4.3.4.2*.

Figure 63: UE-initiated PDU Session Release Call Flow

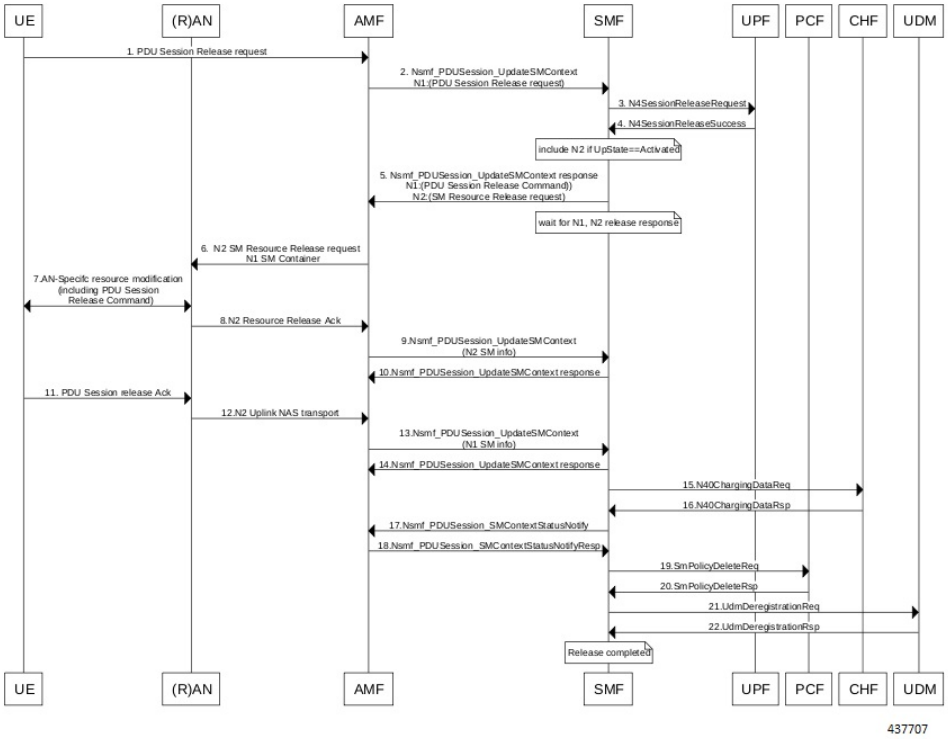


Table 70: UE-initiated PDU Session Creation Call Flow Description

Step	Description
1, 2	The UE sends PDU_SESSION_RELEASE_REQUEST in NAS message to the AMF through the RAN. The AMF sends the message to the SMF in SmContextUpdateRequest.
3, 4	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.

Step	Description
5	The SMF sends SmContextUpdateResponse message with N1 and N2 content. • N1: PDU_SESSION_RELEASE_COMMAND • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
11, 12, 13, 14	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

Network-initiated PDU Session Release Call Flow

The network-initiated PDU session release procedure allows the AMF, the SMF or the PCF to initiate the release of a PDU session.

The following figure depicts the network-initiated PDU session release call flow.

Figure 64: Network-initiated PDU Session Release Call Flow

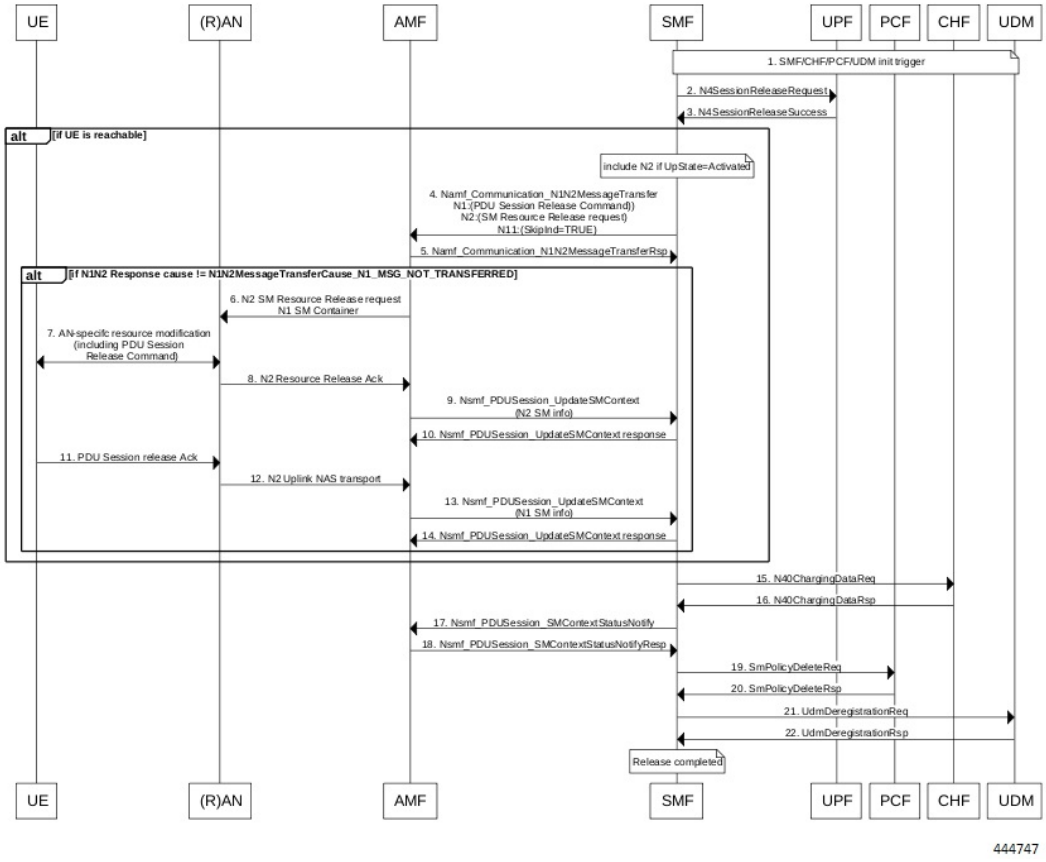


Table 71: Network-initiated PDU Session Creation Call Flow Description

Step	Description
1	This procedure can be triggered by PCF, CHF, UDM, UPF or CLI (clear subscriber) to initiate the release of a PDU session.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same. **Note** Skip the steps 4 to 14 if the AMF has notified that the UE is not reachable.
4	The SMF sends N1N2MessageTransfer message with N11, N1 and N2 content. • N11: SkipInd=True • N1: PDU_SESSION_RELEASE_COMMAND • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.

Step	Description
5	The AMF responds back to the SMF with the cause included in the N1N2MessageTransferRsp message. **Note** Skip the steps 6 to 14 if the AMF sends the cause as N1_MSG_NOT_TRANSFERRED in step 5.
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF transfers N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
11, 12, 13, 14	The UE sends N1 release response in the NAS message to the AMF through the RAN. The AMF sends the N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with the SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

AMF-initiated PDU Session Release

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session.

The following figure depicts the AMF-initiated PDU session release call flow.

Figure 65: AMF-initiated PDU Session Release Call Flow

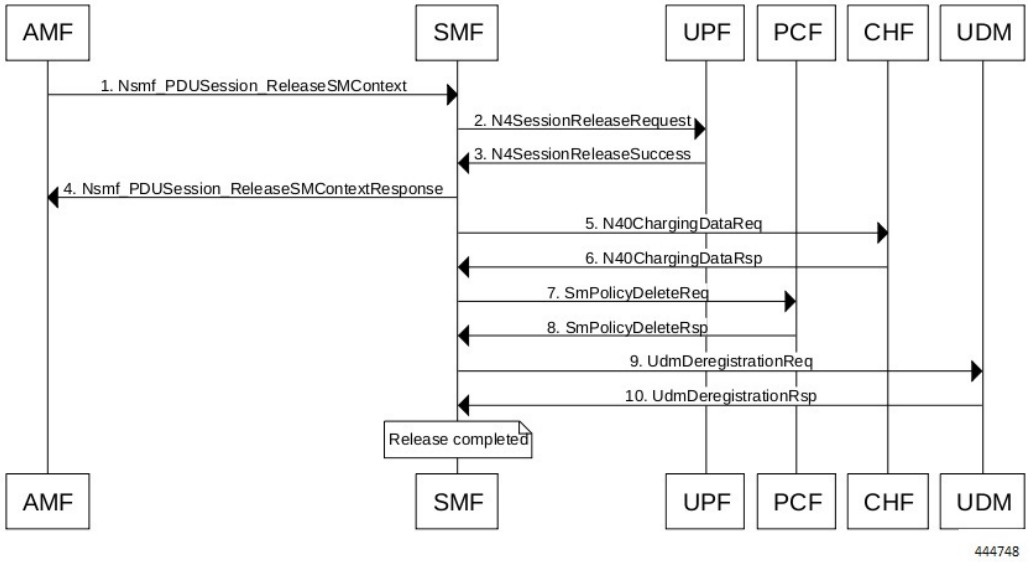


Table 72: AMF-initiated PDU Session Creation Call Flow Description

Step	Description
1	The AMF sends SmContextReleaseRequest.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextReleaseResponse to the AMF.
5, 6	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
7, 8	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
9, 10	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

AMF-initiated PDU Session Release with N11 Release=True

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session with the N11 release in the SmContextModifyRequest being set to True.

The following figure depicts the AMF-initiated PDU session release call flow with the N11 release=True.

Figure 66: AMF-initiated PDU Session Release with N11 Release=True

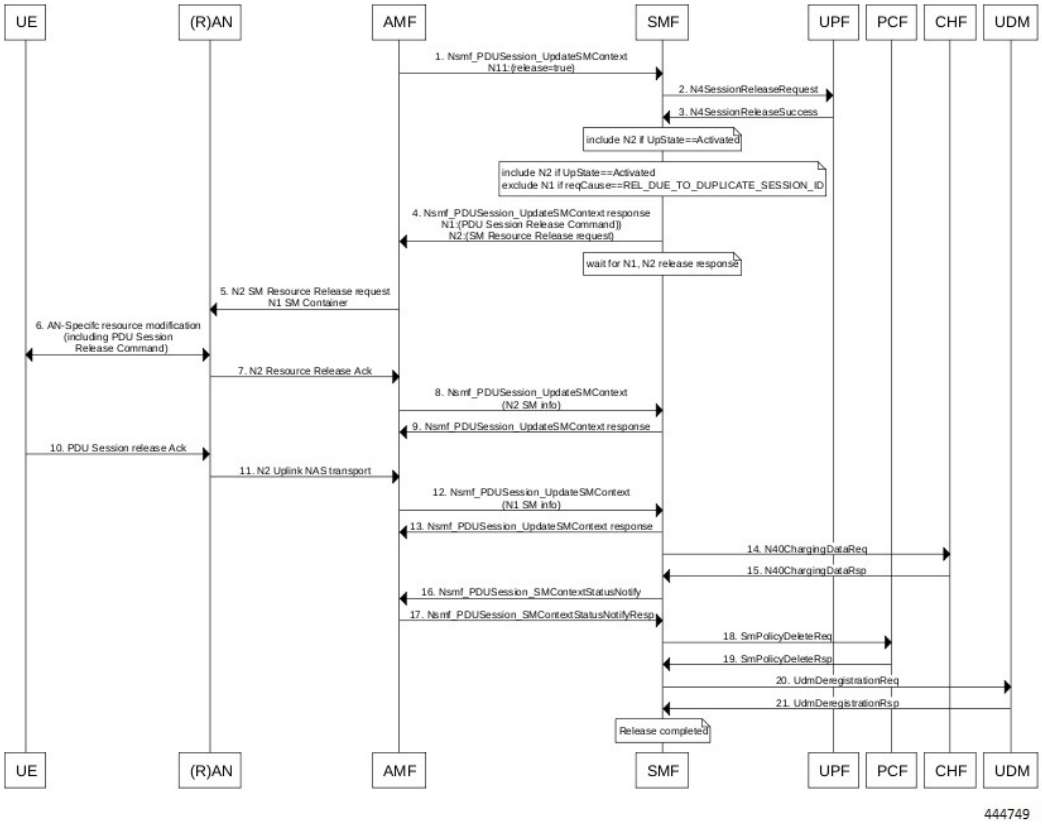


Table 73: AMF-initiated PDU Session Creation Call Flow (N11 release=true) Description

Step	Description
1	The AMF sends SmContextModifyRequest with release=True in 2 causes REL_DUE_TO_DUPLICATE_SESSION_ID or REL_DUE_TO_SLICE_NOT_AVAILABLE.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextUpdateResponse message with N1 and N2 content. • N1: PDU_SESSION_RELEASE_COMMAND, exclude if cause is REL_DUE_TO_DUPLICATE_SESSION_ID, skip steps 10,11,12,13 • N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 7, 8, and 9.
5, 6	The AMF exchanges message with RAN. The RAN forwards it to the UE.
7, 8, 9	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.

Step	Description
10, 11, 12, 13	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
14, 15	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
16, 17	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
18, 19	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
20, 21	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

RAN-initiated PDU Session Release Call Flow

The RAN-initiated PDU session release procedure allows the RAN to initiate the release of a PDU session.

The following figure depicts the RAN-initiated PDU session release call flow.

Figure 67: RAN-initiated PDU Session Release Call Flow

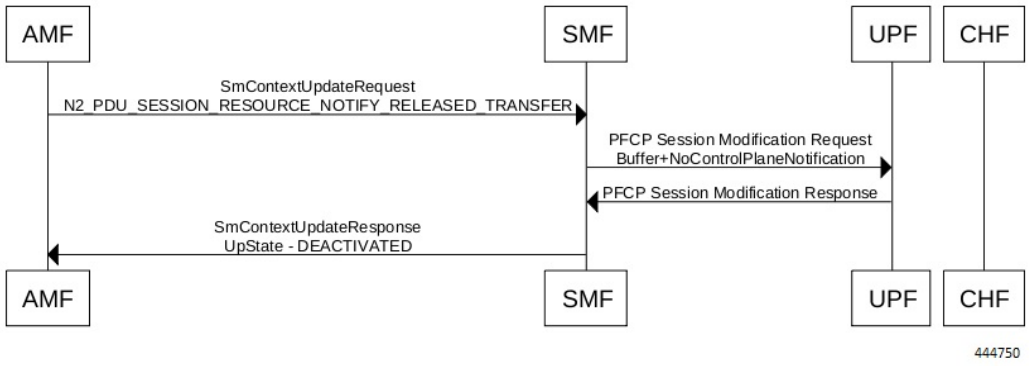


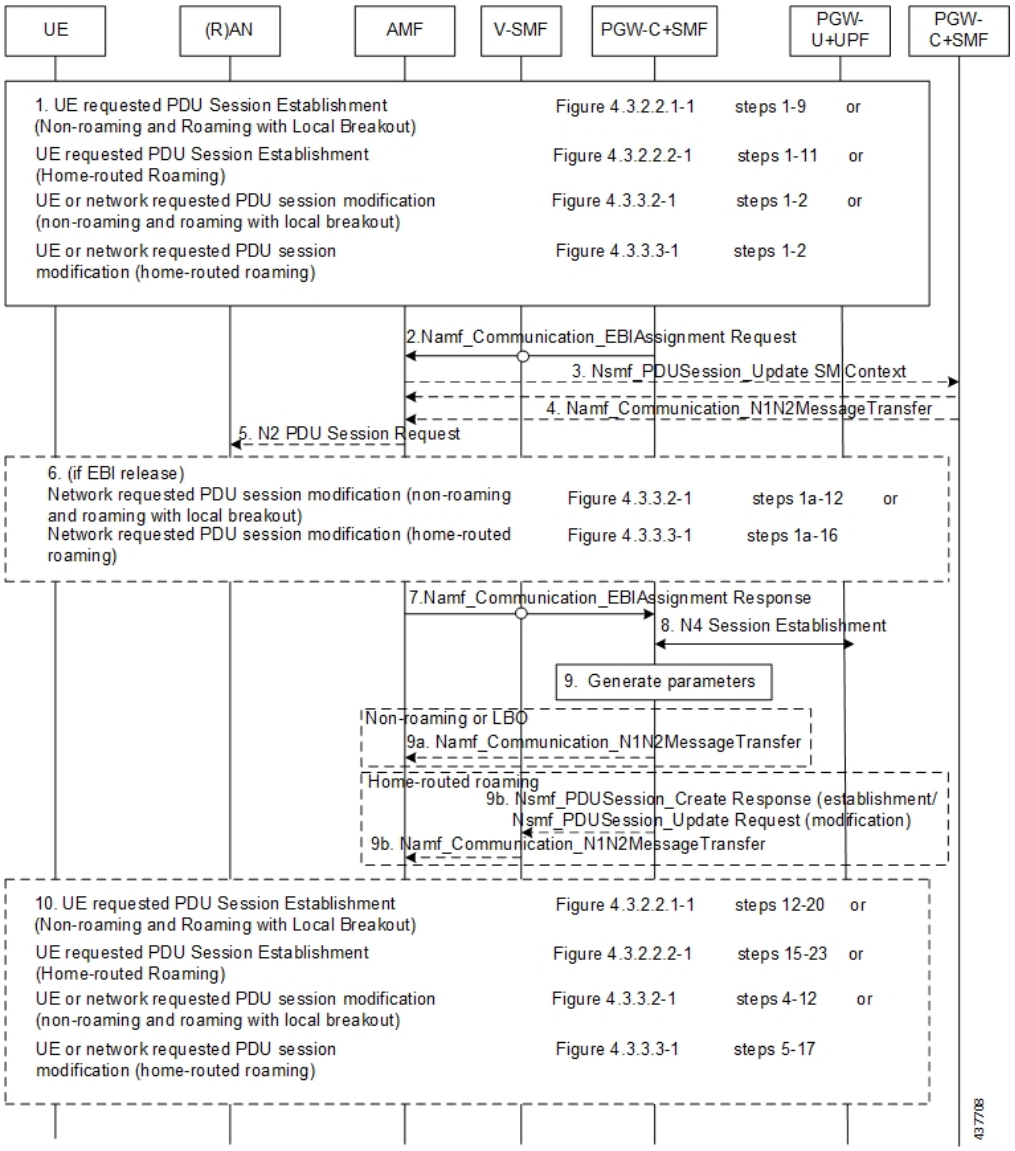
Table 74: AMF-initiated PDU Session Creation Call Flow Description

Step	Description
1	The AMF sends SmContextModifyRequest with N2 type: N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER.
2, 3	The SMF sends N4SessionModificationRequest to the UPF with changing packet rule to Buffer from Forward. The UPF sends the response for the same, that is, the SMF moving to IDLE state.
4	The SMF sends SmContextUpdateResponse message with UpState as Deactivated.

EPS Bearer ID Allocation

This section describes the EPS Bearer ID Allocation procedure.

Figure 68: EPS Bearer ID Allocation Call Flow



Note Not all the steps in the preceding call flow are supported. For more details, see the descriptions in the following table.

Table 75: EPS Bearer ID Allocation Call Flow Description

Step	Description
1	If the PGW-C+SMF (or H-SMF for home-routed cases) determines that EPS bearer IDs (based on operator policies, S-NSSAI, User Plane Security Enforcement information) need to be assigned to the QoS flows in the PDU session, the PGW-C+SMF invokes Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list).

Step	Description
Step 2 through Step 5 apply only when the AMF needs to revoke EBI that was previously allocated for a UE to serve a new SMF request of EBI for the same UE.	
2	(Conditional) If the AMF has no available EBIs, the AMF may revoke an EBI that was assigned to QoS flows based on the ARPs and S-NSSAI stored during PDU Session Establishment, EBI information in the UE context and local policies. If an assigned EBI is to be revoked, the AMF invokes Nsmf_PDUSession_UpdateSMContext (EBI(s) to be revoked) to request the related SMF (called “SMF serving the released resources”) to release the mapped EPS QoS parameters corresponding to the EBI to be revoked. The AMF stores the association of the assigned EBI, ARP pair to the corresponding PDU Session ID and SMF address.
3	The “SMF serving the released resources” that receives the request in Step 3 invokes Namf_Communication_N1N2Message Transfer (N2 SM information (PDU Session ID, EBI(s) to be revoked), N1 SM container (PDU Session Modification Command (PDU Session ID, EBI(s) to be revoked))) to inform the (R)AN and the UE to remove the mapped EPS QoS parameters corresponding to the EBI(s) to be revoked. In home-routed roaming scenario, the H-SMF includes EBI(s) to be revoked to V-SMF to inform V-SMF to remove the mapped EPS bearer context corresponding to the EBI(s) to be revoked. The SMF can also decide to remove the QoS flow if it is not acceptable to continue the service when no corresponding EPS QoS parameters can be assigned. For home-routed roaming scenario, the "SMF serving the released resources" sends an N4 Session Modification Request to request the PGW-U+UPF to release the N4 session corresponding to the revoked EBI(s). In home-routed roaming case, the V-SMF starts a VPLMN-initiated QoS Modification for the PDU session. The V-SMF invokes the Namf_Communication_N1N2Message Transfer based on the corresponding QoS modification message received from H-SMF.
4	If the UE is in CM-CONNECTED state, the AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN. If the UE is in CM-IDLE state and an ATC is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer and Step 5 and Step 6 are skipped. When the UE is reachable, for example, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.
5	The relevant steps of the procedure are executed as specified in the preceding figure.
6	If the AMF successfully assigns EBI(s), it responds with the assigned EBI(s). Otherwise, it responds with a cause indicating EBI assignment failure. If a PDU session from another SMF already exists towards the same DNN, the AMF either rejects the EBI assignment request, or revokes the EBI(s) from the existing PDU session(s) to the same DNN but different SMF. The AMF makes the decision based on the operator policy. **Note** The preceding statement applies only when the S-NSSAI(s) for the PDU sessions are different, otherwise the same SMF is selected for PDU sessions to the same DNN.

Step	Description
7	The PGW-C+SMF sends an N4 Session Establishment/Modification Request to the PGW-U+UPF. For home-routed roaming scenario, if the EBI is assigned successfully, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer. If the CN Tunnel info is allocated by the PGW-C+SMF, the PGW-U tunnel info for the EPS bearer may be provided to PGW-U+UPF. If the CN Tunnel info is allocated by PGW-U+UPF, the PGW-U+UPF sends the PGW-U tunnel info for the EPS bearer to the PGW-C+SMF. The PGW-U+UPF is ready to receive the uplink packets from E-UTRAN. **Note** • In the home-routed roaming scenario, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer and provides it to the V-SMF. Thus, when the UE moves to EPS network, the V-SMF does not need to interact with the PGW-C+SMF to get the EPS bearer context(s). • If the CN Tunnel info is allocated by the PGW-C+SMF and not provided to PGW-U+UPF at PDU session establishment, when the UE moves to the target RAT the PGW-U+UPF cannot receive uplink (UL) data until the PGW-C+SMF has provided the Tunnel Info to the PGW-U+UPF in N4 Session Modification. This causes a short interruption to the UL data during the inter-system handover execution. • SMF supports other RAT tunnel creation for EPS bearers during 5G PDU establishment and in the 5G PDU modification (new flow creation time). SMF sends the additional PDRs for EPS bearers in the N4 establishment and the N4 modification requests to communicate to UPF on these additional tunnel creation for the EPS bearers.
8	If the PGW-C+SMF receives any EBI(s) from the AMF, it adds the EBI(s) received into the mapped EPS bearer context(s). In home-routed roaming scenario, the PGW-C+SMF generates EPS bearer context, which includes per EPS bearer PGW-U tunnel information. In addition, if the default EPS bearer is generated for the corresponding PDN Connection of PDU Session (that is, during the PDU Session establishment procedure), the PGW-C+SMF generates the PGW-C tunnel information of the PDN connection and includes it in UE EPS PDN connection.
8a	(Conditional) In non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS Flow(s) to be sent to the UE in the N1 SM container. PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF via Namf_Communication_N1N2MessageTransfer.
8b	(Conditional) In home-routed roaming scenario, the PGW-C+SMF sends the mapped EPS bearer context(s), the mapping between the received EBI(s) and QFI(s), and EPS bearer context to the V-SMF via Nsmf_PDUSession_Create Response during PDU Session Establishment, or via Nsmf_PDUSession_Update Request during PDU Session Modification. The V-SMF stores the EPS bearer context, and generates N1 SM container and N2 SM information, and forwards them to the AMF via Namf_Communication_N1N2MessageTransfer.
9	The N1 SM container and N2 SM information are sent to the UE and NG-RAN respectively. The relevant steps of the procedure are executed as specified in the preceding figure.

Non-roaming 5G PDU Establishment with N4 Optimization Call Flow

This section describes the call flow of the non-roaming 5G PDU establishment with N4 optimization.

Figure 69: Non-roaming 5G PDU Establishment with N4 Optimization Call Flow

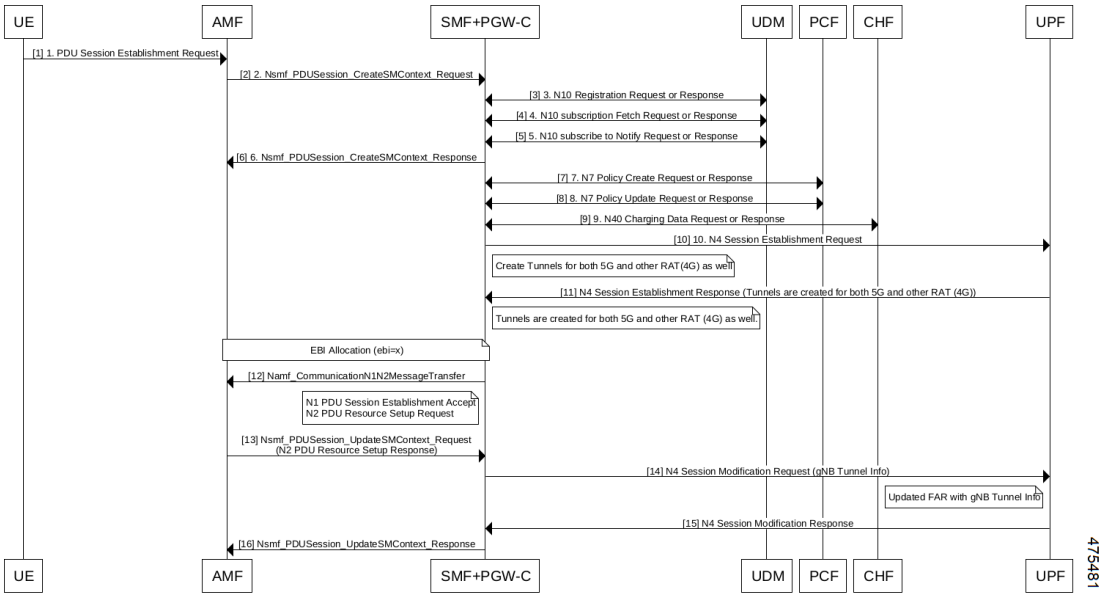


Table 76: Non-roaming 5G PDU Establishment with N4 Optimization Call Flow Description

Step	Description
1	UE sends the PDU session establishment request to AMF.
2	AMF sends the Nsmf PDU session CreateSMContext request to SMF+PGW-C.
3	SMF+PGW-C sends the N10 Registration Request to UDM. Then, UDM sends the N10 Registration Response to SMF+PGW-C.
4	SMF+PGW-C sends the N10 Subscription Fetch Request to UDM. Then, UDM sends the N10 Subscription Fetch Response to SMF+PGW-C.
5	SMF+PGW-C sends the N10 Subscribe to Notify Request to UDM. Then, UDM sends the N10 Subscribe to Notify Response to SMF+PGW-C.
6	SMF+PGW-C sends the Nsmf PDU Session CreateSMContext Response to AMF.
7	SMF+PGW-C sends the N7 Policy Create Request to PCF. Then, PCF sends the N7 Policy Create Response to SMF+PGW-C.
8	SMF+PGW-C sends the N7 Policy Update Request to PCF. Then, PCF sends the N7 Policy Update Response to SMF+PGW-C.
9	SMF+PGW-C sends the N40 Charging Data Request to CHF. Then, CHF sends the N40 Charging Data Response to SMF+PGW-C.

Step	Description
10	SMF+PGW-C sends the N4 Session Establishment Request to UPF. SMF creates a tunnel for both 5G and other RAT (4G).
11	After the creation of the tunnel, UPF sends the N4 Session Establishment Response to SMF+PGW-C.
12	SMF+PGW-C initiates the EBI allocation procedure. Then, SMF+PGW-C sends the Namf Communication N1N2Message Transfer request to AMF.
13	After the N1 PDU Session Establishment is accepted and the N2 PDU Resource Setup Request is sent, SMF+PGW-C sends the Nsmf PDU Session UpdateSMContext Request (N2 PDU Resource Setup Response) to SMF+PGW-C.
14	SMF+PGW-C sends the N4 Session Modification Request to UPF. This request includes the gNB tunnel details.
15	UPF sends the N4 Session Modification Response to SMF+PGW-C. The response includes the updated FAR and the gNB tunnel details.
16	SMF+PGW-C sends the Nsmf PDU Session UpdateSMContext Response to AMF.

Standards Compliance

This feature complies with the following standards:

- *3GPP TS 23.401, Version 15.6.0*
- *3GPP TS 23.502, Version 15.4.0*

Generating EPS PDN Connection Parameters from 5G PDU Session Parameters

This section describes how to generate the EPS PDN connection parameters from the 5G PDU session parameters in the PGW-C+SMF.

When the PGW-C+SMF is requested to set up or modify a PDN connection or a PDU session that supports interworking between EPS and 5GC, the PGW-C+SMF generates the PDN connection parameters from the PDU session parameters.

When the PGW-C+SMF generates the PDN connection parameters based on the PDU session parameters, the following rules hold:

- PDN Type: The PDN type is set to IPv4 or IPv6 if the PDU Session Type is IPv4 or IPv6 respectively. The PDN type is set to Non-IP for Ethernet and Unstructured PDU Session Types.
- EPS Bearer ID: The EBI is requested from the AMF during the establishment of a QoS Flow as described in *3GPP TS 23.502, section 4.11.1.4.1*, for PDU sessions that support interworking between EPS and 5GC. The EBI is obtained from MME during the establishment of an EPS bearer (that is triggered by an establishment of the QoS Flow) as defined in *3GPP TS 23.401* for PDN connections hosted by PGW-C+SMF. The association between EBI and QoS Flow is stored by the SMF.
- APN-AMBR: APN-AMBR is set according to the operator policy. For example, taking the session AMBR into account.
- EPS QoS parameters (including ARP, QCI, GBR, and MBR):

- If the QoS Flow is mapped to one EPS bearer: ARP, GBR, and MBR of the EPS bearer is set to the respective ARP, GFBR, and MFBR of the corresponding QoS Flow.
- For standardized 5QIs, the QCI is mapped 1:1 to the 5QI. For non-standardized 5QIs, the PGW-C+SMF derives the QCI based on the 5QI and operator policy.

Note A GBR QoS flow is mapped 1:1 to a GBR dedicated EPS Bearer if an EBI has been assigned. All other GBR QoS flows will be terminated during interworking. If multiple QoS flows are mapped to one EPS bearer, the EPS bearer parameters are set based on the operator policy. For example, EPS bearer QoS parameters are set according to the highest QoS of all mapped QoS flows.

Note Non-GBR QoS flows for which no EBI has been assigned are mapped to the default EPS bearer.

5G to EPS Handover Using N26 Interface

Feature Description

The SMF supports handover of PDU sessions to EPS on 5GC when the N26 interface is present between the MME and the AMF. The handover supports the creation of applicable default and dedicated bearers.

How it Works

This section describes the 5G to EPS handover procedure and the 5G to EPS handover cancellation procedure.

Call Flows

This section describes the following call flows:

- 5G to EPS Handover Call Flow
- 5G to EPS Handover Cancellation Flow

5G to EPS Handover Call Flow

This section describes the 5G to EPS handover call flow with N26 interface.

The 5G to EPS Handover procedure for the EPS session is compliant with 3GPP 23.502, section 4.11.1.2.1.

1. The AMF requests the SMF to provide the SM Context using Nsmf_PDUSession_ContextRequest.
2. The SMF sends N4 Session Modification to the UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules received from PCC must already be present with the SMF. The SMF must also have the bearer IDs obtained from the Bearer ID Allocation procedure. The SMF creates new PDRs for the N4 session and gets TEID allocated for each bearer as required by the 4G system.

3. The SMF provides EPS bearer contexts to the AMF. The SMF also provides the CN tunnel information to AMF for all bearers for the uplink traffic from E-UTRAN.
4. If indirect data forwarding applies, the AMF sends the Nsmf_PDUSession_UpdateSMContext Request (S-GW address(es) and S-GW DL TEID(s) for data forwarding) to the SMF, for creating the indirect data forwarding tunnel.
5. The SMF sends N4 Modification Request to the UPF to create additional PDRs and FARs to receive the redirected DL data over the indirect tunnel from NG RAN and forwards them to eNodeB. The uplink PDRs must have QFI to match the forwarded DL data from NG-RAN and the associated QER will not have QFI as data needs to be forwarded to the eNodeB. The FAR redirects the received data to the eNodeB over appropriate tunnel based on the QFI.
6. The S-GW sends Modify Bearer Request to the SMF with DL TEIDs on the SMF for the bearers.
7. The SMF sends N4 Modification Request to the UPF to activate the DL data path to E-UTRAN. At this time, both the indirect tunnel and the direct DL path are activated towards the eNodeB.
8. The SMF sends the Modify Bearer Response to S-GW.
9. The AMF initiates Nsmf_PDUSession_UpdateSMContext Request service operation with an indication to release the forwarding tunnels.
10. The SMF sends N4 Modification Request to the UPF to remove the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed.

5G to EPS Handover Cancellation Call Flow

When the Source Radio Access Network (RAN) triggers a handover cancellation after the preparation phase, the AMF invokes the "Nsmf_PDUSession_UpdateSMContext request (SUPI, Relocation Cancel Indication) toward the SMF. Based on the Relocation Cancel Indication, the SMF deletes the session resources established during the handover preparation phase. That is, the SMF removes all the Packet Detection Rules (PDRs), Forwarding Action Rules (FARs), and other rules that were allocated in preparation of handoff for indirect tunnel and the 5G session.

The following call flow depicts the 5GS to EPS handover cancellation procedure.

Figure 70: 5GS to EPS Handover Cancellation Call Flow

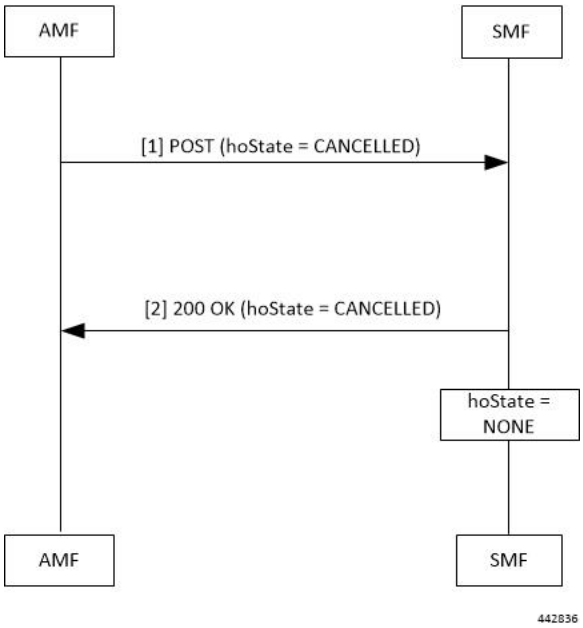


Table 77: 5GS to EPS Handover Cancellation Call Flow Description

Step	Description
1	The AMF requests the SMF to cancel the handover of an existing PDU session by sending a POST request for Sm Context Update service, with the following information: • updating the hoState attribute of the individual SM Context resource in the SMF to CANCELLED • cause information
2	The SMF returns a 200 OK response message including the following information: • hoState attribute set to CANCELLED The SMF cancels the execution of the handover, for example, releases the resources reserved for the handover to the target RAN. Then, the SMF sets the hoState to NONE and deletes any stored targetServingNfId.

Standards Compliance

The 5G to EPS Handover feature complies with the *3GPP TS 23.502, version 15.3.0*.

Create Dedicated Bearer Delay and Retry Support

Feature Description

The Create Dedicated Bearer Delay and Retry Support feature facilitates the following:

- Delays the creation of the dedicated bearer that is based on the configured time after handover is complete.
- Retries the creation of the dedicated bearer for the IMS bearer in either of the following scenarios:
  - When the MME fails with the handover in progress.
  - When the IMS bearer is temporarily unreachable.
- After the handover is complete, the SMF service starts with the configured timer. Then, the dedicated bearer creation begins.
- If the IMS dedicated bearer creation fails, the maximum retries configuration determines the number of retries the creation process attempts. The configured timeout determines the delay of each retry attempt.

How It Works

This section provides a brief of how the Create Dedicated Bearer Delay and Retry Support feature works.

Call Flows

This section includes the following call flow.

Figure 71: EPS Fallback Guard Timer Call Flow

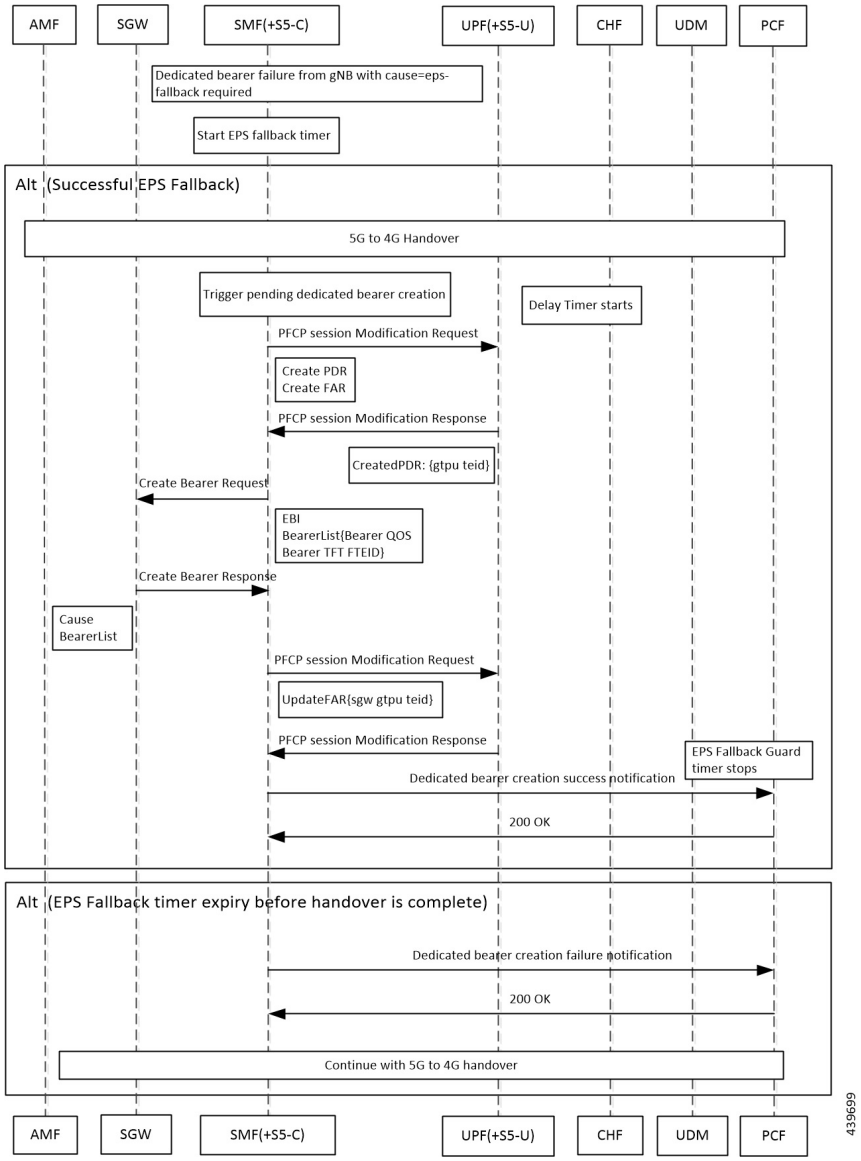


Table 78: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
With the successful EPS fallback following the 5G to 4G handover, steps 3 to12 occur.	
3	EPS triggers pending dedicated bearer creation.
4	Delay timer starts.
5	SMF (+S5-C) sends the PFCP session modification request to UPF (+S5-U).

Step	Description
6	PDR and FAR are created.
7	UPF (+S5-U) sends the PFCP session modification response to SMF (+S5-C).
8	The information on the created PDR with the GTP-U TEID is available.
9	SMF (+S5-C) sends the Create Bearer Request to S-GW.
10	S-GW sends the Create Bearer Response to SMF (+S5-C).
11	SMF (+S5-C) sends the PFCP Session Modification Request to UPF (+S5-U).
12	UPF (+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
13	EPS Fallback Guard Timer stops.
14	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
In the EPS fallback timer expiry before handover completion scenario, steps 13 to15 occur.	
15	SMF (+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
16	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
17	The 5G to 4G handover procedure continues.

Configuring Create Dedicated Bearer Delay and Retry Support

This section describes how to configure the Create Dedicated Bearer Delay and Retry Support feature.

```
config
   profile access accesstemp
     eps-fallback cbr delay delay_time max-retry retry_count
     timeout timeout_value
     end
```

NOTES:

- **delay** *delay_time*: Specifies the time delay in milliseconds for the creation of the dedicated bearer. The valid values range 0 through10000 milliseconds. The default is 0.
- **max-retry** *retry_count*: Specifies the number of times to retry the creation of the dedicated bearer. The valid values range from 0 through 10. The default is 0.
- **timeout** *timeout_value*: Specifies the time gap in seconds before retrying the creation of the dedicated bearer. The valid values range from 1 through 3 seconds. The default is 1.

Verifying the Create Dedicated Bearer Delay and Retry Support Configuration

This section describes how to verify the Create Dedicated Bearer Delay and Retry Support configuration.

Use the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
profile smf smf1
service name smf-service
  access-profile access1
```

```
!
!
profile access access1
eps-fallback cbr delay 100 max-retry 5 timeout 2
```

Handling Dedicated Bearer Procedure Failures Caused by Timer Expiry

Feature Description

This section explains the behavior of SMF when the dedicated bearer procedure does not end within a defined procedure timeout value. The timeout is termed Service Level Agreement (SLA) timer. The SLA timeout defined at procedure level is known as procedure SLA timer.

While processing the dedicated bearer procedure, the SMF interacts with the peer NFs. The peer NFs can be one of the following:

- S-GW
- PCF
- CHF
- UPF

When the SLA timer expires before the completion of dedicated bearer procedure, the graceful clean-up is performed at SMF and peer nodes. This clean-up action is based on the stage at which the dedicated bearer procedure is executing.

How it Works

The SMF starts the procedure SLA timer at the start of the dedicated bearer procedure, and stops at the end of the procedure. The endpoint configuration allows defining the SLA timer at the interface (N11, N7, N40) level. For configuration details, see the Configuring Dedicated Bearer Procedure Failure Handling Feature, on page 263 section in this guide.

Procedure SLA is supported for the following transactions that start a dedicated bearer procedure:

- N7 Policy Notify Request (PCF-initiated Modification)
- Delete Bearer Command (SGW-initiated Deletion)
- Any internal transaction that starts a Dedicated Bearer Procedure. For example, NintSelfTxnExpPcfUpdNotifyReq has SLA timeout handling similar to N7 Policy Notify Request (PCF-initiated Modification).

When the procedure timer expires, required clean-up is performed at SMF and peer nodes. This clean-up action is based on the stage at which the dedicated bearer call flow is present. This operation helps in identifying the procedure instances which are waiting for peers response for longer duration and handling them accordingly.

Call Flows

This section describes the following call flows associated with this feature.

PCF-initiated Modification Call Flow

This section explains the processing of PCF-initiated dedicated bearer modification call flow when the procedure SLA timer expires.

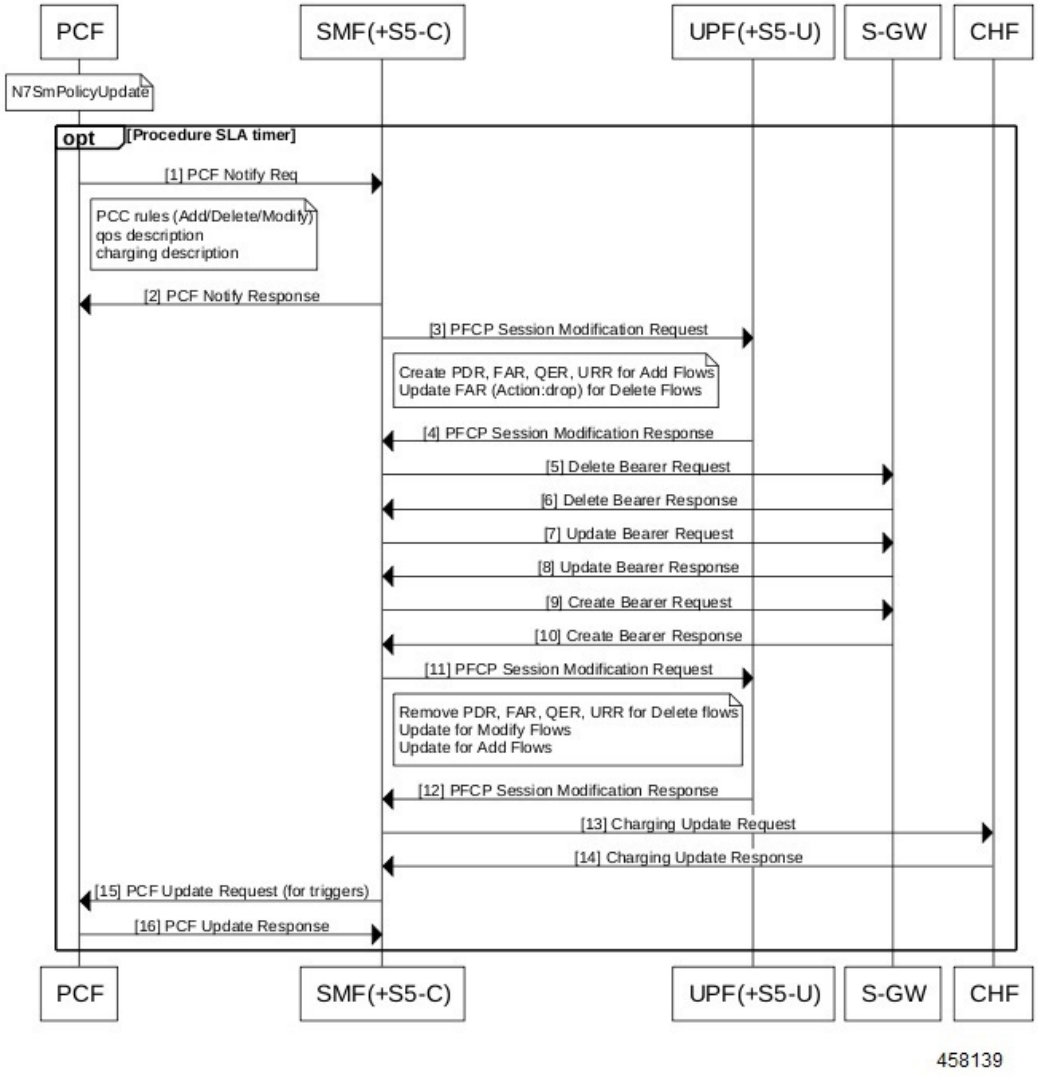
Procedure SLA handling explained in this section include other flavors of dedicated bearer procedure started by internal transactions due to the following triggers:

- PCF-initiated triggers: Piggy-back Dedicated Bearer Procedure, PCF Update/Notify Response triggered Dedicated Bearer Procedure, NIntSelfTxnExpPcfUpdNotifyReq, and so on.
- Other triggers: Clear Sub, Revalidation Timeout, N4 Session Report, Internal Txn to restart dedicated bearer procedure upon collision-abort.

Note The SMF uses procedure SLA configuration for the N7 interface for handling the dedicated bearer procedure failures.

The following figure depicts the dedicated bearer modification call flow initiated by the N7 Policy Notify Request from PCF.

Figure 72: PCF-initiated Modification Call Flow



The following table describes the processing performed at each stage when the procedure SLA timer expires:

Table 79: Processing of PCF-initiated Modification During SLA Timer Expiry

Timeline or Slice availability	Request or Event	Stage - Failure	Timeout due to SLA
Procedure SLA as configured	N7 PCF Notify Request	PCF Notify	Respond to N7 PCF Notify with the HTTP status code "504 Gateway Timeout" and the protocol error as "TIMED_OUT_REQUEST".

Timeline or Slice availability	Request or Event	Stage - Failure	Timeout due to SLA
Procedure SLA as configured		First N4 Modification Request	**For newly added flows:** Async N4 Modification to remove N4 tunnels for the new flows. Send Async PCF update with rule reports based on triggers. **For deleted flows:** Async Delete Bearer Request (DBR) Sync N4 to remove tunnels for deleted rules. Perform sync procedure to avoid loss of usage reports which the UPF sends in N4 modification response for the deleted flows. Async PCF update with rule reports based on triggers.
Procedure SLA as configured		Delete Bearer Request	Sync N4 to remove tunnels for the deleted rules. Perform sync procedure to avoid loss of usage reports which the UPF sends in N4 modification response for deleted flows. Async PCF update with rule reports based on triggers.
Procedure SLA as configured		Update Bearer Request	Not supported currently
Procedure SLA as configured		Create Bearer Request	Async N4 Modification to remove N4 tunnels for the deleted and new flows. Send PCF update with rule reports based on triggers.

Timeline or Slice availability	Request or Event	Stage - Failure	Timeout due to SLA
Procedure SLA as configured		Second N4 Modify Request	**For added flows:** Perform async DBR and async N4 Modification. Send Async Failure Rule report to PCF. **For deleted flows:** Send Async Success Rule report to PCF. Then, update PDU context.
Procedure SLA as configured		Charging Update Request	Last leg, treat as procedure success. Send PCF update with success rule reports based on triggers. Then, update PDU context.
Last Leg – lenient approach no SLA		PCF Update Request	Mark modification complete.

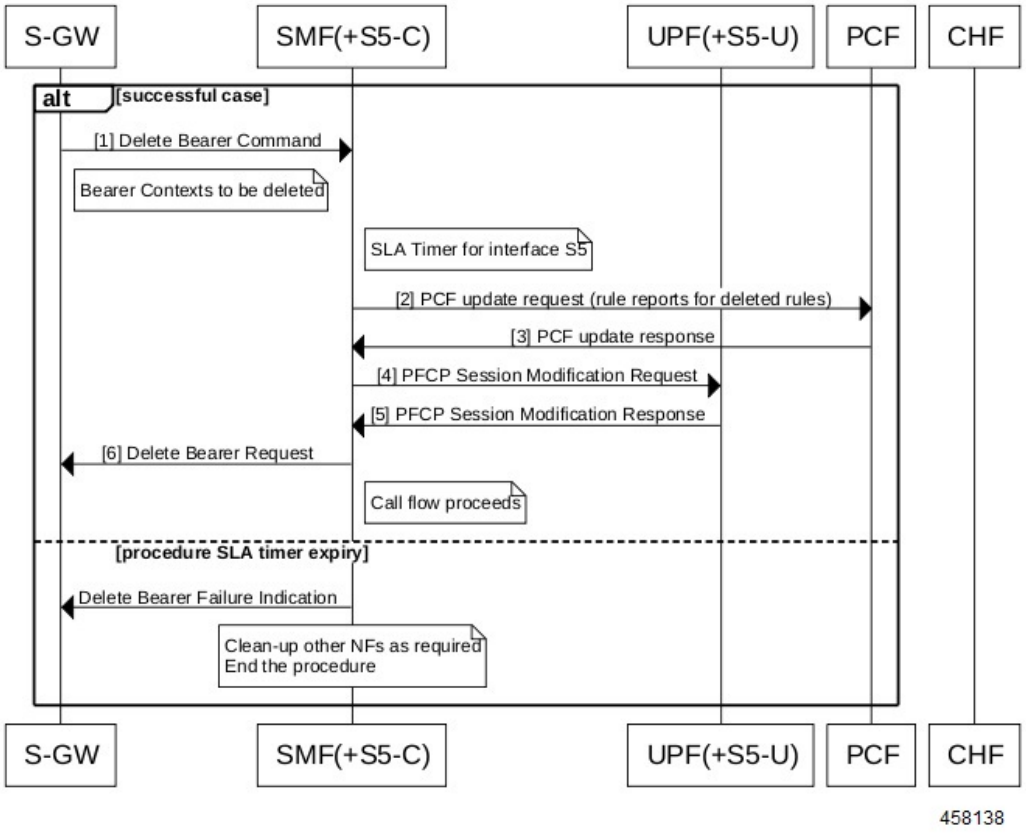
MME-initiated Deletion Call Flow

This section explains the processing of MME-initiated dedicated bearer deletion call flow when the procedure SLA timer expires. Upon the expiry of procedure SLA timer for Delete Bearer Command (DBC), the SMF sends Delete Bearer Failure Indication.

Note The SMF uses procedure SLA configuration for S5 or S2b interface based on the RAT type.

The following figure depicts the dedicated bearer deletion call flow initiated by MME upon receipt of Delete Bearer Command.

Figure 73: MME-initiated Deletion Call Flow



The following table describes the processing performed at each stage when the SLA timer expires:

Table 80: Processing of MME-initiated Deletion During SLA Timer Expiry

Timeline or Slice availability	Request or Event	Stage - Failure	Timeout due to Transaction SLA
Procedure SLA as configured	Delete Bearer Command	Idle	Send Delete Bearer Failure Indication
Procedure SLA as configured		PCF update request	Send Delete Bearer Failure Indication
Procedure SLA as configured		First N4 Modification Request	Async DBR Sync N4 to remove tunnels for the deleted rules. Perform sync procedure to avoid loss of usage reports which the UPF sends N4 modification response for the deleted flows.

Timeline or Slice availability	Request or Event	Stage - Failure	Timeout due to Transaction SLA
Procedure SLA as configured		Delete Bearer Request	Sync N4 to remove tunnels for the deleted rules. Perform sync procedure to avoid loss of usage reports which the UPF sends N4 modification response for the deleted flows.
Procedure SLA as configured		Second N4 Modify Request	Treat as procedure success. Then, update PDU context.
Procedure SLA as configured		Charging Update Request	Treat as procedure success. Then, update PDU context.

Configuring Dedicated Bearer Procedure Failure Handling Feature

This section describes how to configure the Dedicated Bearer Procedure Failure Handling feature.

Configuring Procedure SLA Timer

Use the following sample configuration to configure the procedure SLA timer. The SMF uses this timer to perform the dedicated bearer procedure failure handling operation accordingly.

```
config
   instance instance-id gr_instance_id
      endpoint { dns-proxy | gtp | gtpprime | li | nodemgr | pfcp |
protocol | radius | radius-dns | sbi | service | sgw-service }
         interface { n7 | s2b | s5 }
            sla procedure procedure_time
            end
```

NOTES:

- **endpoint { dns-proxy | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }**: Enters the endpoint configuration for the selected interface. For example, **endpoint sbi** command allows you to enter the SBI endpoint configuration.
- **interface { n7 | s2b | s5 }**: Specify the endpoint interface for which the procedure timer is executing.
- **sla procedure** *procedure_time* : Specify the procedure SLA timer for the selected interface-specific procedure.

  procedure_time must be an integer in the range of 1000-120000.

Verifying Dedicated Bearer Procedure Failure Handling Feature

This section describes how to verify the Dedicated Bearer Procedure Failure Handling feature configuration.

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint** command to verify the procedure SLA timer configuration.

The following is an example output of the **show running-config instance instance-id 1 endpoint sbi** command.

```
smf# show running-config instance instance-id 1 endpoint sbi
instance instance-id 1
 endpoint sbi
  replicas 2
  vip-ip 209.165.200.225
  interface n7
   loopbackPort 9118
   vip-ip 209.165.201.1 vip-port 8090
   sla procedure 4000
  exit
 exit
exit
```

OAM Support for Dedicated Bearer Procedure Failure Handling Feature

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

As part of this feature, new value "timeout" is added to the "reason" label for the smf_service_stats statistics. This new value indicates the expiry of procedure SLA timer.

Troubleshooting Information

This section describes the troubleshooting information.

- Collect the warning and error logs.
- Collect the message traces using the **monitor protocol** command and pcap functionality.
- Examine the statistics of smf_service_stats.

  During the expiry of procedure SLA timer, the reason is shown as “timeout”. The following is an example of smf_service_stats.

For Dedicated Bearer Create:

```
smf_service_stats{Cause="SMF_Internal_Failure",Detailed_Cause="timeout",always_on="disable",app_name="SMF",
cluster="Local",data_center="DC",dcnr="disable",dnn="intershat",emergency_call="false",fourg_only_ue="false",
instance_id="0",pdu_type="ipv4",pra="none",procedure_type="pcf_req_ded_brr_create",qos_5qi="2",
rat_type="EUTRA",reason="timeout",roaming_status="homer",service_name="smf-service",
smf_current_procedure="",status="failures",up_state="UpState_Activated"} 1
```

For Dedicated Bearer Delete:

```
smf_service_stats{Cause="SMF_Internal_Failure",Detailed_Cause="timeout",always_on="disable"
,app_name="SMF",cluster="Local",data_center="DC",dcnr="disable",dnn="intershat",emergency_call="false",
fourg_only_ue="false",instance_id="0",pdu_type="ipv4",pra="none",procedure_type="pcf_req_ded_brr_delete",
qos_5qi="3",rat_type="EUTRA",reason="timeout",roaming_status="homer",service_name="smf-service",
smf_current_procedure="",status="failures",up_state="UpState_Activated"} 1
```

Handling GTP-U Error Indication for 4G Sessions

Feature Description

This section describes how the SMF handles GPRS tunneling protocol, user plane (GTP-U) error indication for the 4G sessions.

Serving Gateway (S-GW) sends GTP-U error indication message including the tunnel IDs to UPF when it receives a GTP-U message with an unknown Tunnel Endpoint Identifier (TEID). The UPF on receiving GTP-U error indication sends N4SessionReportRequest towards SMF including error indication (ERIR). The SMF retrieves EBI based on Fteid included in the N4SessionReportRequest, and initiates deletion of the session or bearer. The SMF sends Delete Bearer Request towards S-GW. On receiving the response from S-GW, the SMF sends either an N4 session modification request or N4 session release request to the UPF based on the bearer type, that is, dedicated or default bearer. CHF and PCF are also notified based on the bearer type.

Note When the SMF receives PFCPSessionReportRequest, the IntSelfTxnN4SessRptReq message is displayed as part of the debug message.

This section also describes how the SMF handles GTP-U Error Indication with Diameter Interfaces.

Standards Compliance

The GTP-U Error Indication Handling feature complies with the following standards:

- *3GPP TS 29.244, Version 15.6.0*
- *3GPP TS 23.527, Version 15.3.0*

How it Works

GTP-U Error Handling Procedure

This section describes the call flow associated with the GTP-U error handling procedure for the 4G sessions.

Figure 74: GTP-U Error Indication Handling Call Flow

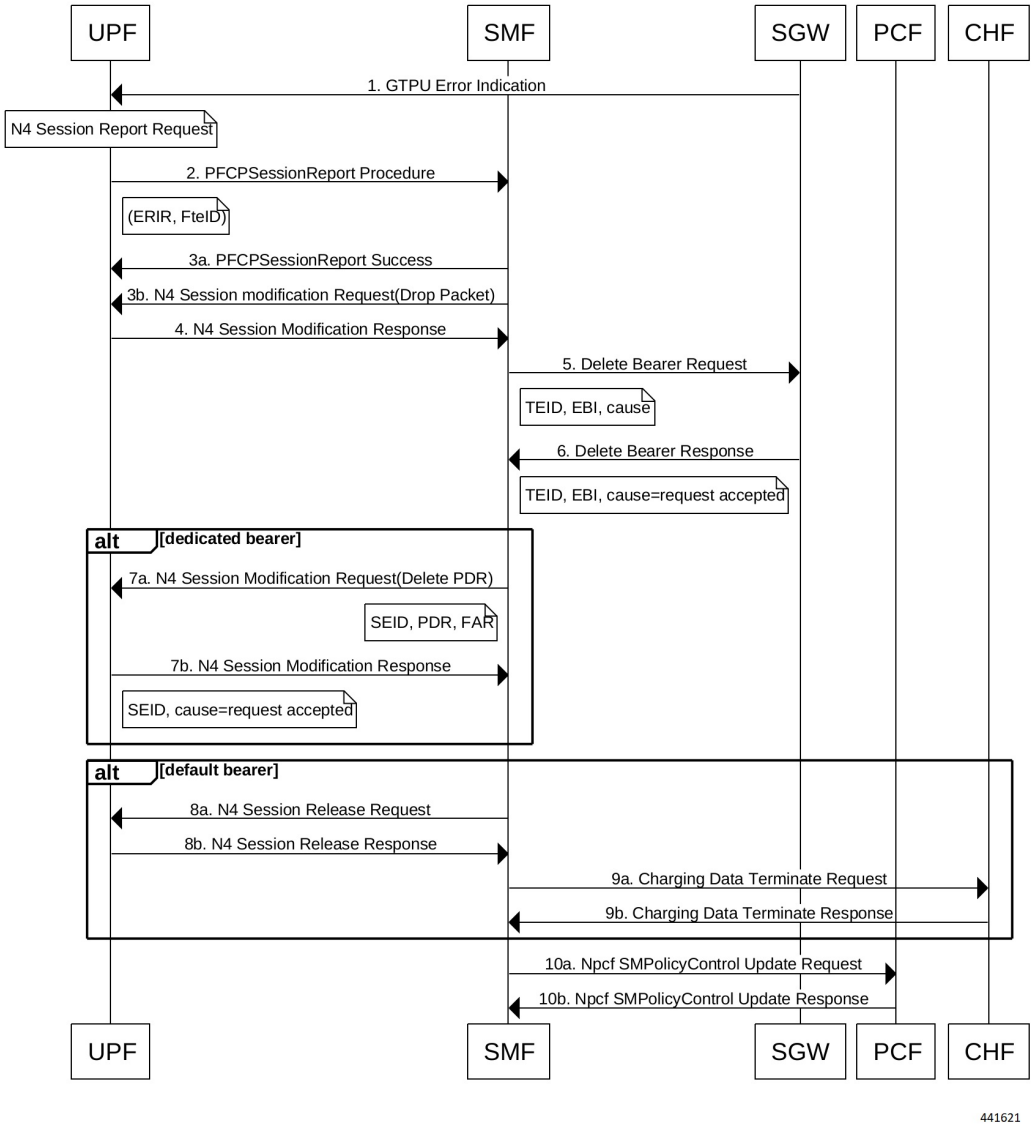


Table 81: GTP-U Error Handling Call Flow Description

Step	Description
1	S-GW sends GTP-U Error Indication towards UPF, indicating the bearer with the failed bearer ID.
2	After receiving GTP-U error indication, the UPF sends PFCPSessionReport towards SMF along with the failed bearer ID.
3a and 3b	The SMF sends PFCPSessionReport Success message and N4 Session Modification Request for dropped packet towards the UPF.
4	The UPF sends N4 Session Modification Response to the SMF.

Step	Description
5	The SMF sends Delete Bearer Request towards S-GW along with TEID, EBI, and cause.
6	The S-GW sends Delete Bearer Response towards SMF along with TEID, EBI, and cause as request accepted.
7a	If the TEID is a dedicated bearer, then the SMF sends N4 Session Modification Request with Delete PDR.
7b	The UPF sends N4 Session Modification Response.
8a	If it is a default bearer, the SMF sends N4 Session Release Request.
8b	The UPF sends N4 Session Release Response.
9a	The SMF sends Charging Data Terminate Request towards CHF.
9b	The CHF responds with Charging Data Terminate Response.
10a	The SMF sends SMPolicyControl Update Request towards PCF.
10b	The PCF sends SMPolicyControl Update Response to the SMF.

GTP-U Error Indication with Diameter Interfaces

SMF supports session report with Error Indication (ERIR). SMF responds to a session report stateless and then processes the request. SMF starts disconnect procedure of 4G sessions on receiving ERIR and triggers Delete Bearer Response (DBR) to S-GW or MME if the ERIR is for default bearer. For more information about the call flow and description, see the UPF-initiated Detach Procedure section.

Configuring Delayed Deletion of Session

Use the following configuration in SMF to delay the disconnect of session after receiving Session Report with ERIR. This configuration is only applicable for default bearer.

```
config
   profile access access
      erir delay  delay_interval
   exit
```

NOTES:

erir delay *delay_interval*: Specify the delay time in milliseconds and the range between 0-3000. Default value is 0 (Disabled).

GTP Path Failure Handling, Restoration, and Recovery

Feature Description

SMF supports:

- Handling of the following GTP-C path management messages as per *3GPP TS 29.274*

  - Echo Request
  - Echo Response

- Sending an Echo Request message to the newly discovered GTP-C peer as per the configuration.
- Sending an Echo Response message as a reply if it receives an Echo Request message from GTP-C peer.
- Retransmitting an Echo Request message to GTP-C peer for configured number of times in case of no response received.
- Clearing all the subscribers associated to a GTP-C peer in case of no response received for an Echo Request message for the configured number of times for that GTP-C peer.
- Clearing all the subscribers associated to a GTP-C peer in case of a different recovery value received from that GTP-C peer.

The feature complies with the following standards:

- *3GPP TS 29.274, version 15.8.0*
- *3GPP TS 23.007*

Note This feature is applicable on 4G calls with legacy interfaces.

Call Flows

The following call flows capture information specific to how GTP-C path management and GTP-C restoration messages are handled.

GTP-C Path Management

Figure 75: GTP-C Path Management

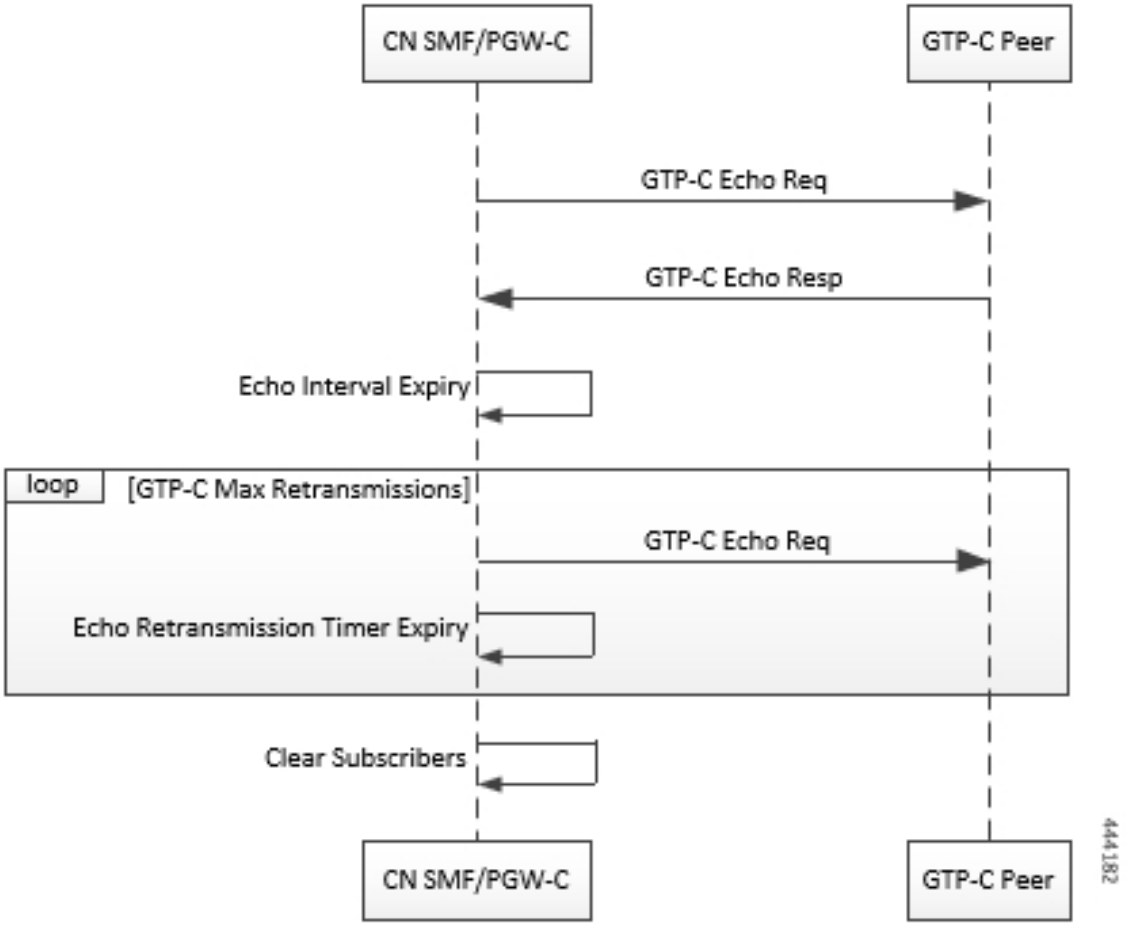


Table 82: GTP-C Path Management

Step	Description
1	Once the GTP-C peer is discovered (an Initial GTP-C Create Session Request or an GTP-C Modify Bearer Request message is received), CN SMF/PGW-C starts sending GTP-C Echo Request Messages periodically to the new GTP-C Peer as per configuration.
2	If GTP-C Echo response is not received, CN SMF/PGW-C retries sending GTP-C Echo Request (configured) N3 times for every configured T3 timer expiry.
3	Once all retries are exhausted, CN SMF/PGW-C clears all the sessions associated to that GTP-C peer.

GTP-C Echo Request Handling

Figure 76: GTP-C Echo Request Handling

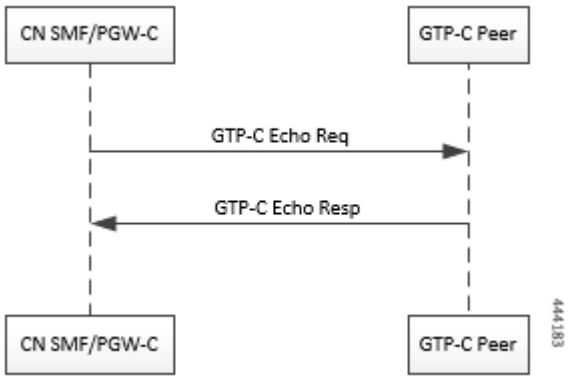


Table 83: GTP-C Echo Request Handling

Step	Description
1	Whenever a GTP-C Echo Request message is received from a GTP-C peer, CN SMF/PGW-C sends GTP-C Echo Response message as a reply.

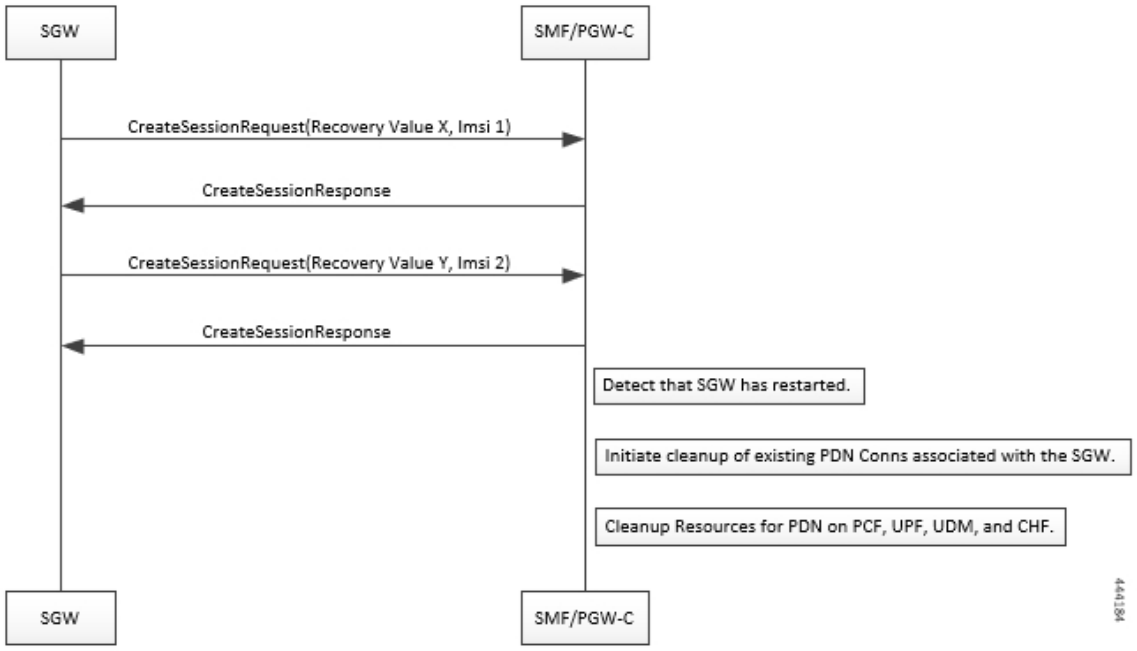
GTP-C Restoration on PGW-C/SMF

PGW-C/SMF can detect that there is a change in recovery value of SGW. PGW-C/SMF can detect this value from the following messages:

- Create Session Request
- Modify Bearer Request
- Create Bearer Response
- Echo Response

If PGW-C/SMF detects that there is a change in recovery value, then it initiates the cleanup of all the PDN connections associated with the SGW.

Figure 77: GTP Restoration due to SGW Restart



Memory and Performance Impact

The Node Manager pod to GTP-C peer path mapping is maintained in etcd and also in the local cache of NodeMgr and GTP-C Pods.

Configuring Echo at GTP Endpoint

Use the following sample configuration to configure the echo parameters at GTP endpoint.

```
config
   instance instance-id gr_instance_id
   endpoint gtp
      interface { s2b | s5 | s5e | s8 | s11 }
      echo interval echo_interval
      echo retransmission-timeout retransmission_timeout_value
      echo max-retransmissions max_retry_count
      end
```

Sample Configuration

```
[unknown] smf# config
Entering configuration mode terminal
[unknown] smf(config)# instance instance-id 1
[unknown] smf(config-instance-id-1)# endpoint gtp
[unknown] smf(config-endpoint-gtp)#
[unknown] smf(config-endpoint-gtp)# interface
s2b s5 s5e s8 s11
[unknown] smf(config-endpoint-gtp)# interface s5
[unknown] smf(config-interface-s5)# echo interval 60
```

```
echo – Enable gtpc path management
interval - Configure echo interval in seconds, ranging from <60-360>
[unknown] smf(config-interface-s5)# echo retransmission-timeout 3
retransmission-timeout - Configure the echo retransmission timeout in seconds, ranging from
 <1-20>
[unknown] smf(config-interface-s5)# echo max-retransmissions 10
max-retransmissions  - Configure maximum retries for GTP echo request, ranging from <0-10>
[unknown] smf(config-interface-s5)#
```

Show Command

The `show peers all` command displays all the connected GTP peers and their node information.

Example:

```
[unknown] smf# show peers all
CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE TIME RPC ADDITIONAL DETAILS
 GR INSTANCE
------------------------------------------------------------------------------------------------------------------------
S5/S8 209.165.201.15:2123209.165.201.16:2123Inbound smf-nodemgr-1 Udp 4 minutes SGW Recovery:
 100, MaxRemoteRcChange:1 1
```

The `show peers all` command is enhanced to display last restart information.

Example:

```
[unknown] smf# show peers all
CONNECTED
ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE TIME RPC ADDITIONAL DETAILS
 GR INSTANCE
------------------------------------------------------------------------------------------------------------------------
S5/S8 209.165.201.15:2123209.165.201.16:2123Inbound smf-nodemgr-1 Udp 4 minutes SGW Recovery:
 100 last-restart-time 1
```

Bulk Statistics

The following dedicated disconnect reasons are used for PDN connections cleared due to peer GTP-C restart or path failure.

- disc_pdnrel_gtpc_peer_restart
- disc_pdnrel_gtpc_peer_pathfail

The following bulk statistics are added in nodemgr pod.

```
# HELP nodemgr_gtpc_msg_stats Gtpc Msg Stats
# TYPE nodemgr_gtpc_msg_stats counter
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_rx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_tx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 4
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_rx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_tx",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="nodemgr"}
 1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
```

```
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="nodemgr"}
 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="209.165.200.239",gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="nodemgr"}
 1
```

Following bulk statistics are added as part of GTP-C Path failure Enhancements:

```
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type="
 gtpc_false_peer_restart_ignore_rc_cfg
",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type="
gtpc_ignore_echo_timeout "
,gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"} 1
```

Following bulk statistics are added as part of GTP Peer Restart Detection Enhancement:

```
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",gtpc_msg_type=
"
gtpc_false_peer_restart_cfg_rc_change",gtpc_peer_ip="209.165.200.239",instance_id="0",service_name="smf-nodemgr"}
 1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="smf-nodemgr"} 1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",gtpc_peer_ip="209.165.200.239"
,gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="smf-nodemgr"} 1
```

Limitations

From *3GPP TS 23.007*, Section 20: It is recommended that GTPv2 Echo Request should be sent only when a GTP-C entity has not received any GTP response message for a previously sent request message on the GTP-C path for, an implementation dependent time period.

Currently, this is not supported.

Even if SMF receives GTPC echo req from peer, it is considered as path is up. The subsequent Echo Req from SMF is received after the echo interval expiry.

Configuration Support for Rejecting 4G-only Devices

The SMF provides configuration support to reject calls from 4G-only UE devices.

To reject calls from 4G-only UE devices, use the following configuration:

```
config
   profile dnn dnnprofile_name
      only-nr-capable-ue true
      end
```

NOTES:

- **only-nr-capable-ue true**: Enable this command to reject any new call attempt for PDN session creation from a 4G only capable UE device.

Change Notification Request Handling

Feature Description

SMF supports the change notification requests with ULI for 4G calls with legacy interface.

SMF can process the following request messages only when either Gx or Gy interface is enabled:

- Change Notification with ULI change
- Change Notification with no change in ULI

Change Notification with ULI Change

This section describes the change notification request and the response call flow with ULI change.

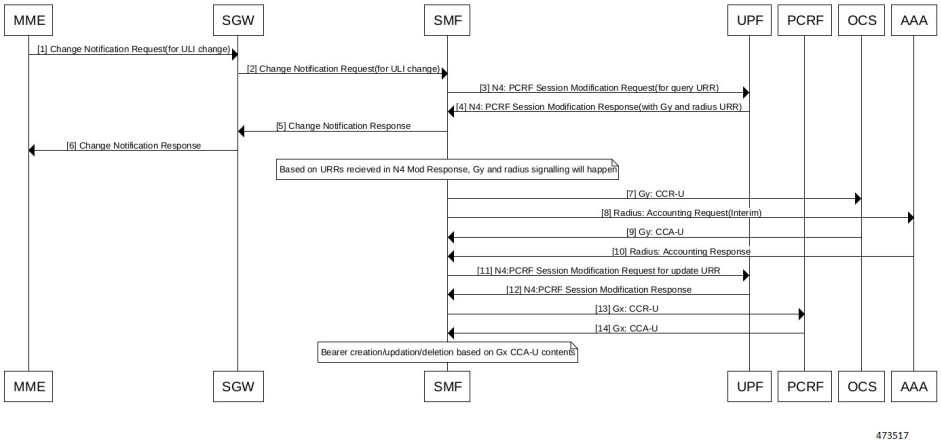


Table 84: Change Notification with ULI Call Flow Description

Step	Description
1	The MME sends a Change Notification Request (for ULI change) to SGW.
2	The SGW forwards a Change Notification Request to SMF.
3	The SMF sends a N4 Session Modification Request for query URR to UPF based on the event triggers armed. **Note** USER_LOCATION_CHANGE event triggers for ULI change.

Step	Description
4	The UPF responds with a N4 Session Modification Response with Gy, and radius URR SMF based on Gy and radius configuration(enabled/disabled).
5	The SMF sends a Change Notification Response to SGW.
6	The SGW forwards a Change Notification Response to MME.
7	Based on the URRs received in N4 Modification Response, Gy, and radius signaling occurs.
8	The SMF sends a CCR-U to OCS and Radius Accounting Request to AAA.
9	The responds with a CCA-U and AAA with Radius Accounting Response.
10	The SMF sends a N4 Session Modification Request for update URR to UPF.
11	The UPF sends a N4 Session Modification Response to SMF.
12	If the event trigger arms, the SMF sends a CCR-U to the PCRF. **Note** USER_LOCATION_CHANGE event triggers for ULI change.
13	The PCRF then sends a CCA-U to SMF.
14	Now, Bearer creation/update/deletion occurs based on Gx CCA-U contents.

Change Notification with No Change in ULI

This section describes the change notification request and the response call flow with no change in ULI.

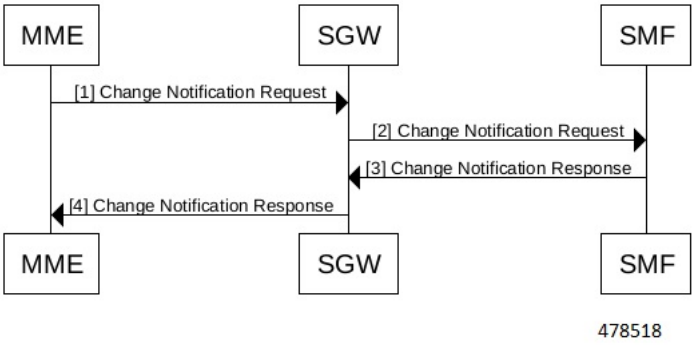


Table 85: Change Notification with No Change in ULI Description

Step	Description
1	The MME sends a Change Notification Request to SGW.
2	The SGW sends a Change Notification Request to SMF.
3	The SMF sends a Change Notification Response to SGW.
4	The SGW sends a Change Notification Response to MME.

Call Flows

This section describes the key call flows for this feature.

- Change Notification with ULI Change, on page 274
- Change Notification with No Change in ULI, on page 275

Change Notification with ULI Change

This section describes the change notification request and the response call flow with ULI change.

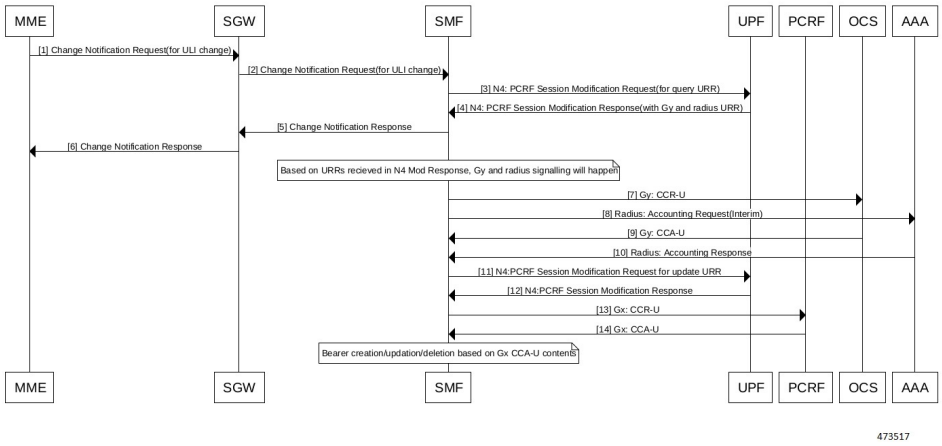


Table 86: Change Notification with ULI Call Flow Description

Step	Description
1	The MME sends a Change Notification Request (for ULI change) to SGW.
2	The SGW forwards a Change Notification Request to SMF.
3	The SMF sends a N4 Session Modification Request for query URR to UPF based on the event triggers armed. **Note** USER_LOCATION_CHANGE event triggers for ULI change.
4	The UPF responds with a N4 Session Modification Response with Gy, and radius URR SMF based on Gy and radius configuration(enabled/disabled).
5	The SMF sends a Change Notification Response to SGW.
6	The SGW forwards a Change Notification Response to MME.
7	Based on the URRs received in N4 Modification Response, Gy, and radius signaling occurs.
8	The SMF sends a CCR-U to OCS and Radius Accounting Request to AAA.
9	The responds with a CCA-U and AAA with Radius Accounting Response.
10	The SMF sends a N4 Session Modification Request for update URR to UPF.

Step	Description
11	The UPF sends a N4 Session Modification Response to SMF.
12	If the event trigger arms, the SMF sends a CCR-U to the PCRF. **Note** USER_LOCATION_CHANGE event triggers for ULI change.
13	The PCRF then sends a CCA-U to SMF.
14	Now, Bearer creation/update/deletion occurs based on Gx CCA-U contents.

Change Notification with No Change in ULI

This section describes the change notification request and the response call flow with no change in ULI.

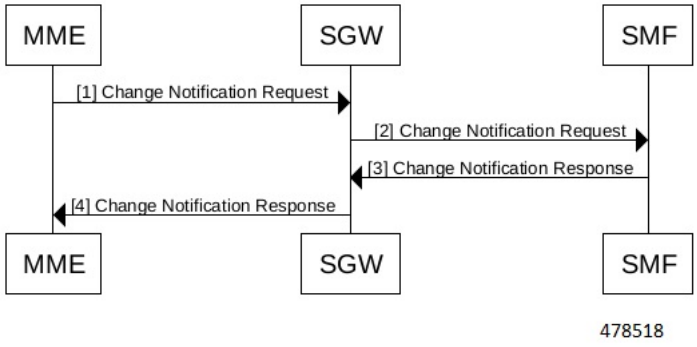


Table 87: Change Notification with No Change in ULI Description

Step	Description
1	The MME sends a Change Notification Request to SGW.
2	The SGW sends a Change Notification Request to SMF.
3	The SMF sends a Change Notification Response to SGW.
4	The SGW sends a Change Notification Response to MME.

Dynamic Configuration Change Support

Feature Description

The SMF allows you to change Access Profile configuration dynamically, without any impact on the existing sessions. For instance, when the configuration dynamically updates the current session continues to use the old values in the in-progress call flow or procedure.

How it Works

This section describes how dynamic change in configuration works for the supported Access Profile configurations.

Access Profile

The Access Profile defines the various parameters for the access-profile configuration.

The following table lists the configurations that allow dynamic update.

Table 88: Access Profile Parameters

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
eps-fallback cbr	**eps-fallback cbr delay** *delay* **max-retry** *retry_count* **timeout** *timeout*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n1 t3591-pdu-mod-cmd	**n1 t3591-pdu-mod-cmd timeout** *timeout* **max-retry** *retry_count*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n1 t3592-pdu-rel-cmd	**n1 t3592-pdu-rel-cmd timeout** *timeout* **max-retry** *retry_count*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value. **Note** The SMF does not support the timer functionality associated to this configuration.
n2 idft enable	**n2 idft enable timeout** *timeout*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
n26 idft enable	**n26 idft enable timeout** *timeout*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n11 n11-failure-profile	**n11 n11-failure-profile** *failure_profile*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value. If the associated Failure-Handling Profile gets deleted or any of the parameters are modified, then the existing call flows are not impacted, which means that the existing call flows continue using the old value.
gtpc gtpc-failure-profile	**gtpc gtpc-failure-profile** *failure_profile*	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value. If the associated Failure-Handling Profile gets deleted or any of the parameters are modified, then the existing call flows are not impacted, which means that the existing call flows continue using the old value.

Semantic and Syntactic Error Handling for 4G and 5G

Table 89: Feature History

Feature Name	Release Information	Description
MBFR, Semantic and Syntactic Error Handling for 4G and 5G	2023.04	SMF handles MBFR, semantic and syntactic errors in QFI,QoS and indicates 5GSM cause. Configurations using event names, rules and actions are included for 4G and 5G errors. **Default Setting**: Disabled – Configuration required to enable

Feature Description

SMF receives the semantic and syntactic errors for QoS rules and QoS description or for mapped EPS Bearer Contexts from the UE.

Error Received While UE is in 5G RAT

- SMF receives the following 5G errors:
  - Semantic error in QoS Operation
  - Syntactic error in QoS Operation
  - Invalid mapped EPS bearer identity

  Following are the applicable actions for configuration:
  - release-session
  - release-flow

- SMF receives the following 4G errors:
  - Syntactical error in packet filters
  - Semantic error in packet filters
  - Syntactical error in TFT Operations
  - Semantic error in TFT Operations

  Following are the applicable actions for configuration:
  - release-session
  - release-flow - Also considered as release bearer

- release-session-ho - SMF retains the flow on 5G and releases during 5G to 4G HO. No impact on 5G to WIFI HO.

Error Received While UE is in 4G RAT

- SMF receives the following 4G errors:
  - Syntactical error in packet filters
  - Semantic error in packet filters
  - Syntactical error in TFT Operations
  - Semantic error in TFT Operations

  Following are the applicable actions for configuration:
  - release-session
  - release-flow - Also considered as release bearer
- SMF receives the following 5G errors:
  - Semantic error in QoS Operation
  - Syntactic error in QoS Operation
  - Invalid mapped EPS bearer identity
  - Syntactical error in packet filters
  - Semantic error in packet filters

  Following are the applicable actions for configuration:
  - release-session
  - release-flow
  - release-session-ho - SMF retains the flow on 4G and releases during 4G to 5G HO. No impact on 4G to WIFI HO.

Cause Handling

SMF supports 4G and 5G Session Management (5GSM) cause handling for the UE-initiated and network-initiated procedures.

N1 Cause Handling for 5G

Following are the supported procedures:

- PDU Session Modification Reject
- PDU Session Modification Request

PDU Session Modification Reject

In N1 PDU Session Modification Reject, the SMF considers the flow creation or modification as a failure and aborts the procedure. Failure notification is sent to PCF.

The `pdu-modify` statistics is added for this cause.

PDU Session Modification Request

SMF handles the N1 PDU Session Modification Request with the mapped EPS Bearer Context with appropriate EBI and an operation code that indicates **Delete existing EPS bearer**. The configuration for the action to be taken handles this scenario.

Semantic and Syntactic Error Handling for 4G

CB Response and UB Response

SMF handles the CB or UB response along with the ePCO containing 5GSM cause.

Different actions occur based on the configuration values for `actiondef`.

SMF supports the CB Response and UB Response from MME. Following is the order of MME/UE cause evaluation:

1. Session level
2. Bearer level
3. ePCO level

There is no support for release bearer in a default bearer action.

Note SMF supports all these causes for emergency sessions.

MFBR Parameter in GBR QoS Flow

MFBR (Maximum flow bit rate) validation is added on receiving an GBR flow creation or QoS modification from PCF.

If the flow is a GBR QoS flow, add MFBR uplink or MFBR downlink as the mandatory parameters. Following are the conditions for validation.

- Either MFBR UL (uplink) or MFBR DL (downlink) should be a non-zero
- GFBR UL should be less than or equal to MFBR UL
- GFBR DL should be less than or equal to MFBR DL

Following are the validation methods from the call flow:

- Validate the conditions when SMF is acting as SMF(Homer) and SMF(Roamer) while the rules are received from PCF .
- Validate the N16 QoS flow for the conditions when the flow received from the hSMF(Roamer) in SMF(Visitor).

Configuration for Semantic and Syntactic Error Handling

Configuration for Adding Event Management Policy

Adding event management policy happens through following configuration:

```
config
   policy eventmgmt policy_eventmgmt_name
      priority  event_priority [ event event_name ] ruledef ruledef_name actiondef
 actiondef_name
      exit
```

NOTES:

- **eventmgmt** *policy_eventmgmt_name*—This CLI allows configuring the event management policies and defining the attributes.
- **priority** *event_priority*—Allows defining the priority of a particular event management policy.
- **event** *event_name*—This is an optional CLI that defines an event for which a particular action is to be performed. It supports the following event names:

  Table 90: Events for Semantic and Syntactic Error Handling

Events	Description
n1-modify	N1 modify request/response
cb-resp	Create bearer response
ub-resp	Update bearer response

  If the **event** is not configured, **actiondef** is executed for all the defined events in case of a rule match.

- **ruledef** *ruledef_name*—Defines a rule for a local policy that when matched an action is performed.
- **actiondef** *actiondef_name*—Configures the action name to be executed.

Configuration for Adding Rule Definition Policies

Following configuration allows adding rule definition policies:

```
config
   policy rulemgmt policy_rulemgmt_name
      ruledef rule_def condition cause cause_string source source_value
      exit
```

- **rulemgmt** *policy_rulemgmt_name*—Defines a rule to be added in the policies.
- **ruledef** *rule_def*—Configures a rule attributes. A ruledef is declared when the conditions match.
- **condition**—Defines the use cases for a rule.

  Cause *cause_string* - It supports **cause-value matches** condition along with the mandatory source value.

- **source** *source_value* —Defines the source for a rule.

  ue, **ran**, **mme** and **amf** are the possible source values.

Configuration for Adding Action Definition Policies

Following configuration adds action definition policies:

```
config
   policy actionmgmt policy_actionmgmt_name
      actiondef actiondef_name
         priority priority_number action action_name [ attributes { rulebase
rulebase_name [ rules rules_name ] } ]
         exit
```

NOTES:

- **actionmgmt** *policy_actionmgmt_name*—Configures the action to be executed.
- **actiondef** *actiondef_name*—Defines the action attributes to be executed.

  The actions differ while the UE is in the 4G or 5G RAT.
- **priority** *priority_number*—Defines the priority in which the actions are to be executed.
- **action** *action_name*—Defines the actions associated with an actiondef in the order of priority. Following action names are used here:
  - release-session
  - release-flow
  - release-flow-ho
- **attributes** —Defines the attributes of a particular action. This is an optional command.
- **rulebase** *rulebase_name*—Defines a collection of protocol rules to match a flow and associated actions to be taken for matching flow.
- **rules** *rules_name*—Defines a list of rules to be executed.

Configuration Example

Example 1: Following is the sample configuration using **n1-modify** event name for the event management configuration:

```
policy eventmgmt evt1
priority 1 event n1-modify ruledef rd1 actiondef ad1
```

Example 2: Following is the sample configuration for adding **cause-source matches** rule definition policy:

```
policy rulemgmt rm1
ruledef rd1
condition cause matches [ 83 ] source ue
```

Example 3: Following is the sample configuration for adding error handling action definition policies:

```
policy actionmgmt am1
actiondef ad1
priority 1 action release-session
priority 2 action release-flow
exit
actiondef ad2
priority 1 action release-flow
exit
```

```
actiondef ad3
priority 100 action release-flow-ho
```

Bulk Statistics Support

1. Following are the statistics for CB Response or UB Response handling with cause errors in 4G:

   - `disc_admin_event_mgmt` - Disconnect reason for release session action.

     Following is an example:

     ```
     smf_disconnect_stats
     {app_name="SMF",cluster="SMF",data_center="DC",gr_instance_id="1",instance_id="1",rat_type="EUTRA",
     reason="disc_admin_event_mgmt",roaming_status="homer",service_name="smf-service",severity="normal",snssai=""}
      11
     ```

   - `create_bearer_resp` - Message type with the respective cause and action for release Bearer or release bearer HO action.

     Following is an example:

     ```
     smf_gtpc_msg_stats
     {app_name="SMF",cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
     instance_id="0",message_type="create_bearer_resp",qos_5qi="",rat_type="EUTRA",reason="76_mme_release_flow",
     service_name="smf-service",smf_current_procedure="pcf_req_ded_brr_create",snssai="",status="failures"}
      1
     ```

2. Following are the statistics for handling of N1 PDU Session Modification Reject or N1 PDU Session Modification Request with cause errors in 4G and 5G:

```
smf_service_stats :

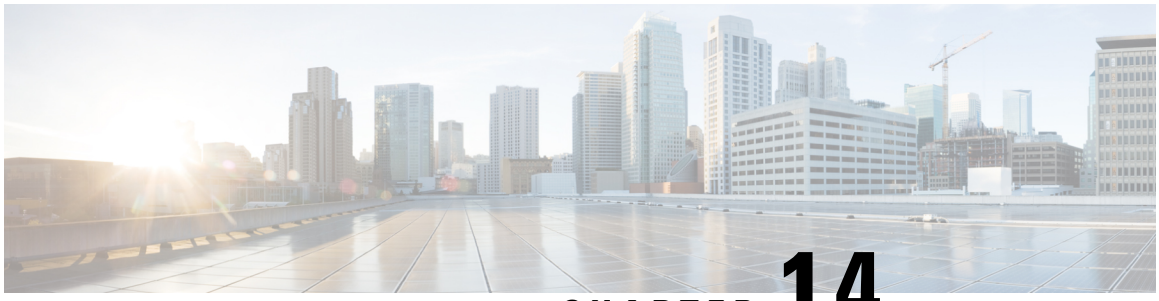
Cause = updated with the cause received in “N1 PDU Session Modification Command Reject” or
 “N1 PDU Session Modification Request”

Detailed_Cause = updated with the Source of cause
procedure_type = updated with "ue_req_pdu_sess_mod” or “pcf_req_pdu_sess_mod”
reason  =  Updated with "Cause"_"Detailed_Cause"_"Action"
```

Following are the examples:

```
smf_service_stats{Cause="84",Detailed_Cause="ue",always_on="",app_name="SMF",
cluster="SMF",data_center="DC",dcnr="",dnn="",emergency_call="false",fourg_only_ue="",
gr_instance_id="1",gtpc_bypass="",idle_mode="",instance_id="1",local_policy="",pdu_type="ipv4",
policy_type="",pra="",procedure_type="ue_req_pdu_sess_mod",qos_5qi="",rat_type="NR",
reason="84_ue_release_flow",roaming_status="homer",
service_name="smf-service",smf_current_procedure="",snssai="",status="success",
up_state="UpState_Activated",upip_active=""}
```

```
smf_service_stats{Cause="85",Detailed_Cause="ue",always_on="",app_name="SMF",
cluster="SMF",data_center="DC",dcnr="",dnn="",
emergency_call="false",fourg_only_ue="",
gr_instance_id="1",gtpc_bypass="",idle_mode="",instance_id="1",local_policy="",pdu_type="ipv4",
policy_type="",pra="",procedure_type="pdu_session_modification_command_reject",qos_5qi="",
rat_type="NR",reason="85_ue_release_flow_Ho",
roaming_status="homer",service_name="smf-service",
smf_current_procedure="pcf_req_pdu_sess_mod",snssai="",status="failures",
up_state="UpState_Activated",upip_active=""}
```



CHAPTER 14

Event Detail Records

- Feature Summary and Revision History, on page 287
- Feature Description, on page 288
- Configuring EDRs, on page 349
- OAM Support for EDR Logging, on page 353

Feature Summary and Revision History

Summary Data

Table 91: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platforms	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 92: Revision History

Revision Details	Release

Introduced support for the following enhancements:
• EDR generation for dedicated bearer and handover (pathswitchreq (Xn handover), pdun2ho, pdn5g4gHo, nrtountrustwifiho, pdun26ho, utn3gppto5g) procedures
• Archival of EDR files in EDR Monitor pod
• New commands to
  • Enable EDR for all subscribers
  • Configure transaction EDR rate, CPU threshold, session threshold, and file archival policy
	2022.04.0

Introduced EDR support for PDU session modification procedure for roaming and non-roaming scenarios	2021.02.2
Provided support for event-level EDR generation	2021.02.0
Custom EDR Generation	2021.01.0

Feature Description

Event Data Records (EDRs) collect information that you can use to perform the following functions:

- Debug or understand the application behavior
- Diagnose the call flow for the specific subscribers

The SMF supports logging of EDRs for both 4G and 5G subscriber sessions including non-roaming and roaming sessions. If the EDR Support feature is enabled, then in a roaming scenario, hSMF and vSMF generate EDRs for PDU session establishment and release procedures. The SMF generates EDR files in comma-separated value (CSV) format. The SMF stores one CSV record per line. The CSV files can be optionally compressed before sending to an external server.

The SMF treats a request message and response message as one EDR event record. For example, N11SmContextCreateReq and N11SmContextCreateResp attributes are logged as an EDR event.

The SMF supports EDR file generation for transaction and transaction-collision level details for subscriber sessions. By default, the EDR generation is disabled.

In release 2021.02.0, the SMF generates EDRs with procedure-level details, event-level details, and field-level details. These granular details help in debugging errors and issues.

EDR Format

In addition to the existing Transaction EDR fields, the application appends procedure-id and event-id along with the respective field values. Application registers the procedure-id, event-id, and field-id along with the corresponding names. This mapping is used to format the CSV event entry in the EDR. Each event entry consists of comma-separated procedure-id, event-id, and field-value. These registered mappings can also be used in CLI commands to disable EDRs at procedure, event, or field level. You can enable or disable the EDRs dynamically during runtime. The existing EDR records remain the same and the runtime changes get reflected only in the newly generated EDR records.

Transaction EDR Format

Transaction-EDR-Fields, list of event-entries [ ]

Event Entries

Procedure-id1, Event-id1, list of field-id1-values [ ]

The following is a sample transaction entry along with a list of events in the CSV format.

```
Version, Field-Count, Transaction-id-value, Start-Time, Elapsed-Time, ……,
Procedure-id1, event-id1, field-id1-value, field-id2-value……,
Procedure-id1, event-id2, field-id1-value, field-id2-value……,
Procedure-id1, event-id3, field-id1-value, field-id2-value……
```

Note There might be different set of fields for a combination of procedure-id and event-id. You can enable or disable the EDRs dynamically during runtime by using a CLI command. For configuration details, see the Configure EDR Files for Generation, on page 350 section in this guide.

EDR File Storage Location

This section provides details on the archival location of EDR files in SMF service pod and EDR monitor pod.

EDR Files in SMF Service Pod

The EDR file is generated in each SMF service pod where the subscriber sessions and events are processed. Based on the EDR file size, the files are archived periodically in non-persistent volume, that is, the SMF service pod. A new file is created before archiving the existing file.

The format of the transaction EDR file name and transaction collision EDR file name are as follows:

<pod-name>_<pod_instance>_<PodStartTime>.transaction.csv

<pod-name>_<pod_instance>_<PodStartTime>.transaction_collision.csv

The directory path of service pod is `/tmp/edr/`.

Example:

smf-service-n0-0_0_ 20220730233455.transaction.csv

Where the pod name is smf-service-n0-0, pod instance is 0, and the pod start time "20220730181014" means 30nd July 2022 18:10:14 UTC.

The format of compressed file name is as follows:

<pod-name>_<pod_instance>_<PodStartTime>.transaction.csv.<fileArchivedTime>.<FileRotationCounter>.gz

Example:

example-service-n0-0_1_20220730181014.transaction.csv.20220730181844.1.gz

EDR Files in EDR Monitor Pod

The SMF service pod sends all the EDR files to edr-monitor pod every 30 seconds. The EDR files remain in edr-monitor pod persistent directory as .csv file. When the total size of all the files exceeds the configured maximum file size, the oldest file is deleted.

The format of file name in edr-monitor pod is <*pod-name*>_<*pod_instance*>_<*PodStartTime*>.*transaction.csv*.

Example:

edr-monitor pod-n0-0_0_ 20220730233455.transaction.csv

The directory path of edr-monitor pod is `/logs/edr/`.

The EDR file size, maximum archived EDR file count, and maximum persistent volune size are configured through CLI commands. For information on the configuration commands, see the Configure EDR Parameters, on page 350 section.

To access the files in the persistent volume of EDR monitor pod, log on to the Ops center with required credentials, and use the edr-monitor pod ingress URL.

To determine the ingress URL, use the following command:

kubectl get ingress -n *namespace* **| grep edr**

Example:

cloud-user@svi-cndp-tb41-gr-setup-smf-cluster-2-cndp-server-1:~$ **kubectl get ingress -n smf-smf | grep edr**

edr-archives-smf-smf nginx **edr-archives.smf-smf.172.18.128.82.nip.io** 10.109.13.65 80, 443 4d5h

EDR Transaction File

The EDR transaction file dumps the transaction information at the end of the transaction. By default, the file generation is disabled.

The following table provides the information that is stored in the file.

Table 93: EDR Transaction File Fields

Field Number	Field Name	Field Description
1	Version	EDR version number. Default value is v1. **Note** The version will change only when there is a change in the encoding order of transaction header fields or change in encoding procedure of any individual field.
2	Field Count	Total number of fields in transaction EDR header. The default value is 15.
3	Transaction ID	Transaction ID

Field Number	Field Name	Field Description
4	Start Time	The transaction start time in yyyy/MM/dd HH:mm:ss.SSS format.
5	Elapsed Ms	The time taken for transaction to end in milliseconds.
6	Subscriber ID	The subscriber ID. For example, imsi-123456789012345
7	Transaction Type	The transaction type (integer) which is defined internally in the application.
8	Transaction Description	The transaction description in string format.
9	Session Primary Key	The primary key of the session.
10	Session Unique Keys	The unique keys for the session separated by |.
11	Session Non Unique Keys	The non-unique keys for the session separated by |.
12	Status	The transaction status (success or error).
13	Status Code	The transaction status code to indicate the failure reason.
14	Procedure Name	The procedure name for which the transaction is submitted.
15	Sub Procedure Name	The sub procedure name for which the transaction is submitted.

Field Number	Field Name	Field Description
16	State	The transaction state. It can be: • Started • New • Ready • Active • Pending • Suspend • SuspendWaitingForResponse • SuspendWaitingForLock • Abort • Finished • Timeout • Unknown
17	Execution stages	The list of stages the transaction went through its lifecycle separated by |

NOTES:

- Each field is separated by comma (,).
- Fields session_uks, session_nuks, execution_stages are a list. These fields are separated by pipe (|). For example, session_uks is denoted as uk1|uk2|uk3.

CSV Format Examples:

```
V1,15,1,2022/08/03
22:12:19.42,22,imsi-123456901234,205,58,CreateSessReq,imsi-123456901234,imsi-123456901234,12.0.0.1|intersat:12.0.0.1|imsi-123456901234,201,10::|intersat:201,10::|1|imsi-123456901234,4|imsi-
123456901234,intersat,roaming,status,none|type,mobile|supi:imsi-123456901234|gpsi,msisdn-233101010101|pei:imei-123456666660|psc,5|snssai:02abf123|dnn,intersat|emergency,false|atsss,false|
 non-3gpp access|
creativity,4|dnai,2001:2:6|dnai,2001:2:6|authstatus,authenticated|qos,QFI=1|policy,2|pcf:2001:2:6|upf:198.18.1.3|upf,v,198.18.1.3,198.18.1.4|ipv4addr,v4,2001|ipv4pool,v4|ipv4range,v4,2001|
ipv4staticaddr,v4,2001|ipv6prefix,v6,2001:10::|ipv6pool,v6,ipv6range,v6,2001:10::|ipv6staticaddr,v6,2001:10::|ifindex,1,0378|ifvalue,01|ifaddr,IPv4,intersat,|ifname,2001:2:6|gtpuer:198.18.1.100|
peerGtpuEpKey:198.18.1.3:198.17.1.6,success,success,PDN Connect
[LTE],S5S8CreateSessReq,Active,init_done|4G SETUP: Idle|4G SETUP: Await UDM Registration|4G
 SETUP: Await UDM Subscription Fetch|4G SETUP: Await UDM Subscribe for Notification|
4G SETUP: Await PCF Create|4G SETUP: Await Address Allocation|4G SETUP: Await PCF Update|4G
 SETUP: Await Charging
Create|finished,3,1313,V2,4,Success,201,3,,3,1316,V2,4,Success,200,3,,3,1319,V2,4,Success,201,3,,3,3329,V2,9,imsi-123456789012345,
imei-123456786666660,msisdn-223310101010101,Success,201,3,||3|1;2;2|3000 mbps|4000 mbps|1000
 mbps|2000 mbps,200000 kbps|400000
kbps,,3,3332,V2,4,Success,204,3,,3,1003,V2,4,Success,201,3,,3,524,V2,4,Success,,3,Request_Accepted,3,2051,V2,18,
imsi-123456789012345,imei-123456786666660,123456789012345,223310101010101,msisdn-223310101010101,Success,,ARC|||||||2;Abf123;;|||1;1|1;0|0|,3,1,intersat,,||5|0;0;15|||,200
 mbps|400 mbps,16,12.0.0.1|2001:db0::b46d:47ff:fe47:4747,2|Abf123||,
WAN,3,1000,V2,40,imsi-123456789012345,imei-123456786666660,123456789012345,223310101010101,msisdn-223310101010101,123|456,Extra|Rgi:123;456;123456|Tai:123;456;1820,2022-08-03
 22:12:19.485844223 +0000 UTC,2022-08-03 22:12:19.772243364
+0000
```

```
UTC,Ue,,198.18.1.100,Success,3,,intershat,WLAN,+00:15+1,3,123|456,10000000,12500000,5,1|1|15,12.0.0.1|2001:db0:b46d:47ff:fe47:4747,46111554,67553994105921,1,5,,2,2|Acf123||,16,1,NR
 Capable UE,1580,198.17.1.6,6168582,198.17.1.3,intershat
```

Procedure-level EDR Generation

The Event Logging feature captures procedure-level information per subscriber. Upon completing a procedure, either successfully or unsuccessfully, the SMF generates event data records capturing the details of procedures and events.

The EDR generation per procedure is configurable. For configuration details, see the Configure EDR Files for Generation, on page 350 section in this guide.

The following table lists the supported procedures and the corresponding IDs.

Table 94: Procedure List

Procedure	Procedure-ID
PDN-SESSION-CREATE or PDU-SESSION-CREATE	3
PDN-SESSION-DELETE or PDU-SESSION-DELETE	4
PDU-SESSION-MODIFY	5
DEDICATEDBEARER	6
HANDOVER	7

Note The procedure IDs remain the same for both roaming and non-roaming procedures.

Further, the SMF captures event-level information per procedure. The following table provides details on the subscriber events and the respective event IDs.

The events captured per procedure are configurable. For configuration details, see the Configure EDR Files for Generation, on page 350 section in this guide.

Table 95: Event IDs

EVENT	EVENT-ID	Applicability of Events to Procedures			
		Create	Release	Modify	Ded Bea
N11SmContext CreateReq	1287	Yes	—	—	—
N11SmContext UpdateReq	1290	Yes	Yes	Yes	—
N11N1N2Message TransferReq	1299	Yes	Yes	Yes	—
N11SmContext UpdateModifyReq	1293	—	—	—	—
N11Ebi AssignmentReq	1302	Yes	—	Yes	—
N11SmContext ReleaseReq	1304	—	Yes	—	—

N11SmContext StatusNotifyReq	1310	Yes	Yes	—	—
N11N1N2Message TransferFail NotificationReq	1339	—	Yes	Yes	—
N4Session ModificationReq	527	Yes	Yes	Yes	Yes
N4Session ReleaseReq	530	Yes	Yes	—	—
N4Session EstablishmentReq	524	Yes	—	—	—
N7SmPolicy CreateReq	3329	Yes	—	—	—
N7SmPolicy DeleteReq	3335	Yes	Yes	—	—
N7SmPolicy UpdateReq	3332	Yes	—	Yes	Yes
N7SmPolicy TerminateNotify Req	3341	—	Yes	—	—
N7SmPolicy UpdateNotifyReq	3338	—	—	Yes	Yes
N10UnsubscribeFor NotificationReq	1432	—	Yes	—	—
N10SubscribeFor NotificationReq	1319	Yes	—	—	—
N10Registration Request	1313	Yes	—	—	—
N10Subscription FetchReq	1316	Yes	—	—	—
N10Deregistration Request	1325	Yes	Yes	—	—
S5S8Delete BearerCmd	2066	—	—	—	Yes
N10Update NotifyReq	1322	—	Yes	Yes	—
N40Charging DataCreateReq	1003	Yes	—	—	—
N40Charging DataUpdateReq	1004	—	—	Yes	—
N40Charging DataReleaseReq	1005	—	Yes	—	
N40Charging NotificationReq	3588	Yes	—	Yes	—
Secondary AuthenReq	2307	Yes	—	—	—
S5S8Create SessReq	2051	Yes	—	—	—
S5S8Delete BearerReq	2057	—	Yes	—	Yes
S5S8Delete SessReq	2055	—	Yes	—	
RadiusCoa DisconnectReq	2313	—	Yes	—	—
RadiusAcctReq	2309	Yes	Yes	Yes	—
metaData	1000	Yes	Yes	Yes	Yes
N16PduSession CreateReq	1444	Yes	—	—	—

N16VsmfPdu SessionRelease Req	1471	Yes	Yes	—	—
N16PduSession HsmfUpdateReq	1447	Yes	Yes	Yes	Yes
N16PduSession HsmfUpdateReq Client	1477	Yes	Yes	Yes	Yes
N16VsmfPdu SessionCreateReq	1468	Yes	—	—	—
N16PduSession VsmfUpdateReq	1451	Yes	Yes	Yes	Yes
N16PduSession NotifyReq	1458	—	Yes	—	—
N11SmContext RetrieveReq	1307	—	Yes	—	—
N16PduSession VsmfUpdateReq Client	1478	Yes	Yes	Yes	Yes
N16PduSession NotifyReqClient	1488	—	Yes	—	—
S5S8Update BearerReq	2062	—	—	—	Yes
S5S8Create BearerReq	2059	—	—	—	Yes
S5S8Bearer ResourceCmd	2061	—	—	—	Yes
S5S8Modify BearerCmd	2064	—	—	—	Yes
N4GtpuRouter AdvertisementReq	542	—	—	—	—
S5S8Modify BearerReq	2053	—	—	—	—
NInternalTxnMsg[1]	1001(xxxx)	Yes	Yes	Yes	Yes
Ntimer NotificationMsg[1]	1002(xxxx)	Yes	Yes	Yes	Yes

[1] - SMF uses several internal messages for handling 3GPP call flows. These internal events are sent and received by SMF and are not 3GPP com
and NTimerNotificationMsg are two generic event IDs defined to represent such internal messages used by SMF. The **xxxx** in the Event ID
message type that is used by SMF internally for easy debuggability.

The SMF uses N40ChargingDataCreateReq, N40ChargingDataUpdateReq, and N40ChargingDataReleaseReq instead of N40ChargingDataR
and release.

The following tables list the detailed event record for the PDU Session Create, Modify, Delete, Handover, and Dedicated Bearer procedures.

Table 96: PDU Session Create Events

tribute	N		Name	Presence	Type	Description
XN EDR fields				M		
ROCEDURE	**E ID**	**EVENT-ID**	VERSION	M		**Event=N11SmContext CreateReq**
			FIELD-COUNT	M		
			SUPI	M		

buten u	N		Name	Presence	Type	Description
			IMEI/PEI	M		
			IMSI	M		
			MSISDN	M		
			GPSI	M		
			STATUS	M		
			STATUS-CODE	O		
			N1-REQ-PDU(PDN)-SESSION-TYPE	O	PduSessionType	
			N1-REQ-SSC-MODE	O		
			CAUSE	O		
			N1-PCO	O	PCO	
			N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION-ESTB-REQUEST
			N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
			N1-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
			N2-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
			N1-REQ-MAX-SUPP-FILTERS	O		
			N1-ALWAYS-ON	O		
			RAT-TYPE	M		
			S-NSSAI-REQUESTED	O	NSSAI	
			GUAMI	O		
			REQUEST-TYPE	O		
			AN-TYPE	O		
			OLD-PDU-SESS-ID	O		
			N1-DNN/APN	O		
			SERVING-NFID	O		
			SERVING-PLMN	O		
			UNAUTH-SUPI	O		
			S-NSSAI-ASSIGNED	O	NSSAI	

Attribute Number	N		Name	Presence	Type	Description
			UP-CONTEXT-STATE	O		
			N1-PDU-SESS-ID	O		
			INDIRECTFWD FLAG	O		
			DIRECTFWD FLAG	O		
			HO-STATE	O		
PROCEDURE ID		**EVENT-ID**	VERSION	M	Client	**Event=N11Sm ContextUpdateReq**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			SUPI	M		
			IMEI	M		
			IMSI	M		
			MSISDN	M		
			PDU(PDN)-SESSION-TYPE	O		
			N1-REQ-MSG-TYPE	O	N1N2MSG REQCONTENT	pdu_session_ modification_request pdu_sess_ modification _command pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification_ complete pdu_session_ release_reject
			N2-REQ-MSG-TYPE	O	N1N2MSG REQCONTENT	

bute u	N		Name	Presence	Type	Description
			N1-RSP-MSG-TYPE	O	N1N2MSG RSPCONTENT	pdu_session_ modification_request pdu_sess_modification _command pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification_ complete pdu_session_ release_reject
			N2-RSP-MSG-TYPE	O	N1N2MSG RSPCONTENT	
			N1-PCO	NA	PCO	
			N1-QOS-RULE	O	QOS-RULE	
			N1-QOS-DESC	O	QOS-DESC	
			CAUSE	O		
			N1-ALWAYS-ON	O		
			5G-SM-CAP	O		
			N1-RSP-MAX-SUPP-FILTERS	O		
			RAT-TYPE	O		
			UP-CONTEXT -STATE	O		
			HO-STATE	O		
			N1-BACKOFF-TIME	NA		
			N1-PDU-SESS-ID	O		
			N1-VGSM-RE -ATTEMPT-IND	NA		
			N1-RE-ATTEMPT -IND	NA		
			N1-SESS-AMBR	O		

Attribute Number			Name	Presence	Type	Description
			N1-CONG-RE-ATTEMPT-IND	O		
			N1-RSP-ALWAYS-ON	—		
PROCEDURE ID		**EVENT-ID**	VERSION	M		**Event=N11N1N2 MessageTransfer Req**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			PDU-SESSION-TYPE	M		
			N1-REQ-MSG-TYPE	O	N1N2MSG REQCONTENT	PDU-SESSION-ESTB-ACCEPT PDU-SESSION-ESTB-REJECT PDU_SESSION_ RELEASE_ COMMAND PDU_SESSION_ MODIFICATION_ COMMAND
			N2-REQ-MSG-TYPE		N1N2MSG REQCONTENT	
			N1-RSP-MSG-TYPE	O	N1N2MSG REQCONTENT	
			N2-RSP-MSG-TYPE		N1N2MSG RSPCONTENT	
			N1-PCO	O	PCO	
			N1-QOS-RULE	O	QOS-RULE	
			N1-QOS-DESC	O	QOS-DESC	
			CAUSE	O		
			N1-ALWAYS-ON	O		
			N1-SESSION-AMBR	O	SESS-AMBR	
			N1-PAA	O	PAA	
			N1-S-NSSAI	O	NSSAI	
			N1-PDU-SESS-ID	O		
			N1-DNN/APN	O		
			N1-BACKOFF-TIME	NA		

buten u	N		Name	Presence	Type	Description
			N1-REQ-SSC-MODE-SELECTED	O		
			N1-REQ-PDU(PDN)-SESSION-TYPE-SELECTED	O		
			N1-SSC-MODE -ALLOWED	O		
			N1-CONG-RE-ATTEMPT-IND	O		
			N1-RE-ATTEMPT -IND	NA		
			N1-RSP-AN-TYPE	NA		
OCEDURE	**E ID**	**EVENT-ID**	VERSION	M		**Event=N7SmPolicy CreateReq**
			FIELD-COUNT	M		
			SUPI	M		
			IMEI/PEI	M		
			GPSI	M		
			STATUS	M		
			STATUS-CODE	O		
			PDU(PDN)-SESSION-TYPE	O		
			QOS-DESC	O	QOS-DESC	
			SESSION-AMBR	O	SESS-AMBR	
			CAUSE	O		

Attribute Number	Name		Name	Presence	Type	Description
PROCEDURE ID		**EVENT-ID**	VERSION	M		**EVENT= N4Session ModificationReq** **N10Deregistration Request** **N7SmPolicy UpdateReq** **N10Subscription FetchReq** **N10Unsubscribe ForNotificationReq** **SecondaryAuthenReq** **N10SubscribeFor NotificationReq** **N40Charging DataCreateReq** **N40Charging DataUpdateReq** **N40Charging DataReleaseReq** **N7SmPolicy DeleteReq** **N11Ebi AssignmentReq** **N4Session EstablishmentReq** **N4Session ReleaseReq** **N10Registration Request** **RadiusAcctReq** **N11SmContext RetrieveReq** **N11SmContext StatusNotifyReq**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			PDU-SESSION -TYPE	M		
			CAUSE	O		
PROCEDURE ID		**EVENT-ID**	VERSION	M		**Event=S5S8Create SessReq**
			FIELD-COUNT	M		
			SUPI	M		
			IMEI/PEI	M		

buten u	N		Name	Presence	Type	Description
			IMSI	M		
			MSISDN	M		
			GPSI	M		
			STATUS	M		
			STATUS-CODE	O		
			PCO	O	PCO	
			PDU-SESSION-TYPE	O		
			SSC-MODE	O		
			DNN/APN	O		
			QOS-RULE	O	QOS-RULE	
			QOS-DESC	O	QOS-DESC	
			SESSION-AMBR	O	SESS-AMBR	
			CAUSE	O		
			PAA	O	PAA	
			S-NSSAI	O	NSSAI	
			RAT-TYPE	M		
			HO-INDICATION			
OCEDURE ID		**EVENT-ID**	VERSION	M		**Event=N16Pdu SessionCreateReq** **N16VsmfPdu SessionCreateReq**
			FIELD-COUNT	M		
			SUPI	O		
			IMEI/PEI	O		
			GPSI	O		
			GUAMI	O	GUAMI	
			REQUEST-TYPE	M	RequestType	
			STATUS	M		
			STATUS-CODE	O		
			PDU/PDN-SESSION-TYPE	O	PduSessionType	
			DNN/APN	M		
			RAT-TYPE	O		

Attribute Number	N		Name	Presence	Type	Description
			S-NSSAI	O	NSSAI	
			SERVING-PLMN	M	PLMN-ID	
			VSMF-ID	M		
			VCNTUNNEL-INFO	M	TUNNEL-INFO	
			HO-PREP-INDICATION	O		
			PGW-S8-CFTEID	O		
			ALWAYS-ON -REQUESTED	O		
			UE-LOCATION	O	UE-LOCATION	
			ROAMING-CHRG-PROF-REQUESTED	O	CHARGING-PROF	
			ALWAYS-ON-GRANTED	O		
			SSC-MODE	O		
			HCNTUNNEL-INFO	M	TUNNEL-INFO	
			SESSION-AMBR	O	SESS-AMBR	
			UE-IPV4-ADDRESS	O		
			UE-IPV6-PREFIX	O		
			QOS-FLOWS-SETUP-LIST	O	QFS	
			ROAMING-CHRG -PROF- SELECTED	O	CHARGING-PROF	
			CAUSE	O		
			N1SM-CAUSE	O		
			UE-IPV6-INTERFACE -ID	O		
			N1-REQ-MSG-TYPE	O		PDU_SESSION_ ESTABLISHMENT _REQ
			N2-REQ-MSG-TYPE	O		
			N1-RSP-MSG-TYPE	O		PDU_SESSION_ ESTABLISHMENT _ACCEPT
			N2-RSP-MSG-TYPE	O		
			N1-PDU-SESS-ID	O		

buten u	N		Name	Presence	Type	Description
			N1-REQ-PDU(PDN)-SESSION-TYPE	O		
			N1-REQ-SSC -MODE	O		
			N1-PCO	O		
			N1-REQ-MAX-SUPP -FILTERS	O		
			N1-ALWAYS-ON	O		
			N1-REQ-PDU(PDN)-SESSION-TYPE-SELECTED	O		
			N1-REQ-SSC-MODE -SELECTED	O		
			N1-QOS-RULES	O		
			N1-QOS-DESC	O		
			N1-SESS-AMBR	O		
			N1-REQ-ALWAYS-ON	O		
			N1-REQ-SSC-MODE -ALLOWED	O		
			N1-CONG-RE-ATTEMPT-IND	O		
			N1-RSP-RE-ATTEMPT-IND	O		
			N1-DNN/APN	O		
OCEDURE	**E ID**	**EVENT-ID**	VERSION	M		**Event= N16VsmfPdu SessionReleaseReq**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			CAUSE	O		
			VGMM-CAUSE	O		
			NGAP-CAUSE	O	NGAP-CAUSE	
OCEDURE	**E ID**	**EVENT-ID**	VERSION	M		**Event= N16PduSession VsmfUpdateReq** **N16PduSession VsmfUpdate ReqClient**

Attribute Number	N		Name	Presence	Type	Description
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			REQUEST-INDICATION	O	N1N2MSG REQCONTENT	
			SESSION-AMBR	O	N1N2MSG REQCONTENT	
			ALWAYS-ON-GRANTED	O	RequestIndication	
			CAUSE	O	SESS-AMBR	
			N1SM-CAUSE	O		
			BACKOFF-TIMER			
			N1-REQ-MSG-TYPE	O		PDU_SESSION_ MODIFICATION _COMMAND PDU_SESSION_ MODIFICATION _COMMAND_REJECT
			N1-RSP-MSG-TYPE			PDU_SESSION_ MODIFICATION _COMMAND PDU_SESSION_ MODIFICATION _COMMAND_REJECT PDU_SESSION_ MODIFICATION _REJECT
			N1-PCO	O		
			N1-QOS-RULE	O		
			N1-QOS-DESC	O		
			N1-PDU-SESS-ID	O		
			N1-ALWAYS-ON	O		
			N1-SESSION-AMBR	O		
PROCEDURE ID		**EVENT-ID**	VERSION	M		**Event=N16Pdu SessionHsmf UpdateReq** **N16PduSessionHsmf UpdateReqClient**
			FIELD-COUNT	M		

buten u	N		Name	Presence	Type	Description
			STATUS	M		
			STATUS-CODE	O		
			IMEI/PEI	O		
			REQUEST-INDICATION	M	RequestIndication	
			VCNTUNNEL-INFO	O	TUNNEL-INFO	
			SERVING-PLMN	O		
			AN-TYPE	O	AccessType	
			RAT-TYPE	O		
			HO-PREP-INDICATION	O		
			CAUSE	O		
			VGMM-CAUSE	O		
			NGAP-CAUSE	O	NGAP-CAUSE	
			ALWAYS-ON	O		
			EPS-IWK	O		
			AN-TYPE-CAN-BE-CHANGED	O		
			UE-LOCATION	O	UE-LOCATION	
			N1-REQ-MSG-TYPE	O		PDU_SESSION_MODIFICATION_REQUEST PDU_SESSION_RELEASE_REQUEST
			N1-RSP-MSG-TYPE	O		
			N1-PDU-SESS-ID	O		
			N1-PCO	O		
			N1-RSP-MAX-SUPP-FILTERS	O		
			N1-REQ-ALWAYS-ON	O		
			N1-QOS-RULES	O		
			N1-QOS-DESC	O		
OCEDURE ID		**EVENT ID=1000**	VERSION	M		**Event=META DATA**
			FIELD-COUNT	M		

Attribute number	N		Name	Presence	Type	Description
			SUPI	M		
			IMEI/PEI	M		
			IMSI	M		
			MSISDN	M		
			GPSI			
			SERVING-PLMN	M		
			UE-LOCATION	M	UE-LOCATION	
			START-TIME	M		
			END-TIME	M		
			TRIGGER-NF	M		
			TRIGGER-EVENT	M		
			SGW-ID	O		
			STATUS	M		
			USERPLANE-STATUS	O	Userplane-status	
			DISCONNECT-REASON	O		
			DNN/APN	M		
			RAT-TYPE	M		
			UE-TIMEZONE	M		
			PDU/PDN-SESSION-TYPE	M		
			UE-PLMN	M		
			SUBSCRIBED-SESS-AMBR-UPLINK	M		
			SUBSCRIBED-SESS-AMBR-DOWNLINK	M		
			SUBSCRIBED-5QI	M		
			SUBSCRIBED-ARP	M		
			PAA	M		
			LOCAL-SEID	M		
			REMOTE-SEID	M		
			ROAMING-STATUS	M		

buten u	N		Name	Presence	Type	Description
			PDU/PDN-SESSION-ID	O		
			ALWAYS-ON	O		
			EPS-IWK	O		
			S-NSSAI	O		
			MAX-SUPP-FILTERS	O		
			SSC-MODE	O		
			UE-TYPE	O		
			LOCAL-CFTEID-TEID	O		
			LOCAL-CFTEID -IP	O		
			REMOTE-CFTEID-TEID	O		
			REMOTE-CFTEID -IP	O		
			VIRTUAL-DNN/APN	O		

Table 97: PDU Session Modify Events

Attribute		Name	Presence	Description
TIME-STAMP	EVENT-ID1=1290	PROCEDURE-ID	M	N11SmContextUpdateReq
EVENT-LIST		VERSION	M	PduSessionModification Request (MESSAGE- 5G-SM-CAP MAX-SUPP-FILTERS PCO ALWAYS-ON QOS-RULE QOS-DESC CAUSE
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		SUPI	M	
		IMEI	M	

Attribute		Name	Presence	Description
		IMSI	M	
		MSISDN	M	
		PDU(PDN)-SESSION -TYPE	O	
		N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT
		N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT
		N1-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT
		N2-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT
		N1-PCO	NA	PCO
		N1-QOS-RULE	O	QOS-RULE
		N1-QOS-DESC	O	QOS-DESC
		CAUSE	O	
		N1-ALWAYS-ON	O	
		5G-SM-CAP	O	
		N1-RSP-MAX-SUPP -FILTERS	O	
		RAT-TYPE	O	
		UP-CONTEXT-STATE	O	
		HO-STATE	O	
		N1-BACKOFF-TIME	NA	
		N1-PDU-SESS-ID	M	
		N1-VGSM-RE- ATTEMPT-IND	NA	
		N1-RE-ATTEMPT-IND	NA	
		N1-SESS-AMBR	O	
		N1-CONG-RE- ATTEMPT-IND	O	
		N1-RSP-ALWAYS-ON	NA	
		DATAFORWARDING	O	
	EVENT-ID	PROCEDURE-ID	M	N10UpdateNotifyReq
		VERSION	M	
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		PDU(PDN)-SESSION -TYPE	M	
		CAUSE	O	

Attribute		Name	Presence	Description
	EVENT-ID4=1299	PROCEDURE-ID	M	N11N1N2Message TransferReq
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		PDU-SESSION-TYPE	M	
		N1MSGREQTYPE	O	N1N2MSGREQ CONTENT
		N2MSGREQTYPE	O	N1N2MSGREQ CONTENT
		N1-PCO	O	PCO
		N1-QOS-RULE	O	QOS-RULE
		N1-QOS-DESC	O	QOS-DESC
		CAUSE	O	
		N1-ALWAYS-ON	O	
		N1-SESSION-AMBR	O	SESS-AMBR
		N1-PAA	O	PAA
		N1-S-NSSAI	O	NSSAI
		N1-PDU-SESS-ID		
		N1-DNN/APN	O	
		N1-BACKOFF-TIME	NA	
		N1-REQ-SSC- MODE-SELECTED	O	
		N1-REQ-PDU(PDN) -SESSION-TYPE -SELECTED	O	
		N1-SSC-MODE-ALLOWED	O	
		N1-CONG-RE- ATTEMPT-IND	O	
		N1-RSP-RE- ATTEMPT-IND	NA	
		N1-RSP-AN-TYPE	NA	
PROCEDURE-ID	**EVENT-ID**	VERSION	M	**Event=N16PduSession HsmfUpdateReq N16PduSessionHsmf UpdateReqClient**
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		IMEI/PEI	O	
		REQUEST-INDICATION	M	RequestIndication

Attribute		Name	Presence	Description
		VCNTUNNEL-INFO	O	TUNNEL-INFO
		SERVING-PLMN	O	
		AN-TYPE	O	AccessType
		RAT-TYPE	O	
		HO-PREP-INDICATION	O	
		CAUSE	O	
		VGMM-CAUSE	O	
		NGAP-CAUSE	O	NGAP-CAUSE
		ALWAYS-ON	O	
		EPS-IWK	O	
		AN-TYPE-CAN-BE -CHANGED	O	
		N1-PDU-SESS-ID	O	
		N1-PCO	O	
		N1-RSP-MAX- SUPP-FILTERS-REQUESTED	O	
		N1-ALWAYS-ON	O	
		N1-QOS-RULES	O	
		N1-QOS-DESC	O	
PROCEDURE-ID	**EVENT-ID**	VERSION	M	**Event= N16PduSession VsmfUpdateReq** **N16PduSessionVsmf UpdateReqClient**
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		REQUEST-INDICATION	O	N1N2MSGREQ CONTENT
		SESSION-AMBR	O	N1N2MSGREQ CONTENT
		ALWAYS-ON-GRANTED	O	RequestIndication
		CAUSE	O	SESS-AMBR
		N1SM-CAUSE	O	
		BACKOFF-TIMER	O	
		N1-REQ-MSG-TYPE	O	PDU_SESSION_ MODIFICATION_ COM PDU_SESSION_ MODIFICATION_ COM

Attribute		Name	Presence	Description
		N1-RSP-MSG-TYPE		PDU_SESSION_ MODIFICATION_ COMMA PDU_SESSION_ MODIFICATION_ COMMA PDU_SESSION_ MODIFICATION_REJECT
		N1-PCO	O	
		N1-QOS-RULE	O	
		N1-QOS-DESC	O	
		N1-PDU-SESS-ID	O	
		N1-ALWAYS-ON	O	
		N1-SESSION-AMBR	O	
	EVENT-ID	PROCEDURE-ID	M	N4Session ModificationReq N40Charging NotificationReq N11N1N2MessageTransfer FailNotificationRe RadiusAcctReq N40ChargingData CreateReq N40ChargingData UpdateReq N40ChargingData ReleaseReq N11EbiAssignmentReq N7SmPolicyUpdate NotifyReq N7SmPolicyUpdateReq
		VERSION	M	
		FIELD-COUNT	M	
		STATUS	M	
		STATUS-CODE	O	
		PDU-SESSION-TYPE	O	
		CAUSE	O	
	EVENT-ID1=1000	PROCEDURE-ID	M	META-DATA
		VERSION	M	
		FIELD-COUNT	M	
		SUPI	M	
		IMEI/PEI	M	
		IMSI	M	
		MSISDN	M	

Attribute		Name	Presence	Description
		GPSI	M	
		SERVING-PLMN	M	
		UE-LOCATION	M	
		START-TIME	M	
		END-TIME	M	
		TRIGGER-NF	M	
		TRIGGER-EVENT	M	
		USERPLANE-STATUS	M	
		SGW-ID	O	
		DISCONNECT-REASON	NA	
		STATUS	M	
		SUBSCRIBED-SESS -AMBR-UPLINK	M	
		SUBSCRIBED-SESS -AMBR-DOWNLINK	M	
		ALWAYS-ON	O	
		MAX-SUPP-FILTERS	O	
		LOCAL-CFTEID-TEID	O	
		LOCAL-CFTEID-IP	O	
		REMOTE-CFTEID-TEID	O	
		REMOTE-CFTEID-IP	O	

Table 98: PDU Session Delete Events

m	u	N	Name	Presence	Type	Description
fields				M		

n u	N	Name	Presence	Type	Description
E ID	**EVENT-ID**	**VERSION**	**M**		**EVENT=N11Sm ContextReleaseReq** **N40ChargingData ReleaseReq** **N7SmPolicy DeleteReq** **N10Unsubscribe ForNotificationReq** **N10Deregistration Request** **N7SmPolicy TerminateNotifyReq** **RadiusCoa DisconnectReq** **RadiusAcctReq** **N7SmPolicy TerminateNotifyReq** **N40Charging NotificationReq** **N10Update NotifyReq** **N11SmContext StatusNotifyReq** **N11N1N2Message TransferFail NotificationReq** **S5S8DeleteSessReq** **N11SmContext RetrieveReq**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		PDU(PDN)-SESSION -TYPE	M		
		CAUSE	O		
E ID	**EVENT-ID**	VERSION	M		**Event=N11SmContext UpdateReq**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		SUPI	M		
		IMEI	M		
		IMSI	M		
		MSISDN	M		
		PDU(PDN)- SESSION-TYPE	O		

m	u	N	Name	Presence	Type	Description
			N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	pdu_session_ modification_request pdu_sess_modification _command pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification _complete pdu_session_ release_reject
			N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
			N1-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	pdu_session_ modification_request pdu_sess_modification _command pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification_complete pdu_session_ release_reject
			N2-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
			N1-PCO	NA	PCO	
			N1-QOS-RULE	O	QOS-RULE	
			N1-QOS-DESC	O	QOS-DESC	
			CAUSE	O		
			N1-ALWAYS-ON	O		
			5G-SM-CAP	O		
			N1-RSP-MAX-SUPP-FILTERS	O		
			RAT-TYPE	O		
			UP-CONTEXT-STATE	O		
			HO-STATE	O		
			N1-BACKOFF-TIME	NA		
			N1-PDU-SESS-ID	O		

n	u	N	Name	Presence	Type	Description
			N1-VGSM-RE-ATTEMPT-IND	NA		
			N1-RE-ATTEMPT -IND	NA		
			N1-SESS-AMBR	O		
			N1-CONG-RE-ATTEMPT-IND	O		
			N1-RSP-ALWAYS -ON	NA		
			DATAFORWARDING	O		
E ID	**EV**	**ENT-ID**	VERSION	**M**		**Event=N11N1N2 MessageTransfer Req**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			PDU-SESSION-TYPE	M		
			N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION- ESTB-ACCEPT PDU-SESSION- ESTB-REJECT PDU_SESSION_ RELEASE_ COMMAND PDU_SESSION_ MODIFICATION_ COMMAND
			N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
			N1-RSP-MSG-TYPE		N1N2MSGREQ CONTENT	
			N2-RSP-MSG-TYPE		N1N2MSGREQ CONTENT	
			N1-PCO	O	PCO	
			N1-QOS-RULE	O	QOS-RULE	
			N1-QOS-DESC	O	QOS-DESC	
			CAUSE	O		
			N1-ALWAYS-ON	O		
			N1-SESSION-AMBR	O	SESS-AMBR	
			N1-PAA	O	PAA	
			N1-S-NSSAI	O	NSSAI	
			N1-PDU-SESS-ID			
			N1-DNN/APN	O		
			N1-BACKOFF-TIME	NA		

m	u	N	Name	Presence	Type	Description
			N1-REQ-SSC-MODE-SELECTED	O		
			N1-REQ-PDU(PDN)-SESSION-TYPE -SELECTED	O		
			N1-SSC-MODE- ALLOWED	O		
			N1-CONG-RE-ATTEMPT-IND	O		
			N1-RE-ATTEMPT -IND	NA		
			N1-RSP-AN-TYPE	NA		
URE ID	**EVE**	**ENT-ID**	VERSION	M		**Event=N16Pdu SessionHsmf UpdateReq** **N16PduSessionHsmf UpdateReqClient**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			IMEI/PEI	O		
			REQUEST- INDICATION	M	RequestIndication	
			VCNTUNNEL-INFO	O	TUNNEL-INFO	
			SERVING-PLMN	O		
			AN-TYPE	O	AccessType	
			RAT-TYPE	O		
			HO-PREP- INDICATION	O		
			CAUSE	O		
			VGMM-CAUSE	O		
			NGAP-CAUSE	O	NGAP-CAUSE	
			ALWAYS-ON	O		
			EPS-IWK	O		
			AN-TYPE-CAN-BE-CHANGED	O		
			N1-PDU-SESS-ID	O		
			N1-PCO	O		
			N1-RSP-MAX-SUPP-FILTERS	O		
			N1-ALWAYS-ON	O		

n	u	N	Name	Presence	Type	Description
			N1-QOS-RULES	O		
			N1-QOS-DESC	O		
E ID		**EVENT-ID**	VERSION	M		**Event= N16PduSession VsmfUpdateReq** **N16PduSessionVsmf UpdateReqClient**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			REQUEST- INDICATION	O	N1N2MSGREQ CONTENT	
			SESSION-AMBR	O	N1N2MSGREQ CONTENT	
			ALWAYS-ON- GRANTED	O	RequestIndication	
			CAUSE	O	SESS-AMBR	
			N1SM-CAUSE	O		
			BACKOFF-TIMER	O		
			N1-REQ-MSG-TYPE	O		PDU_SESSION_ MODIFICATION _COMMAND PDU_SESSION_ MODIFICATION_ COMMAND_REJECT
			N1-RSP-MSG-TYPE	O		PDU_SESSION_ MODIFICATION _COMMAND PDU_SESSION_ MODIFICATION_ COMMAND_REJECT PDU_SESSION_ MODIFICATION _REJECT
			N1-PCO	O		
			N1-QOS-RULE	O		
			N1-QOS-DESC	O		
			N1-PDU-SESS-ID	O		
			N1-ALWAYS-ON	O		
			N1-SESSION-AMBR	O		
E ID		**EVENT-ID**	VERSION	M		**Event= N16Vsmf PduSession ReleaseReq**
			FIELD-COUNT	M		
			STATUS	O		
			STATUS-CODE	O		
			CAUSE	O		

m	u	N	Name	Presence	Type	Description
			VGMM-CAUSE	O		
			NGAP-CAUSE	O		
URE ID	**EVE**	**ENT-ID**	VERSION	M		**Event=N16Pdu SessionNotify ReqClient N16PduSession NotifyReq**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			RESOURCE-STATUS	O	Resourcestatus	
			CAUSE	O		
URE ID	**EVE**	**ENT-ID**	VERSION	M		**Event=S5S8Delete BearerReq**
			FIELD-COUNT	M		
			STATUS	M		
			STATUS-CODE	O		
			LBI-REQUESTED	O		
			EBIS	O		
			FAILED-BEARER -CTX	O	BEARER-CTX	
			CAUSE-REQUESTED	O		
			PCO	O		
			CAUSE-RESPONDED	O		
			LBI-RESPONDED	O		
			UE-LOCAL-IP	O		
			UE-UDP-PORT	O		
			BEARER-CTX	O		
URE ID	**EVE**	**NT-ID=1000**	VERSION	M		**Event= META-DATA**
			FIELD-COUNT	M		
			SUPI	M		
			IMEI/PEI	M		
			IMSI	M		
			MSISDN	M		
			GPSI			
			SERVING-PLMN	M		
			UE-LOCATION	M		

n	u	N	Name	Presence	Type	Description
			START-TIME	M		
			END-TIME	M		
			TRIGGER-NF	M		
			TRIGGER-EVENT	M		
			SGW-ID	O		
			STATUS	M		
			USERPLANE -STATUS	M		
			DISCONNECT -REASON	O		
			STATUS	M		
			UPDATE-TIME	—		

Table 99: Dedicated Bearer Events

Attribute		Name	Presence	Type	Description
TXN EDR fields			M		
PROCEDURE ID	**EVENT-ID**	**VERSION**	**M**		**Event=N7SmPolicy UpdateNotif** **N7SmPolicy UpdateReq** **N4Session ModificationReq** **N10UpdateNotify Req**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		PDU-SESSION -TYPE	O		
		CAUSE	O		
PROCEDURE ID	**EVENT-ID**	VERSION	**M**		**Event=S5S8Delete BearerCmd**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		BEARER-CTX-REQUESTED	O	BEARER-CTX	
		CAUSE	O		
		BEARER-CTX-RESPONDED	O	BEARER-CTX	
		RECOVERY	O		

Attribute		Name	Presence	Type	Description
PROCEDURE ID	**EVENT-ID**	VERSION	**M**		**Event= S5S8Bearer Resource**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		LBI-REQUESTED	O		
		RAT-TYPE	O		
		SERVING-PLMN	O		
		EBI	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Modify BearerCr**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		APN-AMBR	O		
		BEARER-CTX	O	BEARER-CTX	
		CAUSE	O		
		RECOVERY	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Update BearerRe**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		AMBR	O		
		BEARER-CTX	O	BEARER-CTX	
		CAUSE	O		
		RECOVERY	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Create BearerRe**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		LINKED-BEARER -ID	O		
		PCO	O		
		BEARER-CTX	O	BEARER-CTX	
		CAUSE	O		

Attribute		Name	Presence	Type	Description
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Delete BearerReq**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		LBI-REQUESTED	O		
		EBIS	O		
		FAILED-BEARER -CTX	O	BEARER-CTX	
		CAUSE- REQUESTED	O		
		PCO	O		
		CAUSE- RESPONDED	O		
		LBI-RESPONDED	O		
		UE-LOCAL-IP	O		
		UE-UDP-PORT	O		
		BEARER-CTX	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=Metadata**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		SUPI	M		
		IMEI/PEI	O		
		IMSI	M		
		MSISDN	O		
		GPSI	O		
		SERVING-PLMN	O		
		UE-LOCATION	O		
		START-TIME	O		
		END-TIME	O		
		TRIGGER-NF	O		
		TRIGGER-EVENT	O		
		SGW-ID	O		
		STATUS	O		

Attribute		Name	Presence	Type	Description
		SUBSCRIBED-SESS -AMBR-UPLINK	O		
		SUBSCRIBED-SESS -AMBR-DOWNLINK	O		
		LOCAL-CFTEID -TEID	O		
		LOCAL-CFTEID -IP	O		
		REMOTE-CFTEID -TEID	O		
		REMOTE-CFTEID -IP	O		

Table 100: Handover Events

Attribute		Name	Presence	Type	Description
TXN EDR fields			M		
PROCEDURE-ID	**EVENT-ID**	**VERSION**	**M**		**N4Session ModificationReq** **N40ChargingData ReleaseRe** **N40ChargingData UpdateRe** **N40ChargingData CreateReq** **RadiusAcctReq** **N4GtpuRouter Advertisemen** **N7SmPolicy UpdateReq** **N7SmPolicyUpdate NotifyRe** **N11SmContext RetrieveReq** **S5S8Delete SessReq** **N11EbiAssignment Req** **N11SmContextStatus NotifyR**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		PDU(PDN)-SESSION -TYPE	M		
		CAUSE	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=N11SmContext Updat**
		FIELD-COUNT	M		
		STATUS	M		

Attribute		Name	Presence	Type	Description
		STATUS-CODE	O		
		SUPI	M		
		IMEI/PEI	M		
		IMSI	M		
		MSISDN	M		
		PDU(PDN)-SESSION -TYPE	O		
		N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	pdu_session_ modification_reques pdu_sess_ modification _comman pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification _compl pdu_session_ release_reject
		N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
		N1-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	pdu_session_ modification_reques pdu_sess_modification _command pdu_session_ release_req pdu_session_ release_command pdu_session_ release_complete pdu_session_ modification_reject pdu_session_ modification _compl pdu_session_ release_reject
		N2-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
		N1-PCO	NA	PCO	
		N1-QOS-RULE	O	QOS-RULE	
		N1-QOS-DESC	O	QOS-DESC	
		CAUSE	O		
		N1-ALWAYS-ON	O		
		5G-SM-CAP	O		

Attribute		Name	Presence	Type	Description
		N1-RSP-MAX-SUPP-FILTERS	O		
		RAT-TYPE	O		
		UP-CONTEXT -STATE	O		
		HO-STATE	O	Hostate	
		N1-BACKOFF-TIME	NA		
		N1-PDU-SESS-ID	O		
		N1-VGSM-RE-ATTEMPT-IND	NA		
		N1-RE-ATTEMPT -IND	NA		
		N1-SESS-AMBR	O		
		N1-CONG-RE-ATTEMPT -IND	O		
		N1-RSP-ALWAYS-ON	NA		
		DATAFORWARDING	O		
PROCEDURE ID	**EVENT-ID**	**VERSION**	**M**		**Event=N11N1N2 MessageTra**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		PDU-SESSION-TYPE	M		
		N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION- ESTB-ACCE PDU-SESSION- ESTB-REJEC PDU_SESSION_ RELEASE_ PDU_SESSION_ MODIFICAT _COMMAND
		N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
		N1-RSP-MSG-TYPE	O	N1N2MSGREQ CONTENT	
		N2-RSP-MSG-TYPE	O	N1N2MSGREQ CONTENT	
		N1-PCO	O	PCO	
		N1-QOS-RULE	O	QOS-RULE	
		N1-QOS-DESC	O	QOS-DESC	

Attribute		Name	Presence	Type	Description
		CAUSE	O		
		N1-ALWAYS-ON	O		
		N1-SESSION-AMBR	O	SESS-AMBR	
		N1-PAA	O	PAA	
		N1-S-NSSAI	O	NSSAI	
		N1-PDU-SESS-ID	O		
		N1-DNN/APN	O		
		N1-BACKOFF-TIME	NA		
		N1-REQ-SSC-MODE -SELECTED	O		
		N1-REQ-PDU(PDN) -SESSION-TYPE -SELECTED	O		
		N1-SSC-MODE -ALLOWED	O		
		N1-CONG-RE-ATTEMPT-IND	O		
		N1-RE-ATTEMPT -IND	NA		
		N1-RSP-AN-TYPE	NA		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Create SessReq**
		FIELD-COUNT	M		
		SUPI	M		
		IMEI/PEI	M		
		IMSI	M		
		MSISDN	M		
		GPSI	M		
		STATUS	M		
		STATUS-CODE	O		
		PCO	O	PCO	
		PDU-SESSION-TYPE	O		
		SSC-MODE	O		
		DNN/APN	O		
		QOS-RULE	O	QOS-RULE	
		QOS-DESC	O	QOS-DESC	

Attribute		Name	Presence	Type	Description
		SESSION-AMBR	O	SESS-AMBR	
		CAUSE	O		
		PAA	O	PAA	
		S-NSSAI	O	NSSAI	
		RAT-TYPE	M		
		HO-INDICATION	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Update BearerRe**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		AMBR	O		
		BEARER-CTX	O	BEARER-CTX	
		CAUSE	O		
		RECOVERY	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Create BearerRe**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		LINKED-BEARER -ID	O		
		PCO	O		
		BEARER-CTX	O	BEARER-CTX	
		CAUSE	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Delete BearerRe**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		LBI-REQUESTED	O		
		EBIS	O		
		FAILED-BEARER -CTX	O	BEARER-CTX	
		CAUSE-REQUESTED	O		
		PCO	O		
		CAUSE-RESPONDED	O		

Attribute		Name	Presence	Type	Description
		LBI-RESPONDED	O		
		UE-LOCAL-IP	O		
		UE-UDP-PORT	O		
		BEARER-CTX	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Delete BearerCmd**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		BEARER-CTX-REQUESTED	O	BEARER-CTX	
		CAUSE	O		
		BEARER-CTX-RESPONDED	O	BEARER-CTX	
		RECOVERY	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=S5S8Modify BearerReq**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		MEI	O		
		SERVING-PLMN	O		
		RAT-TYPE	O		
		FQ_TEID	O		
		AMBR- REQUESTED	O		
		MME-S4SGSN-ID	O		
		M-MBR	O		
		UE-LOCAL-ADDR	O		
		HENB-LOCAL -ADDR	O		
		UE-UDP-PORT	O		
		CAUSE	O		
		RECOVERY	O		
		LINKED-EBI	O		
		MSISDN	O		

Attribute		Name	Presence	Type	Description
		AMBR-RESP	O		
		APN-RESTRICT	O		
		BEARER-CTX-RESPONDED	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=N16Pdu SessionHsmf** **N16PduSession HsmfUpdate**
		FIELD-COUNT	M		
		STATUS	M		
		STATUS-CODE	O		
		IMEI/PEI	O		
		REQUEST-INDICATION	M	RequestIndication	
		VCNTUNNEL-INFO	O	TUNNEL-INFO	
		SERVING-PLMN	O		
		AN-TYPE	O	AccessType	
		RAT-TYPE	O		
		HO-PREP-INDICATION	O		
		CAUSE	O		
		VGMM-CAUSE	O		
		NGAP-CAUSE	O	NGAP-CAUSE	
		ALWAYS-ON	O		
		EPS-IWK	O		
		AN-TYPE-CAN-BE-CHANGED	O		
		UE-LOCATION	O	UE-LOCATION	
		N1-REQ-MSG-TYPE	O		PDU_SESSION_ MODIFICAT PDU_SESSION_ RELEASE_
		N1-RSP-MSG-TYPE	O		
		N1-PDU-SESS-ID	O		
		N1-PCO	O		
		N1-RSP-MAX-SUPP-FILTERS	O		
		N1-REQ-ALWAYS-ON	O		

Attribute		Name	Presence	Type	Description
		N1-QOS-RULES	O		
		N1-QOS-DESC	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=N16Pdu SessionCreateRe** **N16VsmfPdu SessionCreateReq**
		FIELD-COUNT	M		
		SUPI	O		
		IMEI/PEI	O		
		GPSI	O		
		GUAMI	O	GUAMI	
		REQUEST-TYPE	M	RequestType	
		STATUS	M		
		STATUS-CODE	O		
		PDU/PDN-SESSION -TYPE	O	PduSessionType	
		DNN/APN	M		
		RAT-TYPE	O		
		S-NSSAI	O	NSSAI	
		SERVING-PLMN	M	PLMN-ID	
		VSMF-ID	M		
		VCNTUNNEL-INFO	M	TUNNEL-INFO	
		HO-PREP-INDICATION	O		
		PGW-S8-CFTEID	O		
		ALWAYS-ON-REQUESTED	O		
		UE-LOCATION	O	UE-LOCATION	
		ROAMING-CHRG-PROF-REQUESTED	O	CHARGING-PROF	
		ALWAYS-ON-GRANTED	O		
		SSC-MODE	O		
		HCNTUNNEL-INFO	M	TUNNEL-INFO	
		SESSION-AMBR	O	SESS-AMBR	
		UE-IPV4-ADDRESS	O		

Attribute		Name	Presence	Type	Description
		UE-IPV6-PREFIX	O		
		QOS-FLOWS-SETUP-LIST	O	QFS	
		ROAMING-CHRG-PROF-SELECTED	O	CHARGING- PROF	
		CAUSE	O		
		N1SM-CAUSE	O		
		UE-IPV6-INTERFACE-ID	O		
		N1-REQ-MSG-TYPE	O		PDU_SESSION_ ESTABLISH
		N2-REQ-MSG-TYPE	O		
		N1-RSP-MSG-TYPE	O		PDU_SESSION_ ESTABLISHM
		N2-RSP-MSG-TYPE	O		
		N1-PDU-SESS-ID	O		
		N1-REQ-PDU(PDN) -SESSION-TYPE	O		
		N1-REQ-SSC-MODE	O		
		N1-PCO	O		
		N1-REQ-MAX-SUPP-FILTERS	O		
		N1-ALWAYS-ON	O		
		N1-REQ-PDU(PDN)-SESSION-TYPE -SELECTED	O		
		N1-REQ-SSC-MODE -SELECTED	O		
		N1-QOS-RULES	O		
		N1-QOS-DESC	O		
		N1-SESS-AMBR	O		
		N1-REQ-ALWAYS -ON	O		
		N1-REQ-SSC-MODE -ALLOWED	O		
		N1-CONG-RE-ATTEMPT-IND	O		
		N1-RSP-RE-ATTEMPT-IND	O		

Attribute		Name	Presence	Type	Description
		N1-DNN/APN	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=N11SmContext CreateRe**
		FIELD-COUNT	M		
		SUPI	M		
		IMEI/PEI	M		
		IMSI	M		
		MSISDN	M		
		GPSI	M		
		STATUS	M		
		STATUS-CODE	O		
		N1-REQ-PDU(PDN) -SESSION-TYPE	O	PduSessionType	
		N1-REQ-SSC-MODE	O		
		CAUSE	O		
		N1-PCO	O	PCO	
		N1-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION -ESTB-REQUEST
		N2-REQ-MSG-TYPE	O	N1N2MSGREQ CONTENT	
		N1-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
		N2-RSP-MSG-TYPE	O	N1N2MSGRSP CONTENT	
		N1-REQ-MAX-SUPP-FILTERS	O		
		N1-ALWAYS-ON	O		
		RAT-TYPE	M		
		S-NSSAI- REQUESTED	O	NSSAI	
		GUAMI	O		
		REQUEST-TYPE	O		
		AN-TYPE	O		
		OLD-PDU-SESS-ID	O		
		N1-DNN/APN	O		
		SERVING-NFID	O		

Attribute		Name	Presence	Type	Description
		SERVING-PLMN	O		
		UNAUTH-SUPI	O		
		S-NSSAI- ASSIGNED	O	NSSAI	
		UP-CONTEXT -STATE	O		
		N1-PDU-SESS -ID	O		
		INDIRECTFWDFLAG	O		
		DIRECTFWDFLAG	O		
		HO-STATE	O		
PROCEDURE ID	**EVENT-ID**	VERSION	M		**Event=Metadata**
		FIELD-COUNT	M		
		SUPI	M		
		IMEI/PEI	O		
		IMSI	M		
		MSISDN	O		
		GPSI	O		
		SERVING-PLMN	O		
		UE-LOCATION	O		
		START-TIME	O		
		END-TIME	O		
		TRIGGER-NF	O		
		TRIGGER-EVENT	O		
		SGW-ID	O		
		STATUS	O		
		RAT-TYPE	O		
		UE-TIMEZONE	O		
		SESS-AMBR- UPLINK	O		
		SESS-AMBR-DOWNLINK	O		
		LINKED-EBI	O		
		USERPLANE- STATUS	O		
		LOCAL-CFTEID -TEID	O		
		LOCAL-CFTEID -IP	O		

Attribute		Name	Presence	Type	Description
		REMOTE-CFTEID -TEID	O		
		REMOTE-CFTEID -IP	O		
		DISCONNECT -REASON	O		

NOTES:

- subscribed-sess-ambr-uplink and subscribed-sess-ambr-downlink: These fields are captured in the metadata event for some of the procedures. The values for these fields are printed as saved in pducontext. Bitrates in the metadata event are without any unit such as bps, kbps, or mbps. The default bitrate is read as bits per second (bps).
- Status: In event METADATA (id = 1000), this field indicates the status of the procedure. For other events, it indicates the type of received response message or intended outgoing response type. The status can be one of the following:
  - Success
  - Failed
  - PartialFailure
  - NoRspValidation: This status is used in case the request is sent in **ASYNC (fire and forget)** mode and the response is neither expected nor processed in SMF.
- Status-code: This field indicates HTTP status-code of the response message. This field should be empty for outgoing response messages as smf-service is unaware of the actual status-code filled by rest-ep. In such cases, the status field indicates the response type that SMF intended to send, such as success or failure response.
- Userplane-status is of type number. The number can be one of the following:
  - UpStateNone = 0
  - UpStateEstablishing = 1 // UPF Session is being established or setup
  - UpStateActivating = 2 // UPF Session is being modified to Activate Access Tunnel
  - UpStateActivated = 3 // UPF Session Active for Access & Core Tunnel
  - UpStateDeactivating = 4 // UPF Session is being modified to Deactivate Access Tunnel
  - UpStateDeactivated = 5 // UPF Session Deactivated for Access, valid Core Tunnel Only
  - UpStateModifying = 6 // UPF Session is being modified for QoS or flow parameters
  - UpStateDeleting = 7 // UPF Session is being Released
  - UpStateDeleted = 8 // UPF Session is Released
- PduSessionType is of type number. The number can be one of the following:
  - UnknownSessionType or Invalid = 0

- Ipv4PduSession = 1
- Ipv6PduSession = 2
- Ipv4V6PduSession = 3
- Unstrutured = 4
- Ethernet = 5
- FutureUsePduSessionType = 7

- SSC mode is of type number. The number can be one of the following:
  - UnknownSscMode = 0
  - SscMode1 = 1
  - SscMode2 = 2
  - SscMode3 = 3
  - DupSscMode1 = 4
  - DupSscMode2 = 5
  - DupSscMode3 = 6
  - FutureUseSscMode = 7

- Eps Iwk (Type: Number)
  - EpsInterworkingIndication_DummyEnum = 0
  - EpsInterworkingIndication_NONE = 1
  - EpsInterworkingIndication_WITH_N26 = 2
  - EpsInterworkingIndication_WITHOUT_N26 = 3

- Roaming status (Type: Number)
  - ROAMING_STATUS_NONE = 0
  - ROAMING_STATUS_HOMER =1 *//HOMER*
  - ROAMING_STATUS_VISITOR_LBO =2 *//LBO*
  - ROAMING_STATUS_VISITOR_HR = 3 *//IN-HR*
  - ROAMING_STATUS_ROMER = 4 *//OUT-HR*

- PreemptionCapability (type: Number)

  5G:
  - 0: "PreemptionCapability_DummyEnum"
  - 1: "NOT_PREEMPT"
  - 2: "MAY_PREEMPT"

4G and Wi-Fi:

- 0: Disabled
- 1: Enabled

- PreemptionVulnerability (type: Number)

5G:

- 0: "PreemptionVulnerability_DummyEnum"
- 1: "NOT_PREEMPTABLE"
- 2: "PREEMPTABLE"

4G and Wi-Fi:

- 0: Disabled
- 1: Enabled

- Disconnect-Reason (type: String)

  Disconnect-Reason contains a self-explanatory string. If it holds a number, then the string interpretation is as follows:

  - PduRelReason_Error = 1
  - PduRelReason_SessIdleTimeout = 2
  - PduRelReason_SessCpIdleTimeout = 3
  - PduRelReason_SessAbsoluteTimeout = 4

- RequestType (type: Number)
  - RequestType_DummyEnum = 0
  - INITIAL_REQUEST = 1
  - EXISTING_PDU_SESSION = 2
  - INITIAL_EMERGENCY_REQUEST = 3
  - EXISTING_EMERGENCY_PDU_SESSION = 4

- RequestIndication (type: Number)
  - RequestIndication_DummyEnum = 0
  - UE_REQ_PDU_SES_MOD = 1
  - UE_REQ_PDU_SES_REL = 2
  - PDU_SES_MOB = 3
  - NW_REQ_PDU_SES_AUTH = 4
  - NW_REQ_PDU_SES_MOD = 5

- NW_REQ_PDU_SES_REL = 6
- EBI_ASSIGNMENT_REQ = 7

- AccessType (type: Number)
  - AccessType_DummyEnum = 0
  - AccessType_3GPP_ACCESS = 1
  - AccessType_NON_3GPP_ACCESS AccessType = 2

- PartialRecordMethod (type: Number)
  - PartialRecordMethod_DummyEnum = 0
  - DEFAULT = 1
  - INDIVIDUAL = 2

- TriggerCategory (type : Number)
  - TriggerCategory_DummyEnum = 0
  - IMMEDIATE_REPORT = 1
  - DEFERRED_REPORT = 2

- TriggerType (type: Number)
  - TriggerType_DummyEnum = 0
  - QUOTA_THRESHOLD = 1
  - QHT = 2
  - FINAL = 3
  - QUOTA_EXHAUSTED = 4
  - VALIDITY_TIME = 5
  - OTHER_QUOTA_TYPE = 6
  - FORCED_REAUTHORISATION = 7
  - UNUSED_QUOTA_TIMER = 8
  - UNIT_COUNT_INACTIVITY_TIMER = 9
  - ABNORMAL_RELEASE = 10
  - QOS_CHANGE = 11
  - VOLUME_LIMIT = 12
  - TIME_LIMIT = 13
  - PLMN_CHANGE = 14
  - USER_LOCATION_CHANGE = 15

- RAT_CHANGE = 16
- UE_TIMEZONE_CHANGE = 17
- TARIFF_TIME_CHANGE = 18
- MAX_NUMBER_OF_CHANGES_IN_CHARGING_CONDITIONS = 19
- MANAGEMENT_INTERVENTION = 20
- CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA = 21
- CHANGE_OF_3GPP_PS_DATA_OFF_STATUS = 22
- SERVING_NODE_CHANGE = 23
- REMOVAL_OF_UPF = 24
- ADDITION_OF_UPF = 25
- START_OF_SERVICE_DATA_FLOW = 26
- AMBR_CHANGE = 27

- Resourcestatus (type: Number)
  - DummyEnum = 0
  - RELEASED = 1

- HoState (type: Number)
  - DummyEnum = 0
  - NONE = 1
  - PREPARING = 2
  - PREPARED = 3
  - COMPLETED = 4
  - CANCELLED = 5

For details on the listed attributes, see the tables in the EDR Attributes, on page 340 section.

Procedure EDR Example:

V1,15,28514,10:36.1,97,imsi-310310120106401,1287,N11SmContextCreateReq,imsi-310310120106401:5,,roaming-status:home|ue-type:nr-capable|supi:imsi-310310120106401
|gpsi:msisdn-12000006001|pei:imeisv-1031014232100100|psid:5|snssai:001|dnn:fast.t-mobile.com|emergency:false|rat:nr|access:3gpp
access|connectivity:5g|udm-uecm:10.178.118.192
|udm-sdm:10.178.118.192|auth-status:unauthenticated,success,success,PDU Session
Establishment,N11SmContextCreateReq,Active,init_done|SETUP: Idle|SETUP: Await UDM
Registration|
SETUP: Await UDM Subscription
Fetch|finished,3,1287,V2,33,imsi-310310120106401,imeisv-1031014232100100,3.1031E+14,12000006001,msisdn-12000006001,Success,,2,1,,,193|,,,,,,,NR,
1|||,0100BC|310|310,1,1,,fast.t-mobile.com,3a4528c-851d-4728-856c-1b186ec992e5,310|310,0,,,5,0,0,3,1313,V2,4,Success,201,2,,3,1316,V2,4,Success,200,2,,3,1319,V2,4,Success,201,
2,,,,,,,,,,,,,,,,,,,,,,,,,,,,
V1,15,28528,12:11.5,96,imsi-310310120106401,1304,N11SmContextReleaseReq,imsi-310310120106401:5,imsi-310310120106401:fast.t-mobile.com,snssai:001|emergency:false|peerGtpuEPKey:
10.193.123.12:172.18.90.205|namespace:smf,success,success,PDU Session Release - AMF
initiated,N11SmContextReleaseReq,Active,init_done|RELEASE: Idle|RELEASE: Await UPF Release|
prepone_response|prepone_response|RELEASE: Await Charging Terminate|RELEASE: Await PCF

```
Delete|RELEASE: Await UDM Unsubscribe to
notify|finished,4,530,V2,4,Success,,2,Request_Accepted,
4,1304,V2,4,Success,,2,,4,3335,V2,4,Success,204,2,,4,1325,V2,4,Success,204,2,,4,1000,V2,15,imsi-310310120106401,imeisv-1031014232100100,3.1031E+14,1200000600l,msisdn-1200000600l,310|
310,NR|Ncgi:310;310;0147AD5C2|Tai:310;310;025289,2022-09-01 20:12:11.545199056 +0000
UTC,2022-09-01 20:12:11.631685285 +0000 UTC,amf,1304,,Success,8,disc_pdurel_amf_init_release,,
```

In the preceding example, the initial entries represent the transaction EDRs and last part provided here represents the procedure-level EDRs.

EDR Transaction Collision

This EDR file dumps the transaction collision information whenever the collision occurs. It is useful to debug collision scenarios.

Note The transaction collision EDRs support only up to a maximum of 10 subscribers and not all subscribers unlike the transaction EDRs. The transaction collision EDRs do not support configuration of EDR generation rate, CPU threshold, session limiting, and procedure or event information.

Table 101: EDR Transaction Collision File Fields

Field Number	Field Name	Field Description
1	Subscriber ID	The subscriber ID. For example, imsi-123456789012345
2	Collision Time	Collision time in yyyy/MM/dd HH:mm:ss.SSS format.
3	Force Resolution	Indicates whether the resolution is forced (true/false).
4	Collision Cause	The cause of collision.
5	New Transactions Before Collision	Transactions in the new state before collision handling separated by |.
6	Pending Transactions Before Collision	Transactions in the pending state before collision handling separated by |.
7	Active Transactions Before Collision	Transactions in the active state before collision handling separated by |.
8	Suspended Transactions Before Collision	Transactions in the suspended state before collision handling separated by |.
9	New Transactions After Collision	Transactions in the new state after collision handling separated by |.
10	Pending Transactions After Collision	Transactions in the pending state after collision handling separated by |.

Field Number	Field Name	Field Description
11	Active Transactions After Collision	Transactions in the active state after collision handling separated by |.
12	Suspended Transactions After Collision	Transactions in the suspended state after collision handling separated by |.
13	Aborted Transactions After Collision	Transactions in the aborted state after collision handling separated by |.

CSV Format Examples:

```
supi:imsi-123456789012345,2020/10/06 16:15:11.801,true,SessionLockSamePriority,17,,,,,,|17,,
supi:imsi-123456789012345,2020/10/06 16:15:11.824,true,SessionLockSamePriority,18,,,,,,|18,,
supi:imsi-123456789012345,2020/10/06 16:15:11.857,true,SessionLockSamePriority,19,,,,,,|19,,
supi:imsi-123456789012345,2020/10/06 16:15:11.883,true,SessionLockSamePriority,20,,,,,,|20,,
supi:imsi-123456789012345,2020/10/06 16:15:11.888,true,SessionLockRelease,,,,,,,,x
```

EDR Attributes

This section provides details of the EDR attributes and its sub attributes.

Table 102: QOS-RULE

QOS-RULE-LIST	qr-id|qr-opcode|qr-dqr|qr-qfi|qr-prededence|num-filters| **filters:**flter-id;flter-dir;cmp-type-match-a cmp-type-proto;proto-id;cmp-type-local-addr;local-ip; local-port;cmp-type-remote-addr;;remote-ip;cmp-type-remote-port; remote-port;cmp-type-tos;tos-trffic-class			
	Field	**Sub field**	**Sub-sub field**	**Presence**
	QOS-RULE			
		QOS-RULE-ID		M
		QOS-RULE-OPCODE		M
		QOS-RULE-DQR		M
		QOS-RULE-QFI		M
		QOS-RULE-PRECEDENCE		M
		NO-PKT-FILTERS		
		PKT-FILTER-LIST		O
			PKT-FILTER-ID	M
			PKT-FILTER-DIRECTION	M
			CMP-TYPE-MATCH-ALL	O

			CMP-TYPE-PROTO	O
			PROTO-ID	O
			CMP-TYPE-LOCAL -ADDRESS	O
			LOCAL-IP-ADDRESS	O
			LOCAL-CMP-TYPE-PORT	O
			LOCAL-PORT	O
			CMP-TYPE-REMOTE-ADDRESS	O
			REMOTE-IP-ADDRESS	O
			CMP-TYPE-REMOTE-PORT	O
			REMOTE-PORT	O
			CMP-TYPE-TOS	O
			TOS-TRAFFIC-CLASS	O

Note Delimiters subject to change based on the position of QOS-RULE in the attribute.

Table 103: QOS-DESC

QOS-DESC	[qfi|opcode|5qi|arp|mbr-ul|mbr-dl|gbr-ul|gbr-dl]	
Sub field	**Type**	**Presence**
QFI		M
Opcode		M
5QI		O
ARP	ARP	O
MBR-UPLINK		O
MBR-DOWNLINK		O
GBR-UPLINK		O
GBR-DOWNLINK		O

Note Delimiters subject to change based on the position of QOS-DESC in the attribute.

Table 104: PCO

PCO	[type|PCSCF-ADDR-LIST|DNS-ADDR-LIST| pdu-session-id|QOS-RULE-LIST|SESSION-AMBR| QOS-DESC|S-NSSAI|ms-support-nw_addr-tft|nw-support-nw_addr-tft| PCSCF-ADDR-REQ|DNS-ADDR-REQ|mtu-req|mtu-size]		
Sub field	**Type**	**Presence**	
TYPE	String	M	EPCO or PCO or APCO
PCSCF-ADDR-LIST	PCSCF-ADDR	O	From CSR Response being sent from SMF
DNS-ADDR-LIST	DNS-ADDR	O	From CSR Response being sent from SMF
PDU-SESSION-ID		O	From CSR Response being sent from SMF
QOS-RULE-LIST	QOS-RULE	O	From CSR Response being sent from SMF
SESSION-AMBR	SESS-AMBR	O	From CSR Response being sent from SMF
QOS-DESC	QOS-DESC	O	From CSR Response being sent from SMF
S-NSSAI	NSSAI	O	From CSR Response being sent from SMF
MS-SUPPORT-NW_ADDR-TFT	Boolean	O	From CSR Request being received
NW-SUPPORT-NW_ADDR-TFT	Boolean	O	From CSR Response being sent from SMF
PCSCF-ADDR-REQ	PCSCF-ADDR-REQ	O	From CSR Request being received
DNS-ADDR-REQ	DNS-ADDR-REQ	O	From CSR Request being received
IPV4-MTU-REQUEST	Boolean	O	From CSR Request being received
IPV4-MTU-SIZE	String	O	From CSR Response being sent from SMF

Note In the preceding table, CSR Request and CSR Response messages refer to 4G and Wi-Fi call flows. N11 SM Context Create Request and Response messages refer to 5G call flows.

Table 105: PCSCF-ADDR-REQ

PCSCF-ADDR-REQ	[pco-pcsf-addr-ipv4-req;pco-pcsf-addr-ipv6-req]	
Sub field	**Presence**	**Type**
PCO-PCSF-ADDR-IPV4-REQ	M	Boolean
PCO-PCSF-ADDR-IPV6-REQ	M	Boolean

Table 106: PCSCF-ADDR

PCSCF-ADDR	[ipv4-primary;ipv4-secondary;ipv4-tertiary;ipv6-primary;ipv6-secondary;ipv6-tertiary]	
Sub field	**Presence**	**Type**
PCSF-ADDR-IPV4-LIST	O	List
PCSF-ADDR-IPV6-LIST	O	List

Table 107: DNS-ADDR

DNS-ADDR	[ipv4-primary;ipv4-secondary;ipv4-tertiary;ipv6-primary;ipv6-secondary;ipv6-tertiary]	
Sub field	**Presence**	**Type**
DNS-ADDR-IPV4-LIST	O	List
DNS-ADDR-IPV6-LIST	O	List

Table 108: DNS-ADDR-REQ

DNS-ADDR-REQ	[pco-pcsf-addr-ipv4-req;pco-pcsf-addr-ipv6-req]	
Sub field	**Presence**	**Type**
PCO-PCSF-ADDR-IPV4-REQ	M	Boolean
PCO-PCSF-ADDR-IPV6-REQ	M	Boolean

Table 109: NSSAI

NSSAI	[sst|sd|hplmnsst|hplmnsd]	
Sub field	**Presence**	**Type**
SST	M	Number

SD	O	String
HPLMN-SST	O	Number
HPLMN-SD	O	String

Note Delimiters subject to change based on the position of S-NSSAI in the attribute.

Table 110: PAA

PAA	[ipv4-addr|ipv6-addr]	
Sub field	**Presence**	**Type**
IPV4-ADDR	O	String
IPV6-ADDR	O	String

Table 111: N1N2MSGREQCONTENT or N1N2MSGRSPCONTENT

N1N2MSGREQCONTENT / N1N2MSGRSPCONTENT	[msg-type|cause]	
Sub field	**Presence**	**Type**
MSG-TYPE	M	SMF N1N2MsgType
Cause	O	String

Example: 195|REQUEST_REJECTED_UNSPECIFIED

Table 112: PLMN-ID

PLMN-ID	[mcc|mnc]
Sub field	**Presence**
MCC	M
MNC	M

Note Delimiters subject to change based on the position of PLMN-ID in the parent attribute.

Table 113: GUAMI

GUAMI	[amf-id|plmn-id]	
Sub field	**Presence**	**Type**

AMF-ID	M	String
PLMN-ID	M	PLMN-ID

Table 114: SESS-AMBR

SESS-AMBR	[ambr-dl|ambr-ul]	
Sub field	**Presence**	**Type**
AMBR-DL	O	String
AMBR-UL	O	String

Table 115: UE-LOCATION

UE-LOCATION	[locationType|**Ecgi:** ECGI|**Tai:**TAI] or [locationType|**Ncgi:** NCGI|**Tai:**TAI]		
Sub field	**Presence**	**Type**	—
locationType	M	String	"E
ECGI or NCGI	O	ECGI/NCGI	—
Tai	O	TAI	—

Table 116: ECGI or NCGI

ECGI / NCGI	[plmn-id;cellId]	
Sub field	**Presence**	**Type**
Plmn-id	M	PLMN-ID
Cell-id	M	String

Table 117: TAI

TAI	[plmn-id;tac]	
Sub field	**Presence**	**Type**
Plmn-id	M	PLMN-ID
Tac	M	String

Table 118: ARP

ARP	[preEmpCap;preEmpVul;priority]	
PRE-EMP-CAP	M	PreemptionCapability

PRE-EMP-VUL	M	PreemptionVulnerability
PRIORITY	M	Number

Note Delimiters subject to change based on the position of ARP in the attribute.

Table 119: NGAP-CAUSE

NGAP-CAUSE	[group|value]	
GROUP	O	Number
VALUE	O	Number

Table 120: TUNNEL-INFO

TUNNEL-INFO	[gtp-teid|ipv4-addr|ipv6-addr]	
GTP-TEID	O	String
IPV4-ADDR	O	String
IPV6-ADDR		String

Table 121: QFS

QFS	[qos-rule|qos-desc]	
Qos-rules	O	QOS-RULE
Qos-desc	O	QOS-DESC

Table 122: CHARGING-PROF

CHARGING-PROF	partial-rec-method|category:max-cc:time-limit;type:vol-limit			
	PARTIAL-REC-METHOD			PartialRecordMethod
	TRIGGERS-LIST	TRIGGERS	CATEGORY	TriggerCategory
			MAX-CCC	
			TIME-LIMIT	
			TYPE	TriggerType
			VOL-LIMIT	

Table 123: BEARER-CTX

BEARER-CTX	[ebi|pkt-flow-id|cause|pco|tft|fqteid|qos-desc|charging-id]

Sub field	Presence	Type
EBI/LBI	M	
PKT-FLOW-ID	O	
CAUSE	O	
PCO	O	PCO
TFT	O	
FQTEID	O	
QOS-DESC	O	QOS-DESC
CHARGING-ID	O	

The SMF generates detailed records with field-level details per event. The following table lists the different N1N2 messages and the associated IDs.

Table 124: SMF N1N2 Message Types

MESSAGE	MESSAGE-ID
PDU-SESSION-ESTB-REQUEST	193
PDU-SESSION-ESTB-ACCEPT	194
PDU-SESSION-ESTB-REJECT	195
PDU-SESSION-MOD-REQ	201
PDU-SESSION-MOD-CMD	203
PDU-SESSION-MOD-CMD-REJ	202
PDU-SESSION-MOD-CMD-COMP	204
PDU-SESSION-REL-REQ	209
PDU-SESSION-REL-CMD	211
PDU-SESSION-REL-REJ	210
PDU-SESSION-REL-COMP	212
N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND	76
N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE	130
N2_PDU_SESSION_RESOURCE_SETUP_REQUEST	77
N2_PDU_SESSION_RESOURCE_SETUP_RESPONSE_TRANSFER	78
N2_PDU_SESSION_RESOURCE_MODIFY_CONFIRM_TRANSFER	62
N2_PDU_SESSION_RESOURCE_MODIFY_INDICATION_TRANSFER	63
N2_PDU_SESSION_RESOURCE_MODIFY_REQUEST_TRANSFER	64
N2_PDU_SESSION_RESOURCE_MODIFY_RESPONSE_TRANSFER	65

N2_PDU_SESSION_RESOURCE_MODIFY_UNSUCCESS_TRANSFER	79
N2_PDU_SESSION_HANDOVER_PREP_UNSUCCESS_TRANSFER	93
N2_PDU_SESSION_HANDOVER_COMMAND_TRANSFER	91
N2_PDU_SESSION_PATH_SWITCH_REQUEST_ACK_TRANSFER	84
N2_PDU_SESSION_PATH_SWITCH_REQUEST_ UNSUCCESS_TRANSFER	97
N2_PDU_SESSION_PATH_SWITCH_REQUEST_TRANSFER	82
N2_PDU_SESSION_HANDOVER_REQUIRED_TRANSFER	85
N2_PDU_SESSION_HANDOVER_REQUEST_ACK_TRANSFER	87
N2_PDU_SESSION_HANDOVER_RESOURCE_ ALLOC_UNSUCCESS_TRANSFER	89
N2_PDU_SESSION_PATH_SWITCH_REQUEST_ SETUP_FAILED_TRANSFER	95
N2_PDU_SESSION_RESOURCE_SETUP_UNSUCCESS_TRANSFER	99
N2_PDU_SESSION_RESOURCE_NOTIFY_TRANSFER	101
N2_PDU_SESSION_SECONDARY_RAT_USAGE_TRANSFER	103
N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER	105
N2_PDU_SESSION_RESOURCE_SETUP_FAIL_TRANSFER	107
N2_PDU_SESSION_PATH_SWITCH_SETUP_FAIL_TRANSFER	109
N2_PDU_SESSION_HANDOVER_RESPONSE_ ALLOC_FAIL_TRANSFER	111

Limitations

The EDR Logging feature has the following limitations:

- Event record generation does not work for the following scenarios:
  - All handover (HO) procedures except Xn HO, N2 HO, 5G to 4G HO, 4G to 5G HO, 5G to Wi-Fi HO, and Wi-Fi to 5G HO
  - Idle-Active transition
  - Active-Idle transition
  - 4G PDN modification
- The SMF supports only IMSI (SUPI)-based EDR reporting.
- The SMF currently supports EDR generation in CSV format. The EDR file storage format is not configurable.
- This feature is not applicable to a procedure that does not send a response explicitly to an incoming request.

Configuring EDRs

This section describes how to configure the EDR Logging feature.

Configure EDR Reporting

Note EDR generation occurs after you configure the subscriber ID. Then, you can enable EDR reporting for a specific subscriber or for all the subscribers. If you have enabled the EDR reporting for all the subscribers, then the SMF ignores the individual subscriber ID configuration.

Note To optimize the performance, it is recommended to enable EDR reporting only for a subset of subscribers with specific procedure ID.

To enable or disable the EDR generation for subscribers, use the following sample configuration:

```
config
    edr reporting { enable [ all subscribers | file [ transaction |
transaction-collision ] ] | disable file [ transaction |
transaction-collision ] }
    edr all subscribers
    end
```

NOTES:

- **edr reporting { enable [all subscribers | file [transaction | transaction-collision]] | disable file [transaction | transaction-collision] }**—Specify this keyword to configure the EDR reporting on SMF. Use the **edr reporting enable** command to enable the EDR reporting functionality. Use the **edr reporting disable***file* command to disable the EDR reporting functionality for a specific file. By default, the EDR reporting is disabled.
- Use the **edr reporting enable all subscribers** command or **edr all subscribers** to enable the EDR for all the subscribers.

Note

- To enable EDR reporting for a subscriber, use the **edr subscribers** *subscriber_id* command. *subscriber_id* must be an alphanumeric string. The default value is empty. Ensure to specify the exact subscriber key in this command. The SMF supports only IMSI (SUPI)-based EDR reporting.
- Configure a minimum of one subscriber upon enabling the EDR reporting.
- You can configure a maximum of 10 subscribers for generation of transaction collision EDRs.

Configure EDR Files for Generation

Use the following sample configuration to generate the EDR events at transaction level.

```
config
   edr file { transaction | transaction-collision }
      procedure-id procedure_value
         event-id event_value
            field-id field_value
            end
```

- **edr file { transaction | transaction-collision }**: Specify to generate EDR files with transaction or transaction-collision level details for subscriber sessions.
- **procedure-id** *procedure_value*: Specify the procedure ID or procedure name for which the event reporting must be enabled.
- **event-id** *event_value*: Specify the event ID or event name for which the event reporting must be enabled.
- **field-id** *field_value*: Specify the field ID or field name for which the event reporting must be enabled.
- All procedure IDs, event IDs, and field IDs registered by application, are enabled by default.
- If one or more procedures are enabled, then all the other procedures will be disabled and will not be populated in the transaction EDR. Similarly, if one or more events are enabled under a procedure, all other events under that procedure will be disabled and will not be populated in the transaction EDR.
- If a procedure-id is disabled, no event start, add field, or event-end will be honored for the procedure-id.
- If an event-id is disabled within a procedure id, then event-start, event-end, or add field will not be honored for the procedure-id and event-id combination.
- If a field-id is disabled for an event-id, then add-field will not be honored, and a blank entry will be present instead of value in CSV entry.

Example Configuration:

```
edr file transaction
  procedure-id 24 32
  procedure-id 25
    event-id 5 7 8
    event-id 5
      field-id 10 12 14
```

In the preceding example, **event-id 5 7 8** means enable the event-id 5, 7, and 8 for procedure-id 25. The **field-id 10 12 14** means enable the field-id 10, 12, and 14 for procedure-id 25 and event-id 5.

Configure EDR Parameters

To define the EDR parameters, use the following sample configuration:

```
config
   edr file transaction
      flush interval file_flush_interval
      limit [ size file_size | count file_count| storage edr_storage_size ]
      procedure procedure_value event event_value field field_value
      rate rate_value
```

```
reporting [ disable | enable ]
threshold [ cpu cpu_threshold | session session_thresold  ]
end
```

NOTES:

- **flush interval** *file_flush_interval*—Specify the time interval, in milliseconds, to flush the EDR files. The default value is 1000 ms.
- **limit [size** *file_size* **| count** *file_count*| **storage** *edr_storage_size***]**—Specify the file-related limits.
  - Use the **limit size** *file_size* command to specify the maximum size of an EDR file, after which the EDR file is compressed and new CSV file is created. The default file size is 100 MB.

    The *file_size* must be an integer in the range of 1 to 2048.

Note The system periodically monitors the size of an EDR file once per second or after the configured flush interval, whichever value is higher. After the EDR file reaches its maximum size, it's compressed and new CSV file is created. However, in some scenarios, the data is being continuously written to the EDR file just before the system performs a periodic check based on the previously mentioned threshold limits. This results in an EDR file that might slightly exceed the configured maximum file size.

  - Use the **limit count** *file_count* command to specify the maximum number of EDR files to be preserved. The default file count is 10.

    The *file_count* must be an integer in the range of 2 to 128.

    When the configured file count is reached, the file is moved to persistent volume and then deleted.
  - Use the **limit storage** *edr_storage_size* command to specify the EDR storage size of persistent volume in GiB.

    The *edr_storage_size* must be an integer in the range of 0 to 64. Set the value to 0 to disable persistent volume in edr-monitor pod. The default storage size is 24 GiB.

Important The storage limit can be changed only in “system mode shutdown” mode. Hence, disabling of persistent volume can be done only when the system is in shutdown state.

- **procedure** *procedure_value* **event** *event_value* **field** *field_value*—Specify the transaction-level procedure ID configuration information. The *procedure_value* must be a procedure ID or a procedure name. The *event_value* must be an event ID or an event name along with a field value.

Note

- By default, all the procedure IDs, event IDs, and field IDs, which are registered during the application-start, are enabled.
- If one or more procedures are enabled, then all other procedures are disabled and are not populated in the transaction EDR.
- If one or more events are enabled in a procedure, then all other events in that procedure are disabled and are not populated in the transaction EDR.
- If one or more fields are enabled in an event, then all other fields in that event are disabled and are not populated in the transaction EDR.
- For the disabled procedure IDs, no event-start, add field, or event-end are honored.
- For the disabled event IDs in a procedure ID, no event-start, event-end, or add field are honored for the procedure ID and event ID combination.
- For a disabled field ID within an event ID, no add-field is honored, and a blank entry is available instead of value in CSV entry.

- **rate** *rate_value* —Specify the allowed rate per second to generate EDR records. The default rate is 4096.

  rate_value must be an integer in the range of 32 to 65535.

  When the EDR generation rate limit is reached, transaction EDRs are dropped and a metric is added to track EDR generated, dropped, drop reason, and so on. Note that the rate limiting is performed per service (smf-service) pod instance.

- **reporting [disable | enable]**—Specify the file for which you have to enable or disable reporting.

Important The edr-monitor pods are spawned only when the transaction edr is enabled.

- **threshold [cpu** *cpu_threshold* **| session** *session_thresold* **]**—Specify the threshold to limit the EDR generation.
  - Use the **threshold cpu** *cpu_threshold* command to configure the CPU threshold in percentage. If the threshold is breached for a SMF service pod instance, then the application stops generating EDRs. The *cpu_threshold* must be an integer in the range of 1 to 100, with default value of 80%.
  - Use the **threshold session** *session_thresold* command to configure session threshold per GR instance. If the threshold is breached for a GR instance, then the application stops generating EDRs. The *session_thresold* must be an integer in the range of 0 to 1,000,000, with default value of 100,000.

Note If the rack is running with active-active mode, the session threshold is applied individually for both the GR instances.

Verifying EDR Transactions

Use the following show commands to display the currently registered procedures, events, and fields for the application along with their respective IDs.

show edr transaction-procedure *procedure_id* **event** *event_id*

show edr event *event_id*

You can provide all the procedures and events. Otherwise, you can provide a particular procedure name and event name or procedure-id and event-id.

Note The show command output is based on the mapping registered by the application.

The following is an example of the show command output.

```
Procedure-id 20, Procedure-Name: xyz
    Event-id 1, Event-Name: abc
         1 - Field1-Name
         2 - Field2-Name
         …
         …
         …
     Event-id 2, Event-Name: efgh
          1 - Field1-Name
          2 - Field2-Name
          …
          …
          …
    …
    …
    …
Procedure-id 21, Procedure-Name: bbbb
     Event-id 1, Event-Name: cccc
          1 - Field1-Name
          2 - Field2-Name
          …
          …
          …
     Event-id 2, Event-Name: dddd
          1 - Field1-Name
          2 - Field2-Name
          …
          …
          …
```

This output helps the operator to know current CSV format of a particular procedure-id and event-id pair.

OAM Support for EDR Logging

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

Bulk Statistics for EDR Transactions and EDR Reporting

The SMF maintains the following bulk statistics as part of this feature.

- edr_error_total

  Labels:

  - error_code – The EDR writing error code

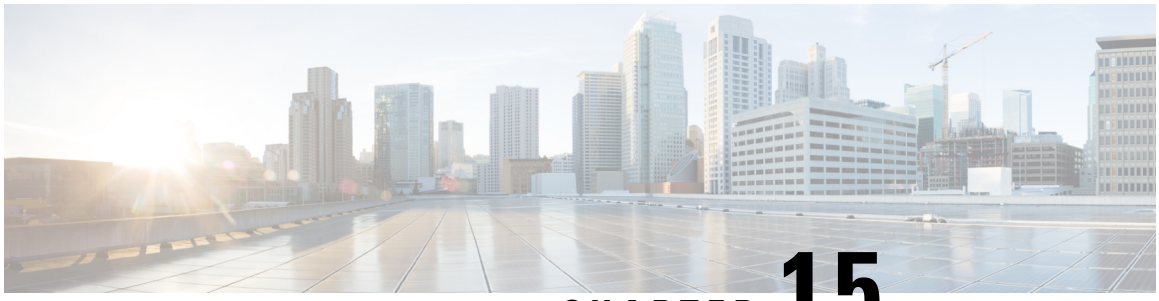
This metric is pegged whenever an error occurs during EDR writing. This metric displays "EdrQueueFull" as the error_code when the writing queue is full and the EDR is dropped.

Following metric is used to monitor the EDR count and status.

- edr_total

  Labels:

  - name – Name of the transaction EDR.
  - status – Status of the EDR transaction if it is successful or has any errors.
  - status_code – The following status codes are supported:
    - EdrReportingDisabled
    - EdrTxnReportingDisabled
    - EdrSessThreshold
    - EdrCpuThreshold
    - EdrRateLimitExceeded
    - EdrFileWriteFailed
    - EdrInvalidEdrId
    - EdrQueueFull
    - EdrIgnored_NoEventRecorded



CHAPTER 15

Failure Handling Support

- Feature Summary and Revision History, on page 355
- Feature Description, on page 356
- Access and Mobility Management Function Failure Handling, on page 356
- Charging Function Failure Handling, on page 359
- Network Repository Function Failure Handling, on page 369
- Policy Control Function Failure Handling, on page 382
- Unified Data Management Failure Handling, on page 387
- User Plane Function Failure Handling, on page 393

Feature Summary and Revision History

Summary Data

Table 125: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 126: Revision History

Revision Details	Release
Enhanced the existing failure handling configuration of N4SessionModificationReq message to support cause codes 0-255.	2021.02.3

Revision Details	Release
Enhanced the existing failure handling configuration of N4SessionModificationReq message to include conditions to control the session termination based on predefined procedures.	2021.02.3
Added retransmission support for the following request messages: • Namf_Communication EBI Assignment Request • Namf_Communication N1 N2 Message Transfer Request	2021.02.2
Added permissible range values for **response-timeout** command in the PCF and UDM configuration	2021.02.0
RAT type FHT support and graceful timeout handling and its related statistics introduced.	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The system performs error handling by segregating error codes into recoverable and non-recoverable error codes. It attempts to recover the endpoints with continuous retries when SMF receives recoverable errors from the NRF server for messages, such as NF Registration, NF Update, NF Heart Beat, and so on. This feature provides a flexible way for handling errors during the NRF interactions with SMF and other network functions, such as Charging Function (CHF), Network Repository Function (NRF), Policy Control Function (PCF), Unified Data Management (UDM), and User Plane Function (UPF).

This feature supports the following functionality:

- Configurable retry actions for specific error codes, which occur during the NRF interactions with other NFs.
- Flexibility to decide on a retry action for an error code after retrying all the endpoints in an NRF.
- CLI configuration under the **profile nf-client-failure** template to configure the error codes and the corresponding retry actions for NRF messages. You can also configure a failover option for an error code after retrying all the endpoints in an NRF.
- Provides HTTPv2 status code range support in the failure handling templates of other NFs.

Access and Mobility Management Function Failure Handling

Feature Description

The SMF supports failure handling of the Access and Mobility Management Function (AMF). Based on the request messages, SMF supports retransmission to the same endpoint.

How it Works

SMF provides retransmission support for the following request messages:

- Namf_Communication EBI Assignment Request
- Namf_Communication N1 N2 Message Transfer Request

When SMF doesn't receive a response for the preceding messages, SMF retransmits the message to the same endpoint. SMF starts the internally configured timer after sending these messages to the AMF. The timer stops after SMF receives a response from the AMF. In case the timer expires while waiting for a response, SMF uses the retry mechanism for which you have configured the number of retry attempts.

Configuring Retransmission for Request Messages

To configure retransmission for the Namf_Communication EBI Assignment and Namf_Communication EBI Assignment messages, use the following sample configuration:

```
config
  profile nf-client-failure nf-type amf
    profile failure-handling failure_handling_name
    service name type namf-comm
      message type { AmfCommEBIAssignment | AmfCommN1N2MessageTransfer
| AmfCommSMStatusChangeNotify }
       status-code httpv2 status_code
       retransmit retransmit_value
       retransmit interval retransmit_interval_value
       retry retry_value
       action retry-and-continue
    exit
  exit
```

NOTES:

- **service name type namf-comm**: Specify the AMF service name type as namf-comm.
- **message type { AmfCommEBIAssignment | AmfCommN1N2MessageTransfer | AmfCommSMStatusChangeNotify }**: Specify the message type of the namf-comm AMF service name type as **AmfCommEBIAssignment**, **AmfCommN1N2MessageTransfer**, or **AmfCommSMStatusChangeNotify**.
- **status-code httpv2** *status_code* : Specify the status code of the service. The *status_code* must be an integer in the range of 0–599.
- **retransmit** *retransmit_value*: Specify the maximum retransmission value for the same endpoint. The *retransmit_value* must be an integer in the range of 1–10.

  If SMF sends message and receive an error in the HTTP status code and if you have configured a valid retransmit count, then that number of retransmission attempts are made to the same endpoint. The maximum retransmit count is used from the first-time configuration of the HTTP status code.

  If SMF receives failure error HTTP code even after retransmission, then SMF retransmits to the same endpoint in the following conditions:

  - If valid retransmit counts are configured for the first HTTP status code that SMF received.

  - If a valid retransmit count, which must not be zero, exists for the received HTTP error code.

- **retransmit interval** *retransmit_interval_value*: Specify the retransmission interval value in milliseconds. The default value is 1000.

  If you have configured the retransmit interval, then SMF waits for the timeout between retransmissions.

- **retry** *retry_value*: Specify the number of retry attempts to the different available endpoints. The *retry_value* must be an integer in the range of 1–10.

- **action retry-and-continue**: Specify the retry as per the configured retry count and continue the session.

Configuration Example

The following is an example configuration of the retransmission for the Namf_Communication EBI Assignment message:

```
config
  profile nf-client-failure nf-type amf
    profile failure-handling FHAMF
    service name type namf-comm
      message type AmfCommEBIAssignment
      status-code httpv2 504
      retransmit 1
      retransmit interval 1000
      retry 1
      action retry-and-continue
    exit
  exit
```

Charging Function Failure Handling

Feature Description

Table 127: Feature History

Feature Name	Release Information	Description
CHF Failure Handling at Rating Group and Application level	2024.01	SMF allows you to define configurable actions to handle the failures associated with the application errors and rating group IDs. This feature introduces new command **failure-handling error-type [rg | app]** in the charging profile configuration. For more information, see the profile charging failure-handling error-type command. **Default Setting**: Disabled - Configuration Required

The SMF supports failure handling of the Charging Function (CHF) server. In the event of the failure of an online CHF server, the SMF relays the charging information to the offline CHF server.

For a seamless transfer of charging information, the SMF invokes the configurations associated with the CHF failure handling profile. If you have configured failure handling, the SMF continues the session with the selected CHF configured in another profile.

SMF supports failure handling of the Charging Function (CHF) server at the following levels.

- HTTP-level status code
- Application-level error code
- Rating group-level result code

You can configure the following actions for application errors.

- Drop data—Drop data corresponding to the Charging ID.
- Terminate—Release the PDU session.
- Continue—Disable charging.

You can configure the following actions for Rating Group errors.

- Convert-offline—Convert to offline charging.
- Delete flow—Delete the flow or rule associated with the rating group.

- Drop data—Drop the data corresponding to the rating group.
- Terminate—Release the PDU session.

Without the configuration, SMF continues with the default behaviour. See Table 5 and Table 6 for the default behavior.

For information on how to select the charging server, see the CHF Selection, on page 1435 section in the Subscriber Charging, on page 1427 chapter of this guide.

How it Works

This section describes how the offline failover support for charging feature works.

Handling a CHF Server Failure

The CHF server failure occurs when the selected CHF sends failure response or sends no response. For a CHF server failure, the NF library sends status code that is based on the failure template. This template is associated with the CHF network profile. The smf-service sends the profile information to smf-rest-ep while sending the IPC message.

The failure template is configured with the list of HTTP error codes and the associated failure actions and retry count, as required. This feature supports the failure actions:

- Retry and Continue—For this failure action, NF library attempts until the configured number of times before fallback. After the configured number of times complete, the NF library falls back to the lower priority CHF server IP address. If a failure or no response is received from the CHF server, the "continue" action is returned to the smf-service.
- Terminate—For this failure action, NF library does not attempt to send a message to other CHF servers. The library sends a reply to smf-service with the action as "terminate". For the "terminate" failure action, the smf-service deletes the session.
- Continue—For this failure action, the smf-service continues the session and sends the charging message to the offline CHF server. This server is configured as part of the local static CHF profile that is meant for offline purposes. In addition, the failure handling profile for offline CHF is configured.

Note For the "continue" failure action, you can configure the offline CHF server at SMF in a separate profile. SMF will use this profile after the CHF server failure. If the offline CHF server is not confgured, the session is continued without imposing any charging.

Relaying to an Offline CHF Server

After CHF server failure, when the SMF continues, it converts the ongoing charging services as follows:

- Converts the services with both online and offline charging method to the offline charging method.
- Converts the services with online charging method to the offline charging method.
- No change for the services with the offline charging method.

HTTP Cause Code Mapping with Failure Actions

The following table lists the mapping of failure actions with the associated HTTP cause code. Based on the network requirements, you can change the mapping.

Table 128: HTTP Cause Code Mapping with Failure Actions

Http-2 Cause Codes and Description		Converged CHF Failure Action			Offline CHF Failure Actions		
Code	Description	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
400	Bad Request	Terminate	No config	No config	Terminate	No config	No config
403	Forbidden	Terminate	No config	No config	Terminate	No config	No config
404	Not found	Terminate	No config	No config	Terminate	No config	No config
405	Method Not allowed	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	No config	No config
408	Request Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
500	Internal Server Error	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
503	Service Unavailable	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
508	Gateway Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
0	No reply from server	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue

Application Error Code-based Failure Handling

The following table lists the application error result codes with the associated SMF failure handling action.

Table 129: Application Error Result Code Mapping with the SMF Failure Handling Action

Application Error Result Code	SMF Failure Handling Action
CHARGING_NOT_APPLICABLE	Terminate Session
END_USER REQUEST_DENIED	Terminate Session
QUOTA_LIMIT_REACHED	Drop traffic for the session
END_USER_REQUEST_REJECTED	Terminate Session

Rating Group-level Failure Handling

The following table lists the Rating Group-level error result codes with the associated SMF failure handling action.

Table 130: Rating Group-level Error Result Code Mapping with the SMF Failure Handling Action

Rating Group-level Error Result Code	SMF Failure Handling Action
RATING_FAILED	Drop traffic corresponding to the Rating Group
QUOTA_MANAGEMENT_NOT_APPLICABLE	Convert to offline
USER_UNKNOWN	Ignored **Note** SMF supports this action only at the session level.
END_USER_SERVICE_DENIED	Drop traffic corresponding to the Rating Group
QUOTA_LIMIT_REACHED	Drop traffic corresponding to the Rating Group
END_USER_SERVICE_REJECTED	Drop traffic corresponding to the Rating Group

Call Flows

This section describes the call flows that are associated with CHF failure handling.

5G Delete Flow Action Call Flow

This section describes the 5G delete flow action call flow.

Figure 78: 5G Delete Flow Action Call Flow

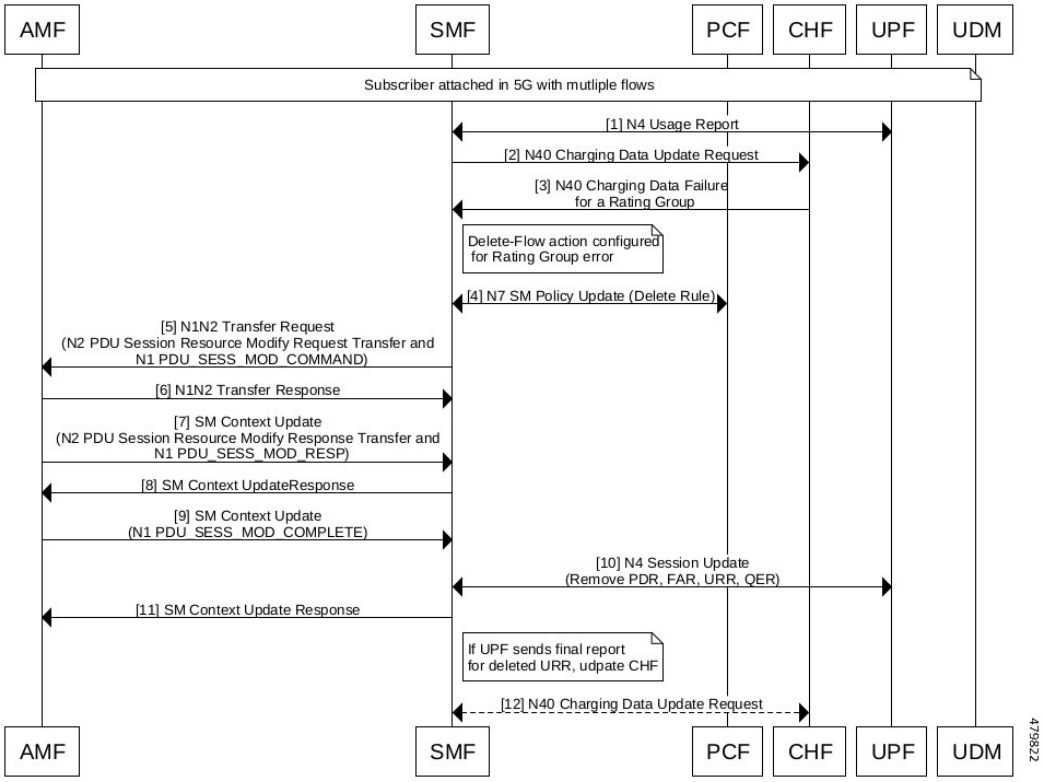


Table 131: 5G Delete Flow Action Call Flow Description

Step	Description
1	A subscriber is attached in 5G with multiple flows. UPF sends the N4 usage report to SMF.
2	SMF sends the N40 Charging Data Update Request to CHF.
3	CHF sends the N40 Charging data failure for a Rating Group to SMF. **Note** Configure the delete flow action for the Rating Group error. This action is used for deletion of the flow or rule associated with the Rating Group.
4	SMF sends the N7 SM Policy Update for deletion of a rule to PCF.
5	SMF sends the N1N2 Transfer Request to AMF. This request includes the N2 PDU Session Resource Modify Request Transfer and the N1 PDU Session Modification message.
6	AMF sends the N1N2 Transfer Response to SMF.
7	AMF sends the SM Context Update to SMF. This update message includes the N2 PDU Session Resource Modify Response Transfer and the N1 PDU Session Modify Response.
8	SMF sends the SM Context Update Response to AMF.

Step	Description
9	AMF sends the SM Context Update to SMF. This update includes the details on the completion of the N1 PDU session modification.
10	SMF sends the N4 Session Update to UPF. This update includes the details on the PDR, FAR, URR, and QER to be removed.
11	SMF sends the SM Context Update Response to AMF. **Note** If the UPF sends the final report for the deleted URR, then SMF sends this update to CHF.
12	SMF sends the N40 Charging Data Update Request to CHF.

4G Delete Flow Action Call Flow

This section describes the 4G delete flow action call flow.

Figure 79: 4G Delete Flow Action Call Flow

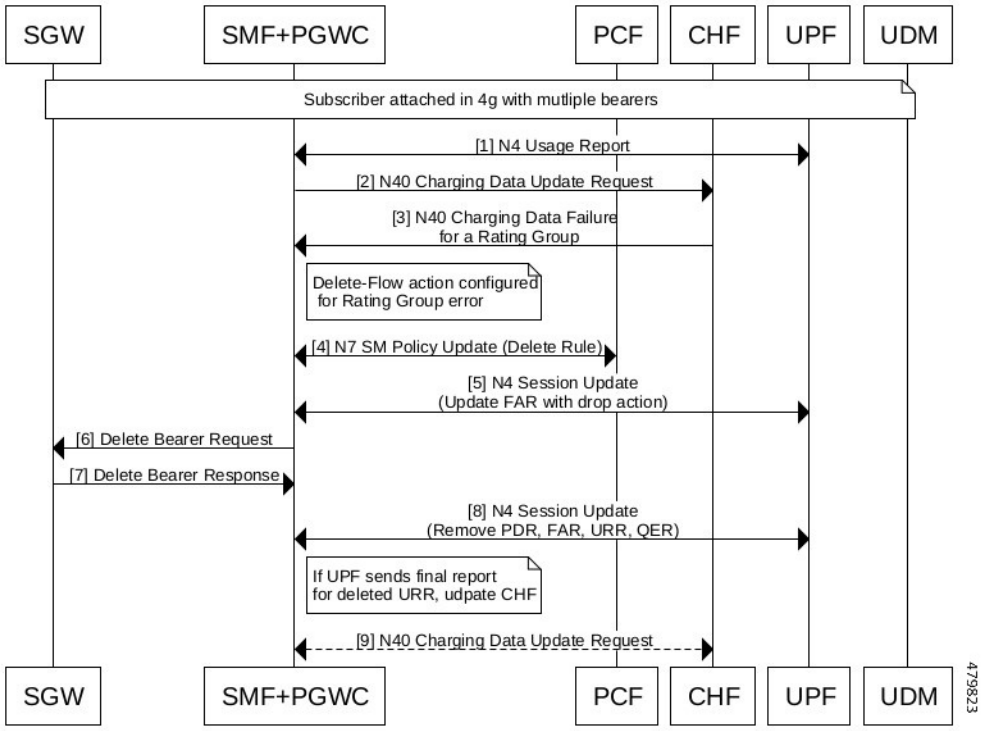


Table 132: 4G Delete Flow Action Call Flow Description

Step	Description
1	A subscriber is attached in 4G with multiple bearers. UPF sends the N4 Usage Report to SMF+PGW-C.
2	SMF+PGW-C sends the N40 Charging Data Update Request to CHF.

Step	Description
3	CHF sends the N40 Charging data failure for a Rating Group to SMF+PGW-C. **Note** Configure the delete flow action for the Rating Group error. This action is used for deletion of the flow or rule associated with the Rating Group.
4	SMF+PGW-C sends the N7 SM Policy Update for deletion of a rule to PCF.
5	SMF+PGW-C sends the N4 Session Update to UPF. This message includes details on updating FAR with the drop action.
6	SMF+PGW-C sends the Delete Bearer Request to S-GW.
7	S-GW sends the Delete Bearer Response SMF+PGW-C.
8	SMF+PGW-C sends the N4 Session Update to PCF. This update includes the details on the PDR, FAR, URR, and QER to be removed. **Note** If the UPF sends the final report for the deleted URR, then SMF sends this update to CHF.
9	SMF+PGW-C sends the N40 Charging Data Update Request to CHF.

SMF Behaviour for Failure Actions

The following table describes the SMF behaviour on receiving different failures (Continue, Ignore, and Terminate) in CDR-(I/U/T).

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Continue	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF if offline CHF is configured	Continue the session without charging	Continue the session without charging	Continue the session deletion
Terminate	Delete the session	Delete the session	Continue the session deletion	Delete the session	Delete the session	Continue the session deletion
Ignore	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion

Standards Compliance

The offline failover support for charging feature complies with the following standards:

- *3GPP TS 32.255, version 15.3.0*
- *3GPP TS 32.290, version 15.4.0*
- *3GPP TS 32.291, version 15.3.0*

Limitations

The offline failover support for charging feature has the following limitation:

- Session Level limits are mandatory from CHF or you must configure them locally. As per the 3GPP specification, the last linked URR can't be removed when the online URR needs to be delinked from the offline URR.

The CHF failure handling at Rating Group and application levels feature has the following limitations:

- In vSMF, only the **terminate** action for the application error is applicable.
- The **drop-data** action is supported only for the online charging.
- If multiple Rating Groups return an error and if one of the errors has the **terminate** action configured, then the PDU session is terminated.
- If multiple Rating Groups return an error and if the Rating Group mapping to the default flow has the **delete-flow** action configured, then the PDU session is terminated.
- If multiple PCC rules and Rating Groups are mapped to a single flow, then any Rating Group error that is configured for **delete-flow** action, results in the deletion of the entire flow.
- For multiple Rating Groups mapped to a single flow, multiple Rating Groups result in failure in the following scenarios:
  - If the **terminate** action is configured, then this action takes the highest priority.
  - If both the **delete-flow** and **drop-data** actions are configured, then the **delete-flow** action takes the higher priority.
  - If both the **convert-to-offline** and **drop-data** actions are configured, then **drop-data** takes the higher priority.

Configuring CHF Failure Handling

This section describes how to configure the CHF failure handling.

This feature involves the following steps:

1. Configuring Failure Handling Profile, on page 367
2. Configuring Offline Server Client and Offline Failure Handling Profile, on page 367

Configuring Failure Handling Profile

You can configure the HTTP status code with the corresponding action for the CHF Create, Update, or Release messages. Based on the configuration of the Failure Handling profile, the SMF takes an action when the CHF server failure occurs.

To configure the failure handling profile, use the following sample configuration:

```
config
  profile nf-client-failure nf-type chf
    profile failure-handling fh_profile_name
      service name type servicename_type
        message type messagetype_value
          status-code httpv2 statuscode_value
            action { continue | retry-and-continue | retry-and-ignore
| retry-and-terminate } retry retry_value
             exit
```

NOTES:

- **profile nf-client-failure nf-type chf**: Specify the name of the network function that is required after the NF client failure.
- **profile failure-handling** *fh_profile_name*: Specify the name of the profile for failure handling.
- **service name type** *servicename_type*: Specify the name of the service type. *servicename_type* can be one of the following values for CHF:
  - nchf-convergedcharging
  - nchf-spendinglimitcontrol
- **message type** *messagetype_value*: Specify the value for the type of message. *messagetype_value* can be one of the following values for CHF:
  - ChfConvergedchargingCreate
  - ChfConvergedchargingUpdate
  - ChfConvergedchargingDelete
- **status-code httpv2** *statuscode_value* : Specify the status code as per the configured failure template. *statuscode_value* must be an integer in the range of 0–599. Use either '-' or ' as separator for the range of status codes.
- **action { continue | retry-and-continue | retry-and-ignore | retry-and-terminate } retry** *retry_value*: Specify the failure action and the number of retry attempts. *retry_value* must be an integer in the range of 1–10.

Configuring Offline Server Client and Offline Failure Handling Profile

To configure the offline client profile and offline failure handling profile for the selected CHF server, use the following sample configuration:

```
config
  profile network-element chf chf_name
    nf-client-profile nf_client_profile_name
```

```
failure-handling-profile fh_profile_name
nf-client-profile-offline offline_server_profile_name
failure-handling-profile-offline fh_profile_offline_name
exit
```

NOTES:

- **profile network-element chf** *chf_name*: Specify the name of the CHF server.
- **nf-client-profile** *nf_client_profile_name*: Specify the name of the NF client profile.
- **failure-handling-profile** *fh_profile_name*: Specify the name of the failure handling profile.
- **nf-client-profile-offline** *offline_server_profile_name*: Specify the NF client profile name for the offline server.
- **failure-handling-profile-offline** *fh_profile_offline_name*: Specify the failure handling profile name for the offline server.

Configuring Action for Rating Group-level and Application-level Errors

Use the following sample configuration to configure an action for Rating Group-level and Application-level errors.

```
config
  profile charging profile_name
    failure-handling error-type [ rg | app ] error-value error_value action
 action_value
    exit
```

NOTES:

- **profile charging** *profile_name*: Enter the Charging Profile configuration mode.
- **failure-handling error-type [rg | app] error-value** *error_value* **action** *action_value*: Configure the failure handling error type as Rating Group or Application with an error value. For the application-level errors, enter one of the following values for *action_value*:
  - **drop-data**—Specify this value to drop data corresponding to the charging ID.
  - **terminate**—Specify this value to release the PDU session.
  - **continue**—Specify this value to disable charging.

  For the Rating Group-level errors, enter one of the following values for *action_value*:
  - **convert-offline**—Specify this value to convert to offline charging.
  - **delete-flow**—Specify this value to delete the flow or rule associated with the Rating Group.
  - **drop-data**—Specify this value to drop data corresponding to the Rating Group.
  - **terminate**—Specify this value to release the PDU session.

Note

- If you haven't configured an action for the Rating Group-level and application-level errors, the SMF continues with the default behavior.
- SMF doesn’t allow mapping of multiple QoS flows to the same Rating Group for dynamic rules.
- The **drop-data** action is applicable to all the flows that are associated to the Rating Group.

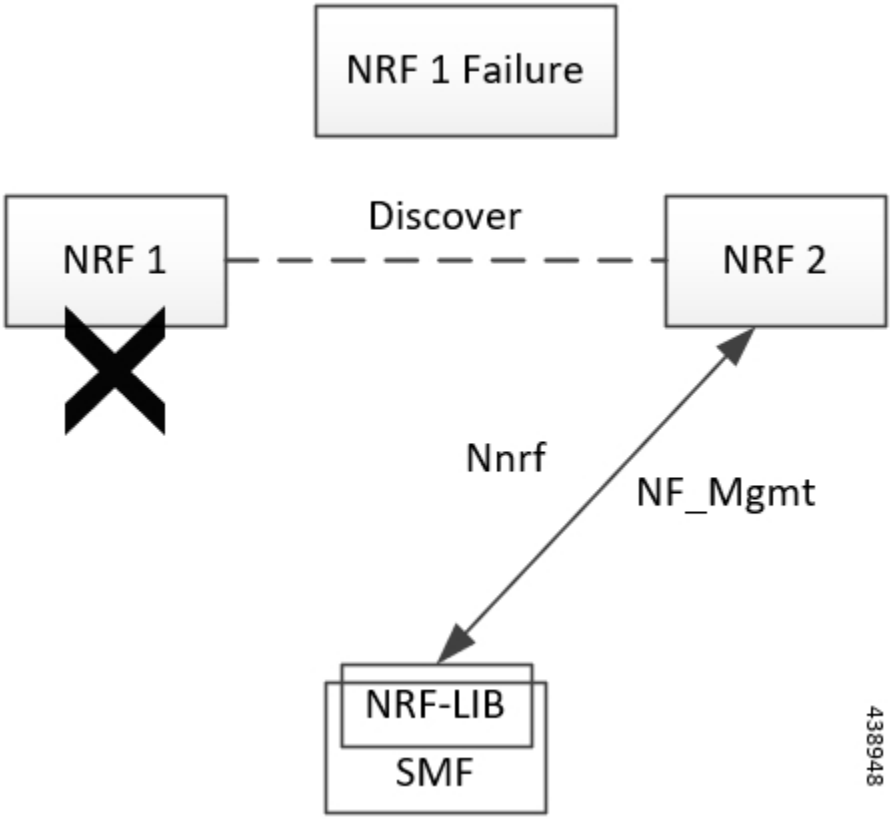
Network Repository Function Failure Handling

Feature Description

The Network Repository Function (NRF) communication failure handling logic is implemented within the SMF. The SMF uses the NF registration messages for tracking the management NRF group operational status.

How it Works

The following figure shows how the SMF handles NRF failures.



In the preceding diagram, NRF 1 is Primary and NRF 2 is secondary for SMF. On bringing up, the SMF registers (NF registration) with NRF 1 and starts NF heartbeat with NRF 1. The SMF uses the heartbeat response to track the operational status.

In case the SMF detects NRF 1 failure by missing NF heartbeat response, the SMF registers to NRF 2 (secondary NRF) and starts sending NF heartbeat. The SMF continues to send NF Register message to NRF 1 to keep track of its status.

If the SMF receives register response from NRF 1, it detects that the NRF 1 is up again. The SMF marks NRF 1 as active once it recovers and stops sending NF heartbeats to NRF 2.

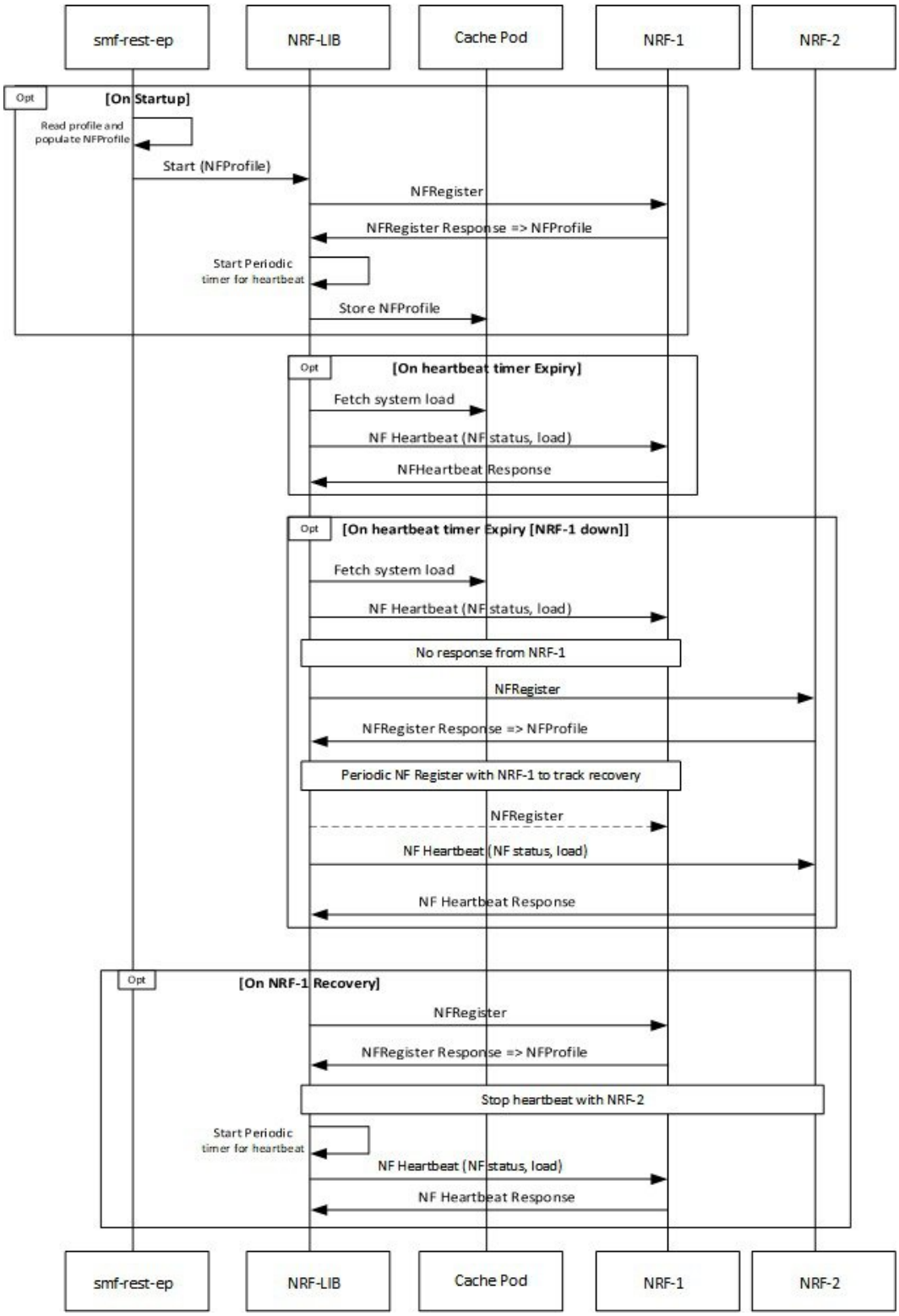
Note NF Reregistration (default behavior) on failover and fallback is configuration driven. When NRF 2 detects that the SMF has stopped sending heartbeats, it checks from NRF 1 if it has received SMF registration by using discovery with SMF instance ID.

As the management and discovery endpoint groups are separate, the Registration based operation status check is not used for NRF failure handling during NF discovery. During NF discovery, the configured NRF endpoints within the group are attempted in the priority order. If the first choice NRF endpoint is not responding, the next best NRF endpoint is chosen.

Call Flow

The following diagram shows the basic NF management call flow covering the NF registration, NF management and the NRF failure handling.

Figure 80: NF Management Call Flow



Configuring NRF Failure Handling

This section provides the NRF configurations that are required for the failure handling of other NFs.

Configuring the Failure Handling Template

To configure the failure handling template, use the following sample configuration:

```
config
  profile nf-client-failure { nf-type { amf | chf | nrf | pcf | udm }
    profile failure-handling failure_handling_name
    end
```

NOTES:

- **profile nf-client-failure { nf-type { amf | chf | nrf | pcf | udm }**: Specify the required NF client failure profile and provide the local configuration support for the following configured NFs:
  - **amf**: Enable the AMF local configuration
  - **chf**: Enable the CHF local configuration
  - **nrf**: Enable the NRF local configuration
  - **pcf**: Enable the PCF local configuration
  - **udm**: Enable the UDM local configuration

    For example, if the NF type selected is **udm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **profile failure-handling** *failure_handling_name*: Specify the failure handling profile name. For example, "udmFail".

Configuration Example

The following is an example configuration of NRF failure handling.

```
group nf-mgmt NFMGMT1
   nrf-mgmt-group nrf-nfmgmt-grp
      failure-handling-profile FHNRF
         locality       LOC1
            heartbeat interval 50
         exit

profile nf-client-failure nf-type nrf
   profile failure-handling FHNRF
      service name type nrf-nfm
         responsetimeout 2300
            message type NRFRegistration
               failover-enabled true
               status-code httpv2 400,500
            action retry
         exit
         status-code httpv2 401,504
         action retry-next
      exit
   exit
message type NFUpdate
   failover-enabled true
```

```
      status-code httpv2 400,503
   action retry
exit
status-code httpv2 411,500
   action retry-next
   exit
exit
message type Heartbeat
      re-registration-enabled true
      status-code httpv2 400,429
   action retry
exit
         status-code httpv2 411,500
            action retry-next
          exit
        exit
     exit
  exit
exit
```

When an AMF failure occurs, use the following example configuration for the range of error codes with the same retry-action and retry-count in the failure handling template.

Note You can use similar configuration during the failure of other NFs.

```
profile nf-client-failure nf-type amf
 profile failure-handling FH1
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH2
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 401
     retry  4
     action continue
    exit
   exit
  exit
 exit

profile failure-handling FH3
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 250-260
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH4
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
```

```
    action continue
   exit
  exit
 exit
exit
profile failure-handling FH5
 service name type namf-loc
  message type AmfCommEBIAssignment
   status-code httpv2 150,160,170-175
    action continue
   exit
  exit
 exit
exit
```

The following configuration is an example of the failure template mapping to DNN.

```
profile dnn intershat
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit
```

The following configuration is an example of the failure template mapping to SMF.

```
profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 209.165.202.129
 bind-port        8008
 fqdn             example.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

Configuring Failure Handling Actions

To configure the failure retry and action for each NF service and the different message types, use the following sample configuration:

```
config
  profile nf-client-failure { nf-type { amf | chf | pcf | udm }
  profile failure-handling failure_handling_name
     service name type service_type
        message type message_type
           status-code httpv2 status_code
           retry retry_count
           action { continue | retry-and-continue | retry-and-terminate |
 terminate }
           end
```

NOTES:

- **service name type** *service_type*: Specify the configured NF service types and provide the local configuration support for the following configured NFs. The service types vary depending on the configured service.

  The AMF service supports the following service types:

  - **namf-comm**
  - **namf-evts**
  - **namf-loc**
  - **namf-mt**

  The CHF service supports the following service types:

  - **nchf-convergedcharging**
  - **nchf-spendinglimitcontrol**

  The NRF service supports the following service type:

  - **nrf-nfm**

  The PCF service supports the following service types:

  - **npcf-am-policy-control**
  - **npcf-bdtpolicycontrol**
  - **npcf-eventexposure**
  - **npcf-policyauthorization**
  - **npcf-smpolicycontrol**
  - **npcf-ue-policy-control**

  The UDM service supports the following service types:

  - **nudm-ee**
  - **nudm-pp**
  - **nudm-sdm**
  - **nudm-ueau**

- **nudm-uecm**

For example, if the *service_type* that is selected is **nudm-sdm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **message type** *message_type*: Specify the configured NF message type and provide the local configuration support for the configured NF.

  The message types vary depending on the configured profile and service type.

- **status code httpv2** *status_code* : Specify the status code for the retry and action for the NF service. Currently only "http" status code is provided. *status_code* must be an integer in the range of 0–599.

- **retry** *retry_count*: Specify the number of times the NF service must retry before proceeding with the action. *retry_count* must be an integer in the range of 1–10.

- **action**: Specify the action. The supported actions are:

  - **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.

  - **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.

  - **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.

  - **terminate**: Specify to terminate the session without any retry. The retry count configuration is invalid with this action.

    The retry and action for a message send is picked based on the first sent status code failure. A different status code in the retry does not lead to picking a new retry count and action.

The following table provides a sample of the configured profile, service, and message type options.

Profile	Service Type	Message Type Options
amf	namf-comm	• AmfCommEBIAssignment • AmfCommN1N2MessageTransfer • AmfCommSMStatusChangeNotify • range
chf	nchf-convergedcharging	• ChfConvergedchargingCreate • ChfConvergedchargingDelete • ChfConvergedchargingUpdate • range
nrf	nrf-nfm	• Heartbeat • NFUpdate • NRFRegistration

Profile	Service Type	Message Type Options
pcf	npcf-am-policy-control	• PcfSmpolicycontrolCreate • PcfSmpolicycontrolDelete • PcfSmpolicycontrolUpdate • range
udm	nudm-sdm	• UdmRegistrationReq • UdmSdmGetUESMSubscriptionData • UdmSdmSubscribeToNotification • UdmSubscriptionReq • UdmUecmRegisterSMF • UdmUecmUnregisterSMF • UdmSdmUnsubscribeToNotification • range

Note The example does not cover all the message options that are provided for each profile and service type.

Configuring NRF Failover Option

The NRF Failover feature enables the user to configure the retry actions for every error code, which occurs during the NRF interactions with SMF and other NFs.

After trying all the hosts or endpoints, the next action is decided based on the failover options, which are configured for the error codes.

To configure the NRF failover functionality, use the following sample configuration:

```
config
  profile nf-client-failure nrf
    profile failure-handling failure_handling_name
       service name type nrf-nfm
          message type { Heartbeat [ re-registration-enabled { false |
true } ] | NFUpdate [ failover-enabled { false | true } ] | NRFRegistration
 [ failover-enabled { false | true } ] }
            status-code httpv2 status_code  action { retry | retry-next }
            end
```

NOTES:

- **message type { Heartbeat [re-registration-enabled { false | true }] | NFUpdate [failover-enabled { false | true }] | NRFRegistration [failover-enabled { false | true }] }** : Specify the NRF message type and enable failover functionality.

The failover options for the NRF messages are as follows:

- **NRFRegistration** or **NFUpdate**
  - **true**—After trying all the hosts or endpoints in an NRF, the system selects the next available NRF.
  - **false**—After trying all the hosts or endpoints in an NRF, the system does not select the next available NRF.

  Spawning of backup routine is only available for those NRFs in which the endpoints have been tried.
- **Heartbeat**
  - **true**—After trying all the hosts or endpoints in an NRF, if the start reregistration option is enabled, then the system starts the reregistration process for the NF clients.
  - **false**—After trying all the hosts or endpoints in an NRF, the system continues the heart beat routine with the same registered NRF.

- **status-code httpv2** *status_code* **action { retry | retry-next }**: Specify the status code and retry action for the NRF service. Currently only "http" status code is provided. *status_code* must be an integer in the range of 0–599.
  - **retry**—The system attempts one more retry to the same endpoint or host.
  - **retry-next**—The system does not retry the same endpoint or host, but it attempts the retry action to the next available endpoint or host.
- The error handling for NF Registration, NF Heartbeat, and NF Update is based on status codes. This functionality is not available for subscription and NF Deregister messages. The user can configure the max retry-count for the subscription and NF Deregister messages by using the endpoint configuration available in the **group nrf management** CLI. The system attempts the retry action based on that configuration.
- The failover-enabled option is applicable for the NF Registration and NF Update messages.
- The reregistration-enabled option is applicable for the NF Heartbeat message.
- The failover-enabled or reregistration-enabled options are not applicable for the NF Deregister message.
- The failover and reregistration options are enabled by default.

Configuring Failure Handling in Network Element Profile

To configure the failure handling in the network element profile, use the following sample configuration:

```
config
  profile network-element { { amf | chf | pcf | udm } nf_profile_name }
    failure-handling-profile profile_name
    end
```

NOTES:

- **failure-handling-profile** *profile_name*: Specify the NRF failure handling network profile for the configured NF type. *profile_name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.

Configuration Example

The following is an example configuration.

```
group nf-mgmt NFMGMT1
   nrf-mgmt-group nrf-nfmgmt-grp
      failure-handling-profile FHNRF
         locality       LOC1
            heartbeat interval 50
         exit

profile nf-client-failure nf-type nrf
   profile failure-handling FHNRF
      service name type nrf-nfm
         responsetimeout 2300
            message type NRFRegistration
               failover-enabled true
               status-code httpv2 400,500
            action retry
         exit
         status-code httpv2 401,504
         action retry-next
      exit
   exit
message type NFUpdate
   failover-enabled true
      status-code httpv2 400,503
   action retry
exit
status-code httpv2 411,500
   action retry-next
   exit
exit
message type Heartbeat
      re-registration-enabled true
      status-code httpv2 400,429
   action retry
exit
         status-code httpv2 411,500
            action retry-next
          exit
        exit
     exit
  exit
exit
```

When an AMF failure occurs, use the following example configuration for the range of error codes with the same retry-action and retry-count in the failure-handling template.

```
profile nf-client-failure nf-type amf
 profile failure-handling FH1
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     retry  4
     action continue
    exit
   exit
  exit
```

```
 exit
 profile failure-handling FH2
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 401
     retry  4
     action continue
    exit
   exit
  exit
 exit

profile failure-handling FH3
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 250-260
     retry  4
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH4
  service name type namf-comm
   message type AmfCommEBIAssignment
    status-code httpv2 100,200,300,400-410
     action continue
    exit
   exit
  exit
 exit
 profile failure-handling FH5
  service name type namf-loc
   message type AmfCommEBIAssignment
    status-code httpv2 150,160,170-175
     action continue
    exit
   exit
  exit
 exit
exit
```

Verifying the NRF Failure Handling

NF Management Failure Handling

The following is an example of management NRF endpoint configuration.

```
product smf# show running-config group nf-mgmt
group nf-mgmt MGM
 nrf-mgmt-group mgmt_group
 locality       LOC1
exit
product smf# show running-config group nrf mgmt
group nrf mgmt mgmt_group
 service type nrf nnrf-nfm
  endpoint-profile epprof
   uri-scheme http
   endpoint-name EP1
    priority 2
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 8082
```

```
    secondary ip-address ipv4 209.165.200.238
    secondary ip-address port 8082
   exit
   endpoint-name EP2
    priority 10
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.200.238
    secondary ip-address port 8082
   exit
  exit
 exit
exit
product smf#
```

In the sample configuration, EP1 is the higher priority endpoint name as its priority is lesser than EP2 (2 against 10). On bringing up, SMF sends NF registration to primary ip:port of EP1 [209.165.200.235:8082]. SMF uses secondary ip:port of EP1 if the primary is down. SMF performs a failover of endpoint to EP2 only if all ip:port of EP1 is down.

On successful registration with EP1 primary, SMF starts heartbeat with EP1 primary. If EP1 primary goes down, SMF detects the same by missing heartbeat response. On detecting that the EP1 primary is down, SMF sends heartbeat to EP1 secondary without reregistration. Also, it periodically sends NF heartbeat to EP1 primary to detect if it has recovered.

If SMF detects that EP1 primary and secondary is down, SMF performs a failover of endpoint to EP2. After the successful failover to EP2 primary, it sends reregistration (default behavior). It is assumed that all the endpoints with an endpoint name shares the same database and so reregistration is only supported when the failover is across endpoint names. In this case, EP1 primary and secondary share the same database. Similarly, EP2 primary and secondary share another database. On failover to EP2 primary, periodic NF registration is sent to primary of the EP1 only (to detect recovery).

Whenever a higher priority endpoint name is detected to be recovered, SMF falls back to the recovered IP:Port. For example, the current active NRF endpoint is EP2 primary and SMF detects that EP1 primary has recovered, then SMF performs reregistration with EP1 primary (default behavior) and stops heartbeat on EP2 primary.

Within endpoint NF heartbeat is used to track operational status. Across endpoints, registration is used to track the operational status. Request message timeout, RPC error, and HTTP response codes 408, 429, 500, 501, 502, 503 are considered as failure to move to the next NRF.

NF Discovery Failure Handling

The following is an example of discovery NRF endpoint configuration.

```
product smf# show running-config profile nf-pair nf-type UDM
profile nf-pair nf-type UDM
 nrf-discovery-group others_group
 locality client LOC1
exit
product smf# show running-config group nrf discovery others_group
group nrf discovery others_group
 service type nrf nnrf-disc
  endpoint-profile ep1
   capacity 30
   priority 50
   uri-scheme http
   endpoint-name ED1
    priority 56
    primary ip-address ipv4 209.165.201.19
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.201.20
```

```
    secondary ip-address port 8082
    exit
   endpoint-name ED2
    priority 10
    primary ip-address ipv4 209.165.201.21
    primary ip-address port 8082
    secondary ip-address ipv4 209.165.201.22
    secondary ip-address port 8082
   exit
  exit
 exit
exit
product smf#
```

In the sample configuration, ED1 is the higher priority endpoint name as its priority is lesser than ED2 (2 against 10). Whenever a NRF discovery is required, primary ip:port of ED1 [209.165.201.19:8082] is attempted. SMF uses secondary ip:port of ED1 if the primary is down. SMF performs a failover of endpoint to ED2 only if all ip:port of ED1 is down. There is no state maintained regarding NRF discovery failure with any NRF endpoint. The SMF always starts with ED1 primary and falls back to ED1 secondary in case of failure, followed by ED2 primary, and so on.

Policy Control Function Failure Handling

Feature Description

The SMF utilizes the NF Failover support to achieve the PCF failover functionality.

The NF Failover feature supports the following functionality:

- Multiple endpoints for a service as primary and secondary endpoints. The endpoints can be configured using the NRF Client Profile configuration and the NRF Failure Profile configuration.
- Failure behavior based on:
  - Message Type
  - HTTP Status Codes in the response messages

Once the PCSCF profile is configured, the SMF assumes that the PDU activation is for the IMS and IMS requires PCF, then SMF rejects the PDU regardless of the failure handling configuration.

- The SMF ignores the failure handling configuration and rejects the PDU creation if there is “pcscf-profile” under profile dnn.
- Operator can’t configure the following parameters under the same “profile dnn”:
  - pcf-interaction false
  - pcscf-profile

How it Works

This section describes how the SMF handles message-level failures and the corresponding HTTP status code-based failures.

The SMF initiates the following messages:

- PcfSmpolicycontrolCreate
- PcfSmpolicycontrolUpdate
- PcfSmpolicycontrolDelete

During the PDU session lifecycle, the SMF exchanges the messages at various stages with the PCF. Depending on the HTTP status code configured in the NRF failure profile, the SMF takes one of the following actions:

- Ignore
- Continue
- Terminate

Table 133: Relationship between PCF Failover Messages and Actions

	PcfSmpolicy controlCreate	**PcfSmpolicy controlUpdate**	**PcfSmpolicy controlDelete**
Ignore	Continue with locally configured/UDM-provided policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Continue with currently available snapshot of policy parameters. Contact PCF for subsequent messages. **PCF-Interaction Status: ON**	Ignore the current failure and delete the session. **PCF-Interaction Status: Session deleted**
Continue	Continue with locally configured/UDM-provided policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Continue with currently available snapshot of policy parameters. **Note** Do not contact PCF for subsequent messages. **PCF-Interaction Status: OFF**	Ignore the current failure and delete the session. **PCF-Interaction Status: Session deleted**
Terminate	Terminate the session.	Terminate the session.	Terminate the session.

PCF Interaction Status

This feature supports the following status messages for SMF-initiated and PCF-initiated messages:

- **PCF-Interaction Status: ON**

  SMF-initiated messages—The SMF continues to initiate the messages towards the PCF whenever the criteria is met.

  PCF-initiated messages—The SMF continues to accept all the messages initiated from the PCF towards the SMF.

- **PCF-Interaction Status: OFF**

SMF-initiated messages—The SMF does not initiate or send the messages towards the PCF whenever the criteria is met. The SMF treats the PCF as if it is not available and continues further actions.

PCF-initiated messages—There are two messages initiated by the PCF.

- SmPolicyUpdateNotifyReq: On receiving this message, the SMF sends a 404 error code in response and cleans up the session and does not send the Delete Request to the PCF.

Note The SMF also sends FIVEGSM_CAUSE value as **REACTIVATION REQUESTED** in the FIVEG_PDU_SESSION_RELEASE_COMMAND to UE for 5G. In case of 4G, the SMF sends cause **REACTIVATION REQUESTED** in DELETE BEARER REQUEST message to the S-GW.

- SmPolicyAssociationTerminationReq—On receiving this message, the SMF sends a success response and cleans up the session. As part of this interaction, the SMF sends a Delete Request to the PCF.

Note This is an exception when the PCF-Interaction Status is set to OFF.

Configuring the PCF Failure Handling Feature

This section desribes how to configure the PCF Failure Handling feature.

Configuring the PCF Failure Handling feature involves the following steps:

- Configuring the PCF Failure Handling Profile, on page 384
- Configuring the Association of Failure Handling Profile, on page 385
- Configuring Secondary and Tertiary IP Addresses, on page 385

Configuring the PCF Failure Handling Profile

To configure the PCF failure handling profile with action, use the following sample configuration:

```
config
  profile nf-client-failure nf-type pcf
    profile failure-handling fhprofile_name
      service name type servicename_type
        message type messagetype_value
          status-code httpv2 status_code
          action { continue | retry-and-continue | retry-and-ignore |
retry-and-terminate } retry retry_value
          exit
```

NOTES:

- **profile failure-handling** *fhprofile_name*: Specify the failure handling profile name.
- **service name type** *servicename_type*: Specify the PCF service name type. *servicename_type* can be one of the following values:

  - npcf-am-policy-control
  - npcf-bdtpolicycontrol
  - npcf-eventexposure
  - npcf-policyauthorization
  - npcf-smpolicycontrol
  - npcf-ue-policy-control

- **message type** *messagetype_value*: Specify the message type. *messagetype_value* can be one of the following values:
  - PcfAmfPolicyControlCreate
  - PcfSmpolicycontrolCreate
  - PcfSmpolicycontrolDelete
  - PcfSmpolicycontrolUpdate

- **status-code httpv2** *status_code*: Specify the HTTPv2 status code. *status_code* must be an integer in the range of 0–599, separated by either '-' or ','.
- **action { continue | retry-and-continue | retry-and-ignore | retry-and-terminate } retry** *retry_value*: Specify the action and the number of retry attempts. *retry_value* must be an integer in the range of 1–10.

Configuring the Association of Failure Handling Profile

To configure the association of FH profile in PCF, use the following sample configuration:

```
config
  profile network-element pcf pcf_profile_name
    nf-client-profile nf_profile_name
    failure-handling-profile fh_profile_name
    exit
```

NOTES:

- **nf-client-profile** *nf_profile_name*: Specify the NF client profile name.
- **failure-handling-profile** *fh_profile_name*: Specify the failure handling profile name.

Configuring Secondary and Tertiary IP Addresses

To configure the secondary and tertiary IP addresses, use the following sample configuration:

```
config
  profile nf-client nf-type pcf
    pcf-profile pcfprofile_name
      locality locality_name
        service name type npcf-smpolicycontrol
          endpoint-profile endpointprofile_name
            endpoint-name endpoint_name
              primary ip-address { ipv4 primary_ipv4_address | ipv6
```

```
primary_ipv6_address | port primary_port_number }
                    secondary ip-address { ipv4 secondary_ipv4_address | ipv6
secondary_ipv6_address | port secondary_port_number }
                    tertiary ip-address { ipv4 tertiary_ipv4_address | ipv6
tertiary_ipv6_address | port tertiary_port_number }
                    end
```

NOTES:

- **primary ip-address ipv4** *primary_ipv4_address*: Specify the IPv4 address of primary endpoint.
- **primary ip-address ipv6** *primary_ipv6_address*: Specify the IPv6 address of primary endpoint.
- **primary ip-address port** *primary_port_number*: Specify the port number of primary endpoint.
- **secondary ip-address ipv4** *secondary_ipv4_address*: Specify the IPv4 address of secondary endpoint.
- **secondary ip-address ipv6** *secondary_ipv6_address*: Specify the IPv6 address of secondary endpoint.
- **secondary ip-address port** *secondary_port*: Specify the port number of secondary endpoint.
- **tertiary ip-address ipv4** *tertiary_ipv4_address*: Specify the IPv4 address of tertiary endpoint.
- **tertiary ip-address ipv6** *tertiary_ipv6_address*: Specify the IPv6 address of tertiary endpoint.
- **tertiary ip-address port** *tertiary_port_number*: Specify the port number of tertiary endpoint.

OAM Support for PCF Failure Handling

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

This feature supports the following statistics:

- PcfSmpolicyControlCreate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PcfSmPolicyControlUpdate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PcfSmpolicyControlDelete
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

- PolicyUpdateNotifyReq
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- PolicyDeleteReq
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- PolicyUpdateRequest
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- Gauge counter for number of subscribers with policy type local/pcf.

Unified Data Management Failure Handling

Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network.

The UDM failure handling support on SMF introduces a new failure handling template (FHT) profile. This profile is associated with the UDM profile in SMF.

The FHT template provides flexibility for SMF to fine tune its interactions with UDM over N10 for the sessions. It supports the SMF to handle the HTTP status codes in response from UDM for both new and existing sessions.

The NF failover support is available in the SMF using the NF Client profile configuration and the NF failure profile configuration. This feature supports the following functionality:

- Configure multiple endpoints for a service as primary and secondary endpoints.
- Specify the failure handling behavior based on:
  - Message Type
  - HTTP Status Codes in the response messages

How it Works

The SMF utilizes the NF Failover to achieve the UDM failover support functionality. This section provides information on how the SMF handles message-level failures and the corresponding HTTP status code-based failures.

The SMF initiates the following messages:

- UE-Connection-Management (UE-CM)
  - Nudm_UECM_Registration
  - Nudm_UECM_DeRegistration
- UE-Subscription-Management (UE-SDM)
  - Nudm_SDM_Get
  - Nudm_SDM_Subscribe
  - Nudm_SDM_Unsubscribe

During the PDU session lifecycle, the SMF exchanges the preceding messages at various stages with the UDM. Depending on the HTTP status code configured in the NF failure profile, the SMF takes one of the following actions:

- Ignore
- Continue
- Terminate

The SMF provides the following actions to attempt the same request to other available UDM servers.

- retry-and-terminate
- retry-and-ignore
- retry-and-continue

When all the retry attempts fail, the SMF takes the appropriate failure handling action. For example, if the FH action is retry-and-terminate, the SMF terminates the call after all the attempts fail.

Note The SMF allows dynamic changes to the failure handling template configuration. Any changes to the configuration apply only to the new calls.

Table 134: Relationship between N10 Messages and Failover Actions

Scenario	Service	Message	Condition	Action	Success Response	Handling of Failure Response		
						Terminate	Continue	Ignore
PDU Session Creation procedures in 5G, 4G, and Wi-Fi Inter-RAT Handover procedures	UECM	Nudm_ UECM _Registration	If the Nudm UECM Registration is not done and the access type is not 4G	Send the message	Mark the Registration is successful	Terminate call	Continue call	Continue call
		Nudm _UECM_ DeRegistration	If the Nudm UECM Registration is done	Send the message	No action	Terminate call	Terminate call	Terminate call
PDU Session Creation procedures in 5G, 4G, and Wi-Fi	SDM	Nudm_SDM _Get	If skipping the subscription fetch config is not enabled	Send the message	Mark the subscription fetch is successful	Terminate call	Continue call	Continue call
		Nudm_ SDM _Subscribe	If the subscription fetch is successful	Send the message	No action	Terminate call	Continue call if the subscription is not done	Continue call if the subscription is not done
PDU Session Release procedures in 5G, 4G, and Wi-Fi	SDM	Nudm_SDM _Unsubscribe	If the subscription fetch is successful and the registration is not done	Send the message	No action	Terminate call	Continue call	Continue call

- **Terminate**: The SMF terminates the call in any message type.
- **Continue**: The SMF ignores the current failure and skips the subsequent interaction for the other messages in the same service group.
- **Ignore**: The SMF ignores failure only for the current interaction and proceeds with the call. The SMF processes the subsequent message interaction.
- Perform UDM subscription fetch only during the session establishment in EPS and NR network.

  If the UDM subscription fetch fails and the FH action is ‘Ignore’ or the configuration to skip subscribe-to-notification is enabled, then the SMF skips the subscribe-to-notification interaction.

- When the UDM failure handling template is not configured, the default failure handling action is 'Terminate'.

Configuring UDM Failure Handling Feature

This section describes how to configure the UDM Failure Handling feature.

Configuring the UDM Failure Handling feature involves the following steps:

- Configuring UDM Failure Handling Profile, on page 390
- Configuring Association of FH profile, on page 390
- Configuring Secondary and Tertiary IP Addresses, on page 391

Configuring UDM Failure Handling Profile

Use the following sample configuration to configure the UDM failure handling profile with action.

```
config
   profile nf-client-failure nf-type udm
      profile failure-handling fh_profile_name
         service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
         | nudm-uecm }
        message type { UdmRegistrationReq | UdmSdmGetUESMSubscriptionData

         | UdmSdmSubscribeToNotification | UdmSubscriptionReq
         | UdmUecmRegisterSMF | UdmUecmUnregisterSMF |
         UdmSdmUnsubscribeToNotification }
            status-code httpv2 0
               action { continue | retry-and-continue | retry-and-ignore
             | retry-and-terminate | terminate }
             end
```

Configuring Association of FH profile

To configure the association of FH profile in the UDM, use the following sample configuration:

```
config
   profile network-element udm udm_profile_name
      nf-client-profile nf_profile_name
      failure-handling-profile fh_profile_name
      failure-handling-profile-rat nr
         failure-handling-profile fh_profile_name
         exit
```

NOTES:

- **failure-handling-profile-rat nr**: Specify the failure handling profile specific to RAT type.
- **failure-handling-profile** *fh_profile_name*: Specify the failure handling network profile name. *fh_profile_name* must be a string.

Verifying the RAT-based FH Profile

This section describes how to verify RAT-based FH profile in the UDM.

Use the **show running-config profile network-element udm** *udm_profile_name* command to verify the feature configuration details.

The following is an example output.

```
nf-client-profile UP1
   failure-handling-profile FH1
   failure-handling-profile-rat nr
      failure-handling-profile FH4
      exit
exit
```

In this example, FH1 is the default failure handling profile. However, if the RAT type is configured as **nr**, then the failure handling profile FH4 is used.

Configuring Secondary and Tertiary IP Addresses

To configure secondary and tertiary IP addresses, use the following sample configuration:

```
config
   profile nf-client nf-type udm
      udm-profile udmprofile_name
         locality LOC
            service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
 | nudm-uecm }
               endpoint-profile epprofile_name
                  endpoint-name endpoint_name
                     primary ip-address { ipv4 primary_ipv4_address | ipv6
primary_ipv6_address | port primary_port_number }
                    secondary ip-address { ipv4 secondary_ipv4_address | ipv6
 secondary_ipv6_address | port secondary_port_number }
                     tertiary ip-address { ipv4 tertiary_ipv4_address | ipv6
 tertiary_ipv6_address | port tertiary_port_number }
                     end
```

NOTES:

- **primary ip-address ipv4** *primary_ipv4_address*: Specify the IPv4 address of primary endpoint.
- **primary ip-address ipv6** *primary_ipv6_address*: Specify the IPv6 address of primary endpoint.
- **primary ip-address port** *primary_port_number*: Specify the port number of primary endpoint.
- **secondary ip-address ipv4** *secondary_ipv4_address*: Specify the IPv4 address of secondary endpoint.
- **secondary ip-address ipv6** *secondary_ipv6_address*: Specify the IPv6 address of secondary endpoint.
- **secondary ip-address port** *secondary_port*: Specify the port number of secondary endpoint.
- **tertiary ip-address ipv4** *tertiary_ipv4_address*: Specify the IPv4 address of tertiary endpoint.
- **tertiary ip-address ipv6** *tertiary_ipv6_address*: Specify the IPv6 address of tertiary endpoint.
- **tertiary ip-address port** *tertiary_port_number*: Specify the port number of tertiary endpoint.

Configuring Response Timeout Parameter

To configure response timeout for fail-open support over the UDM interface (N10), use the following sample configuration:

```
config
  profile network-element udm udm_profile_name
    response-timeout timeout_value
    exit
```

NOTES:

- **response-timeout** *timeout_value*: Specify the response timeout in milliseconds. *timeout_value* must be an integer in the range of 1000-30000.

  Default: 4000

Verifying the Response Timeout Configuration

The following is an example configuration.

```
[unknown] smf# show running-config profile network-element udm
profile network-element udm udm1
nf-client-profile UP1
failure-handling-profile FH4
query-params [ dnn ]
response-timeout 2000
exit
[unknown] smf#
```

Statistics

The following statistics are supported for all the UDM message status with status as Attempted/Success/Skipped/Failed for all UDM services and message combination.

```
udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC"
,instance_id="1",msg_status="attempted",rat_type="nr",service_name="smfservice",
udm_end_point="",udm_msg="UdmSmSubscription”} 1
```

```
udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC",
instance_id="1",msg_status="skipped",rat_type="nr",service_name="smfservice",udm_end_point="",
udm_msg="UdSmSubscription"} 1
```

OAM Support for UDM Failure Handling Feature

This section describes the operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The SMF maintains the following statistics in support of the UDM Failure Handling feature.

- Nudm_UECM_Registration
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

- Nudm_UECM_DeRegistration
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm_SDM_Get
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm_SDM_Subscribe
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm_SDM_Unsubscribe
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

The "udm_msg_processing_status" statistic in smf-service tracks the number of UDM messages with status as—Attempted, Success, Skipped, and Failed.

For example:

```
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="attempted",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdmSmSubscription"} 1
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="skipped",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdSmSubscription"} 1
```

User Plane Function Failure Handling

Feature Description

During a session, if the User Plane function (UPF) is in congested state, it rejects the Packet Forwarding Control Protocol (PFCP) establishment messages from SMF with a cause code in the response message. To reduce call loss, the SMF retries to send PFCP establishment messages to a different UPF. Then, SMF selects a UPF based on configured priority value and capacity (that is, load information from UPF).

The SMF provides a failure handling template (FHT) profile for PFCP. This profile is associated with the UPF profile in SMF.

The FHT template provides flexibility for SMF to fine tune its interactions with UPFs for sessions. It enables SMF to handle the error cause codes in response from UPF for both new and existing sessions. Based on the error cause codes in response from UPF, this feature provides the following configurable actions:

- ignore
- terminate
- retry-terminate

This following table describes the configuration options available for N4 Session Establishment Request, N4 Session Modification Request, and N4 Session Report Request messages.

Table 135: Configuration Matrix

Message type	Applicable action	Applicable cause code	Default beha
N4Session EstablishmentReq	retry-terminate	• pfcp-entity-in -congestion • system-failure • service-not -supported • no-resource -available • no-response -received • reject	terminate
N4Session ModificationReq	terminate	• mandatory-ie -incorrect • session-ctx-not -found • no-response -received • reject • no-resource -available • pfcp-entity-in -congestion	continue
N4SessionReportReq	ignore terminate	2-255	terminate

Configuring the UPF Failure Handling Feature

This section describes how to configure the UPF Failure Handling feature.

Configuring the UPF Failure Handling feature involves the following steps:

1. Configuring UPF Failure Handling Profile, on page 395
2. Configuring the Failure Profile Association, on page 397

Configuring UPF Failure Handling Profile

To configure the UPF failure handling profile, use the following sample configuration:

```
config
  profile failure-handling fh_profile_name
     interface pfcp message { N4SessionEstablishmentReq |
N4SessionModificationReq | N4SessionReportReq }
       cause-code cause_ID
       action { ignore | retry-terminate { max-retry retry_value } |
terminate }
       end
```

NOTES:

- **profile failure-handling** *fh_profile_name*: Specify the UPF failure handling profile name.
- **interface pfcp message { N4SessionEstablishmentReq | N4SessionModificationReq | N4SessionReportReq }**: Specify the failure handling for N4SessionEstablishmentReq (for new sessions), N4SessionModificationReq messages (for existing sessions), and N4 Session Report Request.

  .

Note UPF reselection is not applicable for message type N4SessionModificationReq because the session is already active on a UPF.

- **cause-code** *cause_ID*: Specify the error codes that the SMF receives in the failure response message from the UPF.

  For the N4SessionEstablishmentReq and N4SessionModificationReq message types, the *cause_ID* must be one of the following values:

  - **pfcp-entity-in-congestion**: Specify this cause code when the UPF is congested.
  - **reject**: Specify this option to handle the cause codes in the failure response message from UPF. The cause codes are not configured by using the CLI commands available for this feature.
  - **no-response-received**: Specify this option to determine the scenarios where SMF does not receive any response from UPF.
  - FHT does not support the following cause codes, which are configured with their default behaviour:
    - **request-reject-unspecified**
    - **cond-ie-missing**
    - **invalid-length**
    - **invalid-fw-policy**
    - **invalid-fteid-alloc-opt**
    - **no-established-pfcp-assoc**
    - **rule-creation-mod-failure**.

For the N4SessionReportReq message type, the *cause_ID* must be an integer in the range of 2– 255. Separate the cause code value using either '-' or ',' or both. For example, **cause-code 72-74,76,78-100**

When the **N4SessionReportReq** keyword is configured, the SMF triggers the Session Deletion Request followed by the rejection of Session Report. The UPF responds to the delete request and clears the session gracefully.

- **action { ignore | retry-terminate { max-retry** *retry_value* **} | terminate }**: Specify the action to perform based on the error cause code received in the failure response message from the UPF.
  - **ignore**—Specify to ignore the session. This FH action is applicable for N4SessionReportReq message type.
  - **retry-terminate max-retry** *retry_value* —Specify number of retry attempts to an alternate UPF. If the retry attempt fails, the session is terminated. This FH action is applicable for N4SessionEstablishmentReq message type.

    Default value: 2

    Maximum value: 5

Note If all the UPFs are in congested state, the call fails even if the action is set to **continue**.

  - **terminate**—Specify to terminate the session. This FH action is applicable for N4SessionEstablishmentReq, N4SessionModificationReq, and N4SessionReportReq message types.

    You can configure different failure handling conditions based on the procedures applicable only for the N4SessionModificationReq message type. To configure the conditions, use the following command:

    action terminate condition { handover-execution | handover-preparation | modify | idft | handover-cancel }

    Configuring the **condition** command is optional.

Note The SMF allows configuration of one or more conditions for failure handling of N4 session modifications.

    The SMF either terminates or allows the existing session to continue according to the configured conditions. For example, if any of the handover execution procedures fail during N4 modification, the SMF terminates the session.

    The cause codes 0-255 are supported. Precedence of the cause codes are in the following order:

    1. Predefined string
    2. Number
    3. Range
    4. Reject

    Reject is the default cause code.

The following table describes the configuration for cause codes:

Table 136: Configuration for Cause Codes

Cause code	Configuration
0-63	Corresponding template configuration
64-255	reject

Verifying the UPF Failure Handling Configuration

Use the **show running-config** command to view the configuration.

The following is an example output of the command.

```
show running-config profile failure-handling interface pfcp
profile failure-handling FH1
 interface pfcp message N4SessionEstablishmentReq
  cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
  cause-code system-failure action terminate
  cause-code service-not-supported action terminate
  cause-code no-resource-available action retry-terminate max-retry 3
  cause-code no-response-received action retry-terminate max-retry 1
  cause-code reject action terminate
 exit
 interface pfcp message N4SessionModificationReq
  cause-code mandatory-ie-incorrect action terminate
  cause-code session-ctx-not-found action terminate
  cause-code reject action terminate
 exit
 interface pfcp message N4SessionReportReq
  cause-code 69 action terminate
  cause-code 72-74,76,78-100 action terminate
 exit
exit
```

Configuring the Failure Profile Association

To configure the failure profile association, use the following sample configuration.

```
config
  profile upf-group  upf_group_name
    failure-profile failure_profile_name
    end
```

NOTES:

- **profile upf-group** *upf_group_name*: Specify the UPF group name.
- **failure-profile** *failure_profile_name*: Specify the UPF failure profile name.

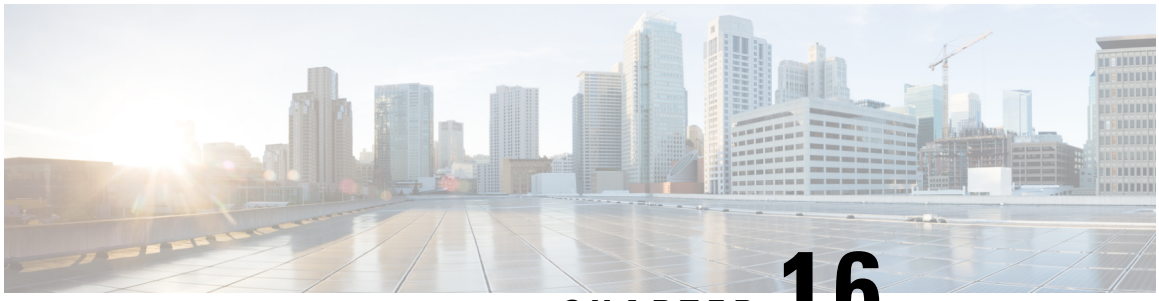
OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF supports the following disconnect reasons as part of “smf_disconnect_stats”:

- smf_sess_pdn_rel_peer_request_reject — This disconnect reason is applicable for 4G and WiFi calls.
- smf_sess_pdu_rel_peer_request_reject — This disconnect reason is applicable for 5G calls.



CHAPTER 16

Flow Failure Handling for Access and Mobility Procedures

- Feature Summary and Revision History, on page 399
- Feature Description, on page 400
- How it Works, on page 400

Feature Summary and Revision History

Summary Data

Table 137: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 138: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the QoS flow failures for access and mobility procedures. The SMF receives the QoS flow failure details as part of the following call flows from NG-RAN to N2 messages.

- Xn handover
- Service request procedures (UE and network-initiated)
- N2 handover with or without changing AMF
- N26 4G to 5G handover
- N26 5G to 4G handover

How it Works

The SMF processes N11 messages with N2 message details to determine the accepted and failed QoS flow IDs. For failed QoS flow IDs, the SMF excludes the resources locally and communicates the following information to the external interfaces:

- Sends the N4 Session Modification Request to UPF to delete the QERs, URRs, UL or DL PDRs, UL or DL FARs which are applicable to the QoS flow IDs.
- Sends the Charging Data Update Request to CHF by including multi-unit usage details for the removed URRs. If SMF receives a usage report from UPF, SMF sends this report to CHF.
- Sends the N1 N2 transfer message with N1 message details to UE as the PDU Session Modification Command.
- Based on the received Policy Control Request Triggers and SM Policy Decision last Request Rule Data, SMF sends the Rule Reports SM Policy Control Update to PCF.

Call Flows

This section describes the following call flows:

- QoS flow failure handling for Xn handover call flow
- QoS flow failure handling for N2 handover call flow
- QoS Flow failure handling for N26 4G to 5G handover call flow
- QoS flow failures for service request procedures
- PDU UE synchronization procedure
- Flow Failure Management Call Flows

QoS Flow Failure Handling During Xn Handover

This section describes the QoS flow failure handling during the Xn handover.

Figure 81: QoS Flow Failure Handling during Xn Handover

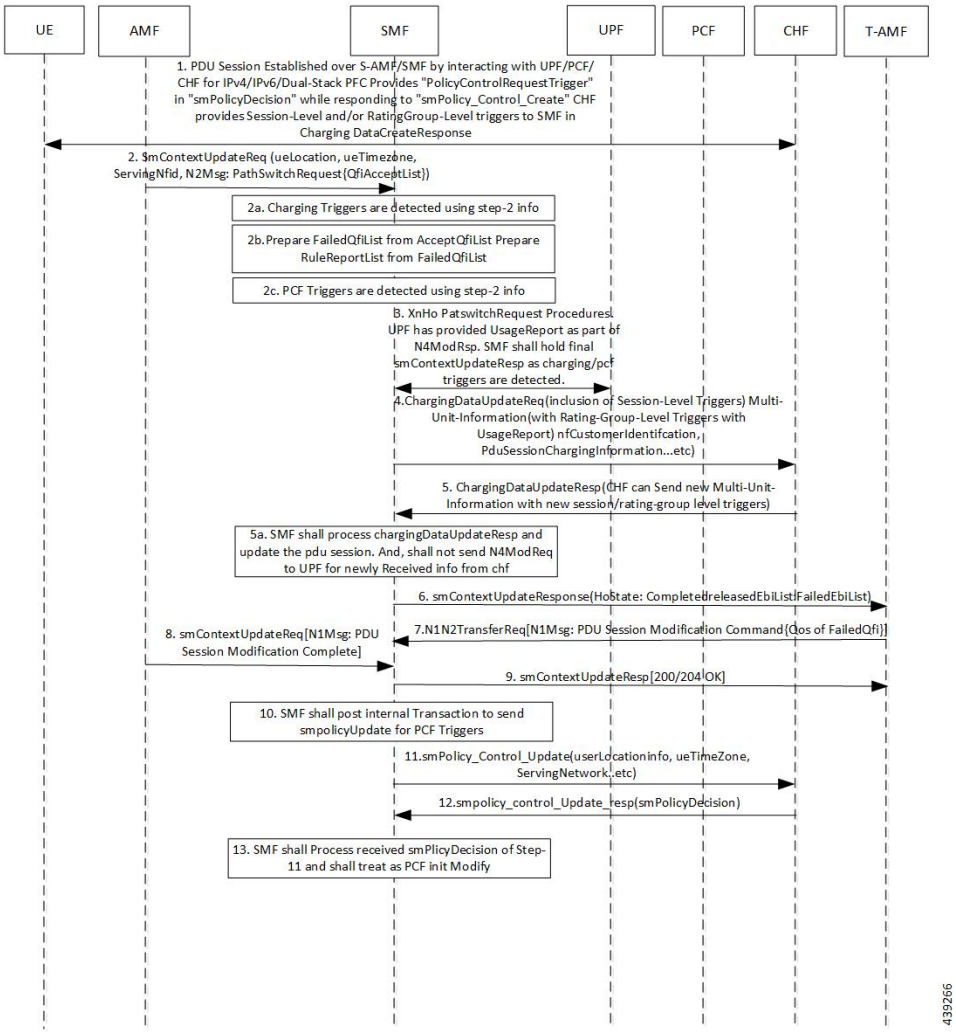


Table 139: QoS Flow Failure Handling Call Flow Description

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.
2	The AMF sends SM Context Update Request to SMF. This request includes the information on UE location, UE time zone, and N2 message path switch request with the list of the accepted QoS Flow Identifier (QFI).

Step	Description
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The SMF extracts the list of failed QFI, failed rule report, and failed EPS bearer ID (EBI) from the received list of the accepted QFIs.
2c	The PCF triggers are identified through the information that is received in Step 2.
3	For Xn handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
5	The CHF sends the Charging Data Update Response to the SMF. This response may include the multi-unit information with new session or rating-group-level triggers.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
6	The SMF sends the SM Context Update Response by including the N2 message path switch request acknowledgment and the list of failed EBI list.
7	The SMF and T-AMF process the N1 N2 Transfer Request for the PDU Session modification for the QoS about failed QFIs. The SMF includes the PDU Session Modification command to communicate the information on the QoS flow failure list to the UE.
8	The AMF sends the SM Context Update Request N1 message to the SMF to communicate about the handover completion.
9	The SMF sends the SM Context Update Response as “200/204 OK” to T-AMF. The SMF does not process the received N1 message from UE.
10	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers to send to the PCF. The SMF posts this information to communicate Rule Report for the failed QFIs or any identified armed access-side triggers.
11	The SMF sends the SM Policy Control Update to the PCF. This update includes details, such as user location information and UE time zone.
12	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
13	The SMF processes the received SM policy decision and initiates the PCF modify procedures.

QoS Flow Failure Handling During N2 Handover

This section describes the flow failure handling procedure during the N2 handover.

Figure 82: Flow Failure Handling During N2 Handover

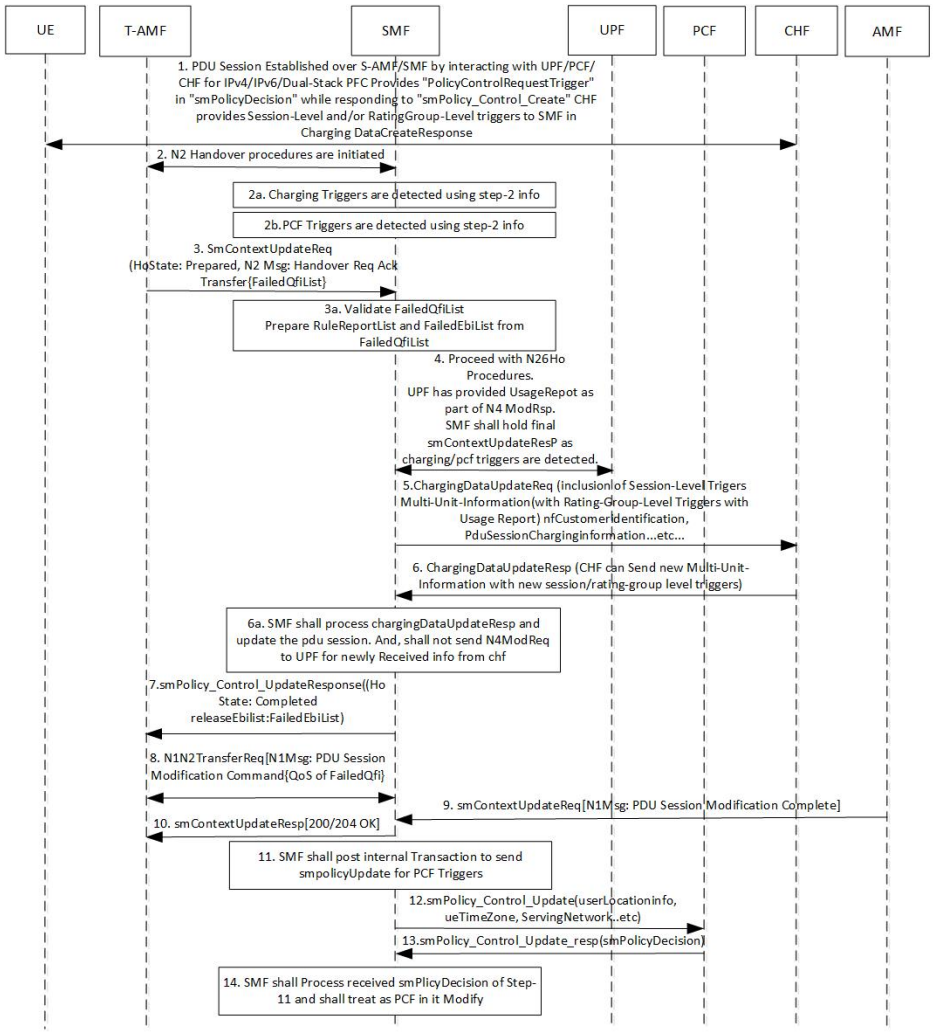


Table 140: Description for Flow Failure Handling During N2 Handover

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.
2	The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as preparing, UE location, UE time zone, target serving NF ID, and serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID.

Step	Description
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N2 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	The SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

QoS Flow Failure Handling During N26 4G to 5G Handover

This section describes the flow failure handling procedure during the N26 4G to 5G handover.

Figure 83: QoS Flow Failure Handling During N26 4G to 5G Handover

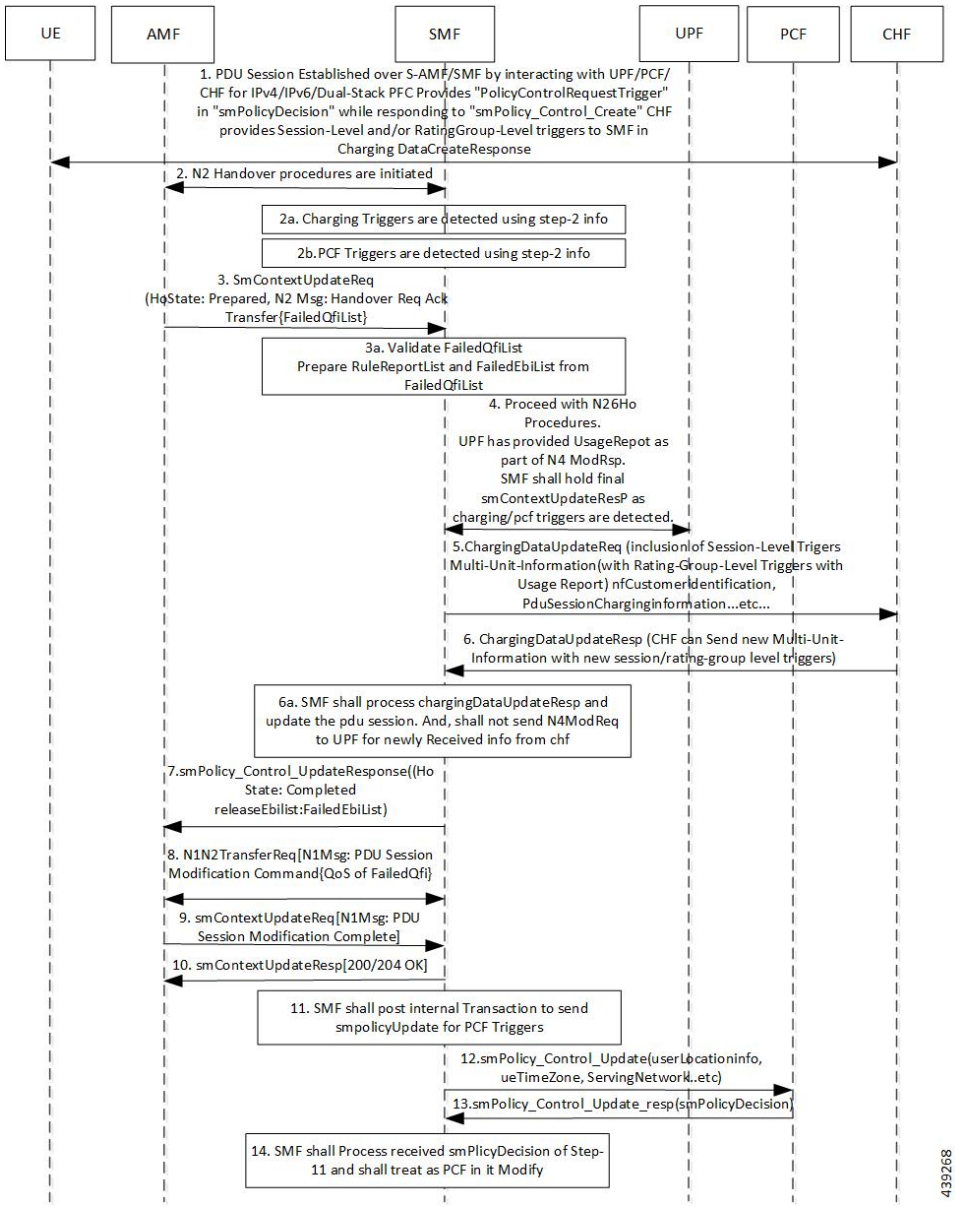


Table 141: Description for QoS Flow Failure Handling During N26 4G to 5G Handover

Step	Description
1	The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.

Step	Description
2	The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as prepared, UE location, UE time zone, target serving NF ID, serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID and the N2 message path switch request with the list of the accepted QFIs to the SMF.
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N26 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 Modification Response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with the handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	the SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

QoS Flow Failures for Service Request Procedures

The SMF supports both UE and Network Service Request procedures. For these procedures, the SMF processes the received SM Context Update Request to update the N3 tunnel path from idle to active state.

The QoS flow failures for service request procedures are handled in the same way as described in the 3GPP 23.502, Section 4.2.3.2. However, QoS flow failure list is handled with the PDU Session Setup Response Transfer N2 message, which is received as SM Context Update Response when subscriber moves from Idle to Active State.

Figure 84: PDUIM Idle to Active Mode

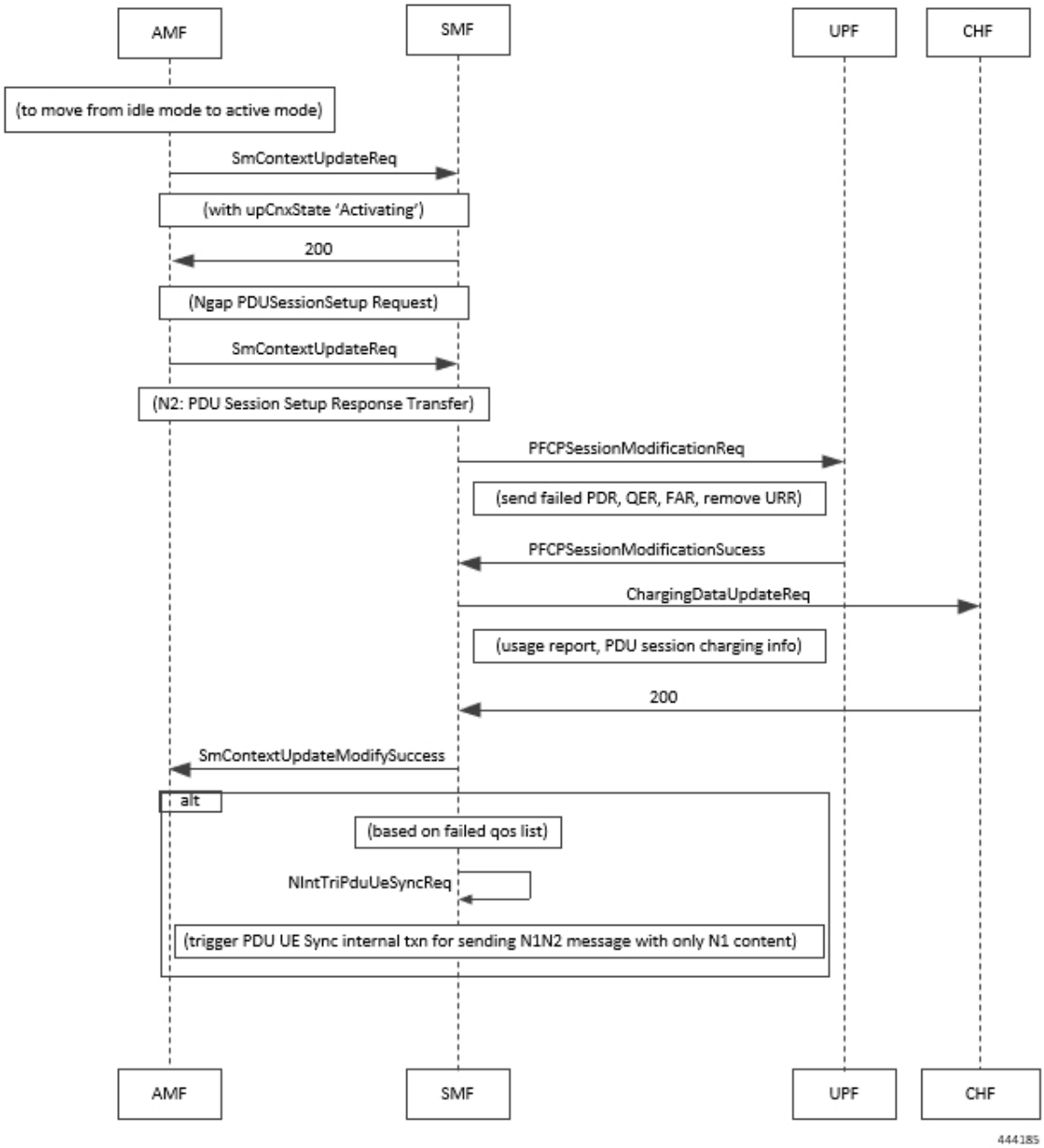


Table 142: QoS Flow Failures for Service Request Procedure

Step	Description
1	The SMF sends the SM Context Update Request message for the User Plane Connection State as Activated.
2	SMF sends 200 response along with PDU Session Setup Request towards AMF. AMF sends N2 message **PDU Session Setup Response Transfer** which contains QoS flow faliure list.
3	SMF validates failed QFIs to extract failed PCC rules and failed flows.
4	SMF updates received DL tunnel information (gNB, delete PDRs, delete QERs). After the tunnel information is updated, SMF removes URR based on failed flows and sends N4 Session Modification Request towards UPF.
5	UPF provides usage report as part of N4 Session Modification Response. SMF sends SM Context Update Response for User Plane Connection State as Activated along with released EBIs as failed EBIs and triggers internal transaction to process charging and PCF triggers.
6	SMF sends Charging Data Update Request to CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
7	SMF sends internal transaction based on failed QFIs to initiate PDU UE Sync Procedure to send N1/NAS signalling. Refer to PDU UE Sync Procedure call flow diagram for N1N2 message transfer

PDU UE Synchronization Procedure

This section describes the UE synchronization procedure.

1. PDU UE synchronization procedure in idle mode receives the failed QFIs, QoS rules and EBIs.
2. UE synchronization procedure fills N1 message PDU Session Modification command with QoS Descriptions, QoS Rules, and EPS Bearer Context from received QFI, QoS rule ID, and EBI respectively.
3. The SMF includes the created N1 container to N11 message without any N2 content.
4. The SMF sends N1N2 Transfer Request message towards AMF and starts the N1N2 retransmission timer. The SMF waits for N1N2 Transfer Response.
5. If N1N2 Transfer Success is received, the SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.

Statistics

This procedure creates statistics for the following events:

- N1N2TransferRequest Attempt
- N1 modify success
- N1 modify failure
- UE sync procedure suspend

- On resuming UE sync procedure if it was suspended by other procedure

N1N2 Retransmission

Once N1N2 retransmission timer expires, following action is taken:

1. SMF increments the N1N2 retry counter
2. SMF sends N11N1N2 Transfer Request message towards AMF and restarts the N1N2 retransmission timer. SMF waits for N1N2 Transfer Response.
3. If N1N2 Transfer Success is received, SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.
4. Once the N1N2 retry counter reaches the configured maximum number, the procedure is aborted.

Collision Case

AMF informs SMF about HO procedure by rejecting the N1N2 Transfer Request with temporary reject cause. Also any other procedure can pre-empt the UE synchronization procedure while it is awaiting N1 update from the UE.

Figure 85: Collision Case

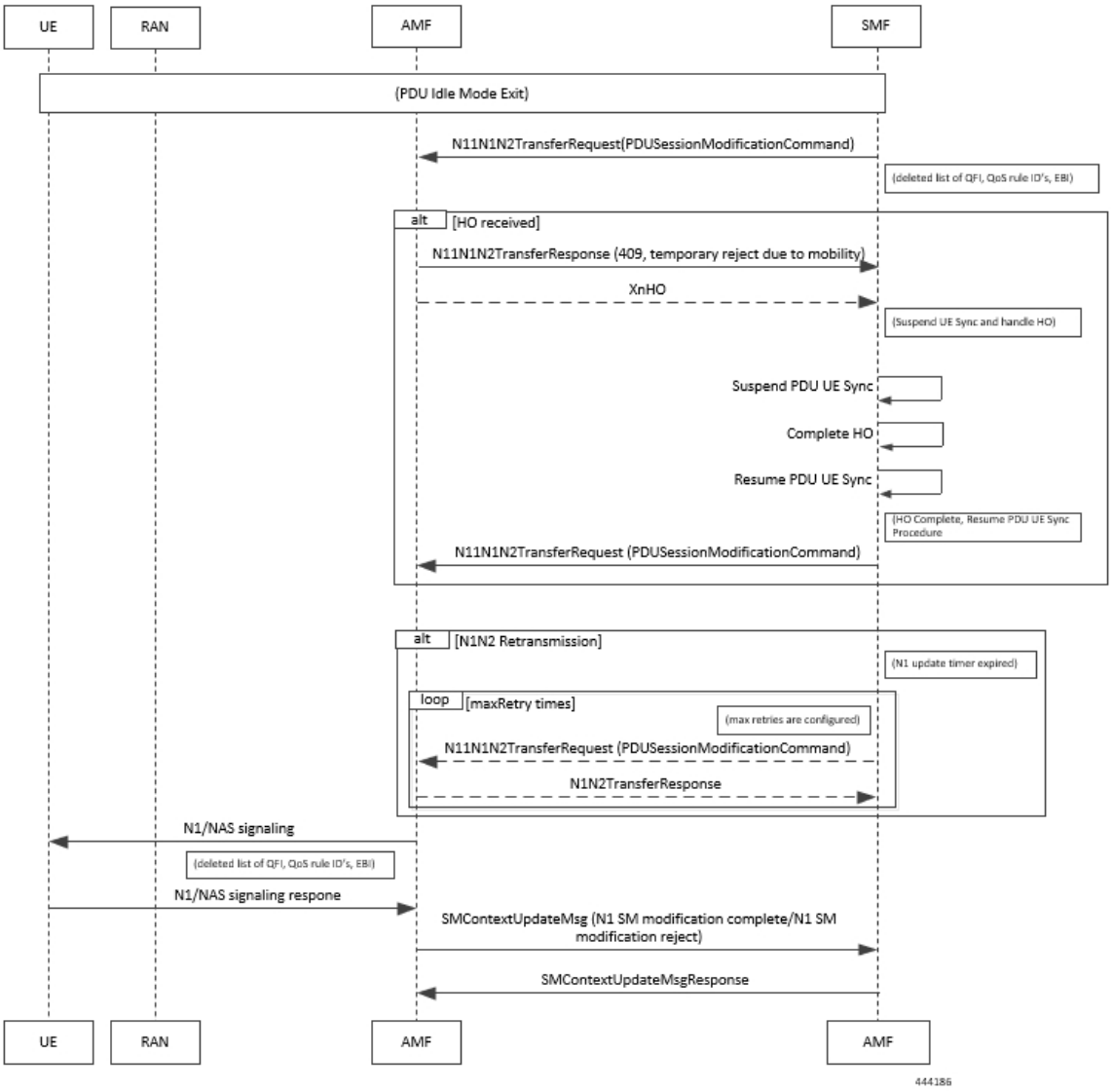


Table 143: Collision Case

Step	Description
1	If N1N2 Transfer Failure with cause as **Temporary Reject Handover Ongoing** is received, SMF awaits HO procedure to pre-empt PDU UE Sync Procedure.
2	While awaiting N1 Update or handover from UE, if any procedure (including handover) is triggered then: • If suspended by the handover procedure, it starts the N1N2 retry timer. • If aborted by PDU release or PDU setup procedure, it cleans up all the timers and aborts the N1N2 retry.

Step	Description
3	In case UE sync procedure is suspended by handover then on expiry of N1N2 Retry Timer, UE sync resumes after handover is processed.
4	On resuming if the UE sync procedure finds that the RAT has changed then it aborts the procedure and stop any timers.
5	On resuming the procedure in the same RAT the UE sync procedure reinitiates N11N1N2Transfer request message.

Handling Failed QoS Flow Identifier During PDU Setup Procedure

The SMF supports handling of the failed QoS Flow Identifier (QFI) during the PDU setup procedure.

NG-RAN rejects a QoS flow due to various reasons. When the NG-RAN node reports unsuccessful establishment of a QoS flow, the SMF uses cause value to identify the reason for the unsuccessful establishment.

Figure 86: Handling Failed QFIs During PDU Setup

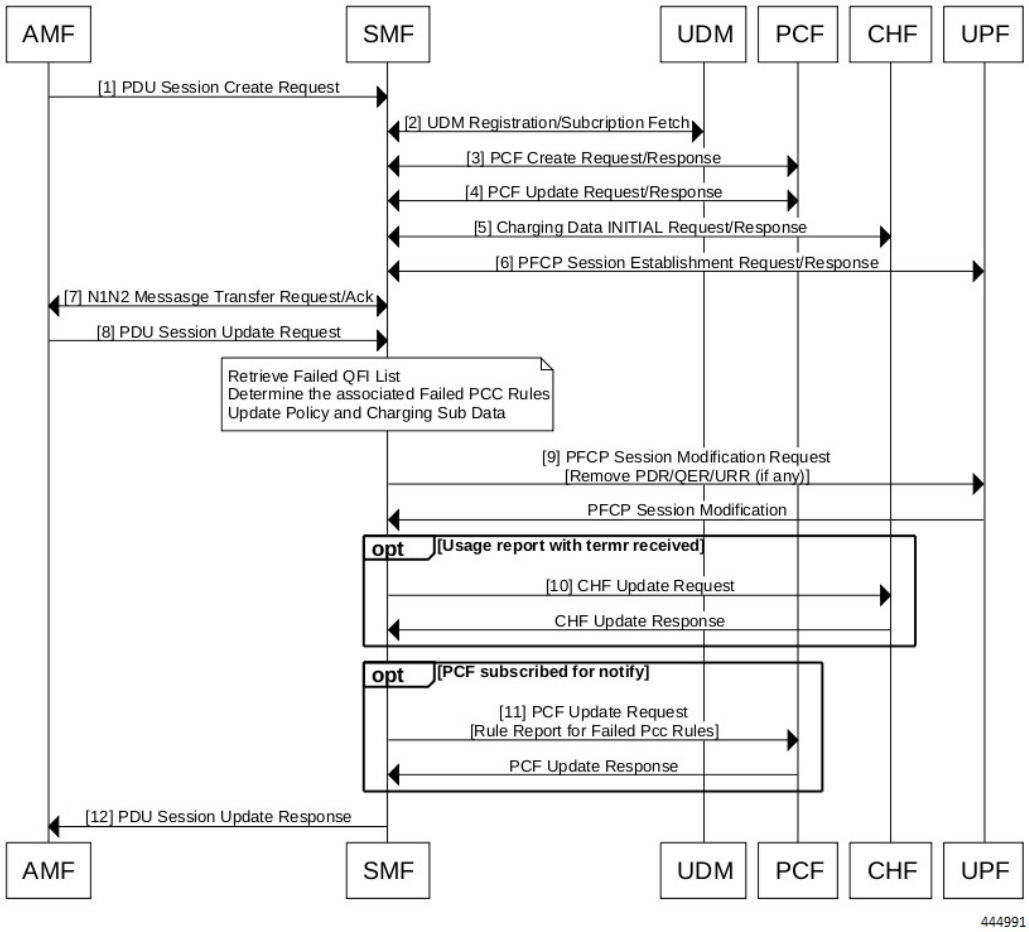


Table 144: Description for Failed QFI Handling During PDU Setup

Step	Description
1-7	The SMF, AMF, UDM, PCF, CHF, and UPF communicate with each other to perform the PDU setup procedure as defined in the 3GPP specification.
8	The AMF sends SM Context Update Request to the SMF. This request carries N2 payload “PDU Session Resource Setup Response Transfer”. This message includes the list of QoS flows failed to be established, if any, in the QoS Flow Failed to Setup List IE. The SMF marks the failed PCC rules and the charging descriptors associated with them for deletion.
9	The SMF sends PFCP Session Modification message to the UPF. This message carries Remove Packet Detection Rules (PDR), Remove QoS Enforcement Rules (QER), and Remove Usage Reporting Rules (URR) for the failed PCC rules in addition to the existing Update FAR for Downlink (DL) Tunnel Endpoint Identifier (TEID) of the successful PCC rules.
10	The SMF sends the CHF Update Request message to the CHF upon receiving a termination request. The CHF sends the CHF Update Response as an acknowledgment.
11	If the PCF has subscribed for notification on failed PCC rules, the SMF sends PCF Update Request with rule report containing the failed PCC rules dropped by the NG-RAN.
12	The SMF sends the PDU Session Update Response to the AMF. The SMF triggers internal transaction based on the failed QFI list. Then, the SMF initiates PDU UE Sync Procedure to send N1/NAS signalling. The SMF notifies the UE about the failed QoS flows using N1 messaging, and the UPF and PCF nodes about the associated failed PCC rules.

Handling Failed QoS Flow Identifier During PDU Session Modification

The SMF supports handling of the failed QoS flows over N2 interface during the PDU session modification.

If the modification of a PDU session or a QoS flow fails, the NG-RAN node falls back to the older configuration. That is, it falls back to the configuration of the session or the flow that was available before receiving the PDU SESSION RESOURCE MODIFY REQUEST message.

The SMF receives the QoS Flow Identifier for which the flow add/modify failed during the PDU SESSION RESOURCE MODIFY REQUEST.

If the new flow addition fails, the SMF performs the following:

- Removes the failed flow towards N1 (UE)
- Stops sending the failed flow-related information towards N4 (UPF)
- Stops sending the failed flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the rule report for the failed flow towards N7 (PCF).

If the modification of flow fails, the SMF performs the following:

- Replaces the old information for the failed flow towards N1 (UE)
- Stops sending the modified flow-related information towards N4 (UPF)

- Stops sending the modified flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the Rule Report for the failed flow towards N7 (PCF).

The following table captures the SMF behavior for the cause values included in the PDU Session Resource Modify Unsuccessful Transfer IE. These cause values are applicable for the PDU session modification procedure.

Cause Group	Cause Value	SMF Behavior	Comment
Radio Network Layer Cause			
	Unspecified		General
	Unknown PDU Session ID	Delete the session	N1 FiveGSM Cause reactivation requested
	Unknown QoS Flow ID	Send delete details to N1 Send PCF report about rule(s)	
	Multiple PDU Session ID Instances	Delete the session	
	Multiple QoS Flow ID Instances	Delete the session	N1 FiveGSM Cause reactivation requested
	Xn handover triggered	Act based on collision handling	
	Not supported 5QI value	Send delete details to N1 Send PCF report about rule(s)	
	IMS voice EPS fallback or RAT fallback triggered	Already supported	
Transport Layer Cause			
	Transport resource unavailable	Send delete details to N1 Send PCF report about rule(s)	
	Unspecified		
NAS Cause			
	Normal release	Delete the session	
	Authentication failure	Delete the session	
	Deregister	Delete the session	
	Unspecified	Delete the session	

Cause Group	Cause Value	SMF Behavior	Comment
Protocol Cause			
	Transfer syntax error	N1 rollback Error log fail procedure	
	Abstract syntax error (reject)	N1 rollback Error log fail procedure	
	Abstract syntax error (ignore and notify)	N1 rollback Error log fail procedure	
	Message not compatible with receiver state	N1 rollback Error log fail procedure	
	Semantic error	N1 rollback Error log fail procedure	
	Abstract syntax error (falsely constructed message)	N1 rollback Error log fail procedure	
	Unspecified	N1 rollback Error log fail procedure	
Miscellaneous Cause			
	Control processing overload	N1 rollback Error log fail procedure	
	Not enough user plane processing resources	N1 rollback Error log fail procedure	
	Hardware failure	Delete the session	
	O&M intervention	N1 rollback Error log fail procedure	
	Unknown PLMN	Delete the session	

Bulk Statistics

The following statistics provide details about the failed QoS flows over the N2 interface.

- policy_pdu_flows_total
  - total attempted
  - total succeeded

- total failed

- policy_pdu_flows_current
  - current attempted
  - current succeeded
  - current failed

Flow Failure Management Call Flows

The following call flow provides the details of the different flow failure scenarios during the EPS to 5GS handover. This call flow also describes how the SMF manages these failures and keeps the flows intact across 5GS network elements and the subscriber.

- Flow failure from source in EPS to 5GS Handover
- Flow failure from target in EPS to 5GS Handover

Figure 87: Flow Failure Management Call Flow

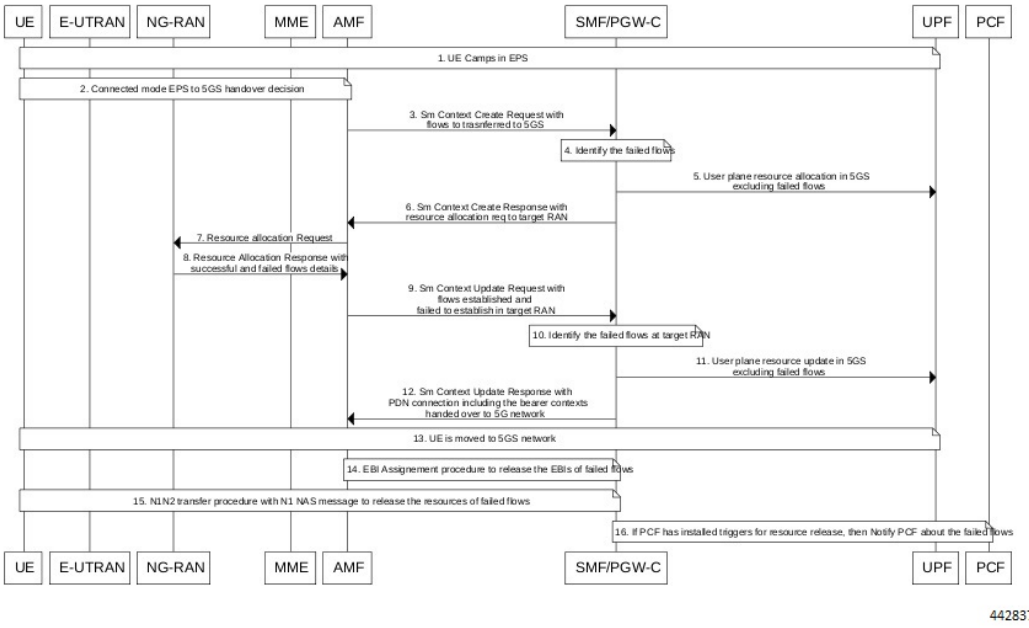


Table 145: Flow Failure Management Call Flow Description

Step	Description
1	The EPS interworking capable UE initially camps on the EPS network.
2	This step involves taking the connected mode EPS to 5GS handover decision.
3	During the EPS to 5GS handover procedure, the PDN Connection in the Sm Context Create request from the AMF carries the EPS bearer contexts to be handed over to 5GS network.

Step	Description
4	The SMF identifies the bearer contexts that were established in EPS and missing in PDN connection as failed flows.
5	The SMF performs the resource allocation in 5GS network and sends it to the UPF excluding the failed flows.
6	The SMF sends the Sm Context Create Response with resource allocation request to the target RAN.
7	The AMF forwards the resource allocation request to the NG-RAN.
8	The NG-RAN sends the resource allocation response with the details of successful and failed flows to the AMF. The target RAN node may not be able to allocate the resources for all the requested flows during EPS to 5GS handover procedure. The target RAN shares information about such failed flows in the resource allocation response.
9	The AMF sends the Sm Context Update Request with flows established and failed to establish in the target RAN.
10	The SMF identifies the failed flows at the target RAN.
11	The SMF performs the user plane resource update in 5G network excluding the failed flows.
12	The SMF sends the Sm Context Update Response with PDN connection including the bearer contexts handed over to the 5GS network.
13	The UE is moved to the 5GS network.
14	The SMF uses the EBI assignment procedure to release the EBIs of failed flows.
15	The SMF sends the N1N2 transfer request with the N1 NAS message to the UE to remove the resources of failed flows.
16	If the PCF has installed triggers to release the resources, then the SMF notifies the PCF about the failed flows.

Handling of Flow Failures from Source in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from source RAN in EPS to the 5GS handover.

Figure 88: Flow Failure Handling Call Flow (From Source in EPS to 5GS Handover)

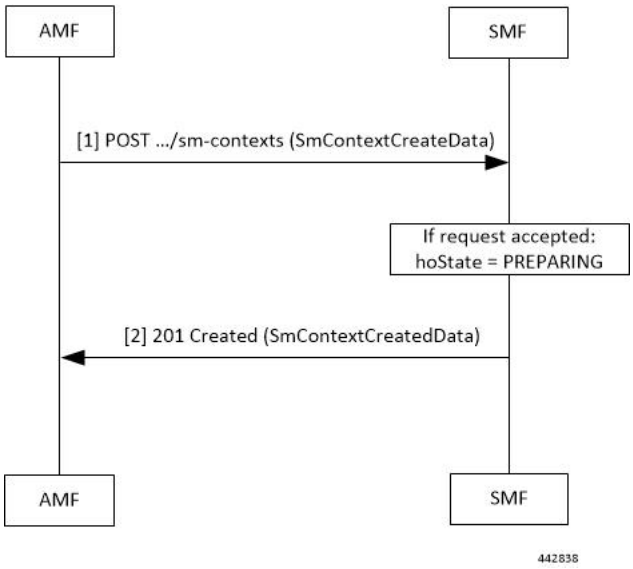


Table 146: Flow Failure Handling Call Flow Description (From Source in EPS to 5GS Handover)

Step	Description
1	The AMF sends a POST request for Sm Context Create Service, with the following additional information: • UE EPS PDN connection, including the EPS bearer contexts, representing the individual SM context resource to be created. The UE EPS PDN connection may not carry the flows which source does not want to establish in the 5GS network. • hoState attribute set to PREPARING • targetId identifying the target RAN Node ID and TAI based on the Target ID IE received in the Forward Relocation Request message from the source MME.
2	If the corresponding PDU session is detected based on the EPS bearer contexts and the handover of the PDN connection to 5GS network is possible, then the SMF returns a 201 Created response including the following information: • hoState attribute set to PREPARING and N2 SM information to request the target RAN to assign resources to the PDU session, excluding the flows which are not received in the UE EPS PDN connection. • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • allocatedEbiList containing the EBIs allocated to the PDU session. The POST response includes the Location header and the URI of the created SM context resource. The AMF stores the association of the PDU Session ID and the SMF ID, and the allocated EBIs associated to the PDU Session ID.

Handling of Flow Failures from Target in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from target RAN in EPS to the 5GS handover.

Figure 89: Flow Failure Handling Call Flow (From Target in EPS to 5GS Handover)

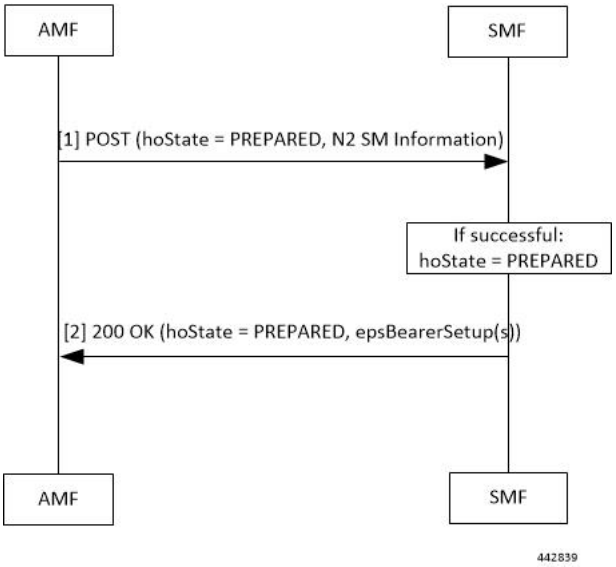


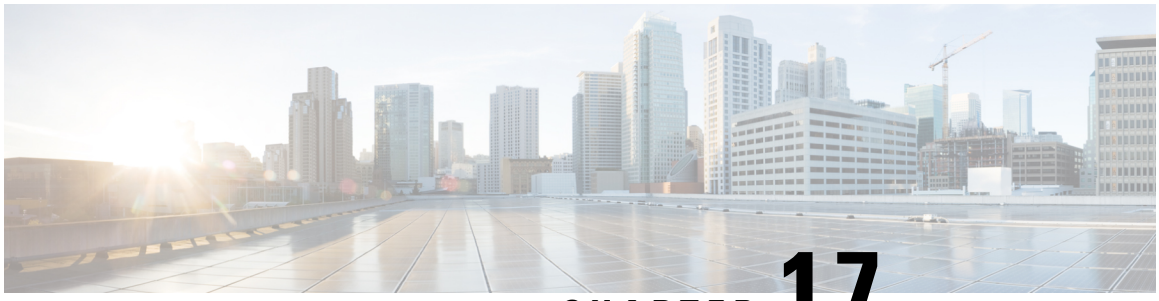
Table 147: Flow Failure Handling Call Flow Description (From Target in EPS to 5GS Handover)

Step	Description
1	The AMF updates the SM context in the SMF by sending POST request with the following information: • hoState attribute set to PREPARED • N2 SM information received from the target RAN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session (that is, GTP-U F-TEID of the target RAN for downlink traffic), if the target RAN succeeded in establishing resources for the PDU session; the target RAN may not be able to establish resources for all the flows; the target RAN includes such failed flows information
2	If the target RAN succeeded in establishing resources for the PDU sessions, the SMF sets the hoState attribute to PREPARED and returns a 200 OK response including the following information: • hoState attribute set to PREPARED • the epsBearerSetup IEs containing the list of EPS bearer contexts successfully handed over to the 5GS and the CN tunnel information for data forwarding, generated based on the list of accepted QFIs received from the RAN; This is the final list of flows handed over to the 5GS network.

Standards Compliance

The QoS Flow Failure Handling for Access and Mobility Procedures feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*



CHAPTER 17

GTPP Endpoint

- Feature Summary and Revision History, on page 421
- Feature Description, on page 422
- Information Elements Support, on page 425
- Standards Compliance, on page 425
- Limitations, on page 426
- Configuring the GTPP Profile, on page 426
- Configuring the GTPP Endpoint, on page 429

Feature Summary and Revision History

Summary Data

Table 148: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	Not Applicable

Revision History

Table 149: Revision History

Revision Details	Release
First introduced.	2023.03.0

Feature Description

The GTPP Endpoint is an App-infra-based service that enables the GPRS Tunneling Protocol Prime (GTPP) protocol functionality for the SMF service. The SMF with Legacy Interfaces supports the GTPP Charging (Gz) interface in the GTPP Endpoint.

For offline charging, the Gz is the reference point from a Charging Data Function (CDF) to the CGF for transporting of CDRs.

The GTPP Endpoint provides the following support to the SMF service:

- Handles the usage and event accounting at a Bearer level and the accounting information gets stored as part of the subscriber session.
- Generates CDR content from this accounting information and then transfers to the GTPP Endpoint. The GTPP Endpoint is responsible for encoding the received CDRs into ASN.1 (based on the configured dictionary).
- Sends the received CDRs to the CGF server using the GTPP protocol.

For more information on this feature, see the UCC 5G SMF Configuration and Administration Guide > GTPP Endpoint chapter.

Charging Related Transfers

Each Charging Data Function (CDF) has an O&M-configurable address list of Charging Gateway Function (CGFs) to which it can send its CDRs. The list is organized in CGF address priority order. If the primary CGF is not available, then the CDF sends the CDRs to the secondary CGF and so on.

Each CDR generating function only sends records to the CGF(s) of the same PLMN, not to CGF(s) located in other PLMN.

Each CGF in the PLMN must know the other CGFs' network addresses to recommend another CGF address in case of redundancy. This is achieved by O&M configuration facilities that enable each CGF to have a configurable list of peers' CGF addresses.

CDR Transport through GTPP

GTPP delivers Charging Dara Records (CDR) from the Charging Data Function (CDF), which generates CDRs to the Charing Gateway Function CGF(s). The GTPP protocol is required if the CGF resides outside the CDFs. It utilizes some aspects of GTP, which is used for packet data tunnelling in the backbone network.

GTPP operates on the Gz interface and peforms the following functions:

- Transfers CDR between the CDF and the CGF.
- Redirects CDRs to another CGF.
- Detects communication failures between the communicating peers, using echo messaging.
- Advertises to peers about its CDR transfer capability. For example, after a period of service downtime.

- Prevents duplicate CDRs that might arise during redundancy operations. If configured, the CDR duplication prevention function is carried out by marking potentially duplicated CDR packets, and delegating the final duplicate deletion task to a CGF, or the Billing Domain.

Path Protocol

GTPP uses path protocol to transport CDRs from CDF to CGF over the Gz interface to facilitate charging. The UDP path protocols is supported for GTPP:

Note Path Protocol TCP is not supported

- Ports for signalling the request messages:
  - The UDP Destination Port with the server port number 3386 is reserved for GTPP. Alternatively, another port can be used as configured by O&M.
  - The UDP Source Port is a locally allocated port number for sending network element.
- Ports for signalling the response messages:
  - The UDP Destination Port is the value of the Source Port of the corresponding request message.
  - The UDP Source Port is the value from the Destination Port of the corresponding request

GTPP Message Types

GTPP defines a set of messages between two associated nodes. The following table lists GTPP messages.

Table 150: GTPP Messages

Message Type Value (Decimal)	GTPP Message
1	Echo Request
2	Echo Response
3	Version Not Supported.
4	Node Alive Request
5	Node Alive Response
6	Redirection Request
7	Redirection Response
240	Data Record Transfer Request
241	Data Record Transfer Response

Endpoint GTP Prime

The Endpoint GTP Prime is primarily used to set the storage size limit (default 1 GB), which is applicable when **k8s use-volume-claim Pod** is set to true. Though gtpp-profiles configuration alone brings up gtpp-ep pod, it is recommended to configure gtpprime endpoint as well, with basic configuration such as **storage**, or **replica**. This configuration is used by the gtpp-ep pod.

Ensure to configure GTPP profiles charging agent ip address and ports in the Endpoint under the Gz interface.

Note The **gtpp-ep** always ignores **nodes** config. When **k8s single-node** is set to false, it spawns 2 replicas of gtpp-ep in the Active or Standby mode independent of replicas and nodes configuration.

GTPP Resiliency

The GTPP endpoint provides resiliency by supporting CDR archiving and file storage.

CDR Archiving

In an overload of CDRs scenario, the CGF server becomes slow in providing a response. This scenario leads to unacknowledged CDRs due to sendReqList buffer being full and then the CDRs drop. To avoid the CDR drop in such a case, the GTPP endpoint enqueues new CDRs into the archive list.

GTPP performs the CDR archiving in the following way:

- The archive list flush happens in a paced manner depending on the network load condition.
- After all the CGFs become inactive or due to back-to-back switchovers, an archive record is written into HDD in the paced manner to avoid losing the archived CDRs.
- Archive list is replicated on standby GTPP endpoint pod.

Note

- The archive list is maintained per GTPP profile level. The maximum size of the archive list is 5M.
- After reaching the maximum configured size, the oldest record is purged and a new record is added.
- Archive list gets replicated on the standby pod. When the active pod is inactive, the standby pod becomes the active pod and starts processing the CDRs to retain all the archive records.

CDR File Storage

GTPP performs the CDR file storage in the following way:

1. When all the CGFs are inactive, all the CDRs are written into a file in HDD on the active GTTP endpoint.
2. The CDRs are stored on the standby GTPP endpoint.
3. After the inactive CGF becomes active, the CDRs are read from the file on the active GTPP endpoint and sent to the CGF.

4. After all the CDRs are read from one file, the file gets deleted from the active GTPP endpoint. Then, the file delete replication information is sent to the standby GTPP endpoint.
5. Standby GTPP endpoint deletes the file from HDD.

Note During the CDR reading from HDD process, when some CDRs are sent to CGF and some CDRs are still in the file and the active GTPP endpoint becomes inactive, then the last read file is sent from the new active GTPP endpoint pod. The CGF receives various duplicate CDRs in such a case.

Information Elements Support

Following are the Information Elements (IEs) supported for the Gz support with GTPP feature.

Table 151: TLV and TV IEs

Information Element	Description
TLV Information Elements	
254	Address of Recommended Node
253	Requests Responded
252	Data Record Packet
251	Charging Gateway Address (this IE is also used in TS 29.060 [200])
250	Sequence numbers of Cancelled Packets
249	Sequence numbers of Released Packets
TV Information Elements	
127	Charging ID
126	Packet Transfer Command

Standards Compliance

The GTPP endpoint support complies with the following Charging specific 3GPP standards:

- *3GPP TS 32.251 "Telecommunication management;Charging management;Packet Switched (PS) domain charging"*
- *3GPP TS 32.295 "Telecommunication management; Charging management; Charging Data Record (CDR) transfer"*
- *3GPP TS 32.297 "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer"*

- *3GPP TS 32.298 "Telecommunication management; Charging management; Charging Data Record (CDR) parameter description"*

Limitations

The following are the limitations in the SMF with Diameter Interfaces Charging feature:

- The SMF with Diameter Interface does not support Local storage mode, TCP, and Redirect Request or Responses.
- The SMF with Diameter Interfaces supports only the custom24 CDR Dictionary.
- In case of switchover, only the new CDR Send Request buffer is checked on the new standby GTPP pod.
- In case of switchover, only the new archive is checked on the new stand by GTPP pod.
- In case of double fault, old archive CDR and old Send Request buffer are lost.

Configuring the GTPP Profile

To configure the GTPP profile, use the following configuration:

```
config
   profile gtpp-profile profile_name gtpp
      dictionary
      ignore  ignore_value
      instance-id
         charging-agent address IPv4_adress port UDP_port
         server{ cgf address IPv4_adress max-cdrs max_cdrs { node-alive Enable
| Disable}
               port UDP_port priority priority deadtime time_interval
               echo-interval  echo_interval timeout timeout_val max-retry
               max_retry max-pdu-size max_pdu_size wait-time time_interval }
      local-storage
      mode
         local
         streaming-parallel
      cgf-server-redundancy-support
     exit
  exit
exit
```

NOTES:

- **dictionary**: Specify a dictionary for ASN.1 based encoding of a CDR.
- **ignore** *ignore_value*: Specify the configuration to ignore the echo-rc-change. This CLI control option provides a flexibility to detect a CGF path failure due to a change in the echo response RC.
- **instance-id**: Specify the instance ID of a GR instance.
    - **charging-agent**: Configure the charging agent.

- **address***IPv4_address*: Specify the IP address of the interface configured within the endpoint that is used to transmit CDR records to the CGF.
- **port**: Specify the UDP port.

Note The Charging agent IP address and port configured in GTPP profiles should also be configured in the endpoint gtpprime under the Gz interface. The Runtime configuration update of the Charging agent IP address and port is not recommended. Ensure to add new profile with new Charging agent IP address and port.

- **server**: Configures server details.
  - **cgf**: Configure the CGF server with the following parameters:
    - **address** *IPv4_address*: Enter the IPv4 address of CGF server, using dotted-decimal notation range.
    - **max**: Configure maximum number of unacknowledged CDRs for a CGF. Must be an integer ranging from 1 to 2000.

Note The runtime configuration change of **max** is not recommended. Follow the Method of procedure:

1. Delete the **cgf** having old **max** and then commit the change.
2. Add the **cgf** again with a new **max** value.

    - **node-alive Enable | Disable** : Enable or disable sending Node Alive Request to a GTPP Server (such as CGF).
    - **port**: Specify which port that the CGF is using.
    - **priority**: Specify the relative priority of this server when system is selecting which CGF server to use.

- **deadtime**: Configure the deadtime in seconds. Must be an integer ranging from 1 to 65535. Default value is 120.
- **max-cdrs**: Designate the maximum number of CDRs in a GTPP message. Must be an integer ranging from 1 to 255.
- **max-pdu-size**: Designate the maximum size of the PDU, in bytes. Must be an ranging from 1024 to 1460.
- **timeout**: Specify the number of times the system attempts to communicate with a CGF that is not responding.
- **wait-time**: Specify the time to wait before sending the GTPP request.

- **local-storage**: Specify local storage details.
- **mode**: Specify a storage mode to be used.
  - **local**: Specify the use of HDD to store CDRs
  - **streaming-parallel**: Specify the use of HDD to store CDRs, if CGF fails. When CGF comes up, stream the CDRs to the CGF. Streaming is in a parallel and newly generated CDRs are sent to CGF along with CDRs streamed from HDD.
- **cgf-server-redundancy-support**: Enable or disable the CGF server redundancy support per GTPP profile. By default this configuration is disabled.

Configuration Example

The following is an example configuration for GTPP profile.

```
profile gtpp-profile pf2 gtpp
 dictionary custom24
 mode       streaming
 cgf-server-redundancy-support disable
 instance-id 1
  charging-agent
   address 10.10.10.205
   port    3386
  exit
  server
   max-pdu-size  1460
   timeout       30
   max-retry     3
   max-cdrs      5
   wait-time     30
   echo-interval 60
   deadtime      120
   cgf address 10.10.10.80 port 3386 max 100 priority 1 node-alive disable
   cgf address 10.10.10.90 port 3386 max 100 priority 2 node-alive disable
  exit
 exit
exit
```

Verifying GTPP Profiles

Use the **show running-config profile gtpp-profile pf2 gtpp** command to verify the GTPP Profile configuration.

The following is an example output of the show running-config profile gtpp-profile pf2 gtpp command.

```
profile gtpp-profile pf2 gtpp
 dictionary custom24
 mode       streaming
 cgf-server-redundancy-support disable
 instance-id 1
  charging-agent
   address 10.10.10.205
   port    3386
  exit
  server
   max-pdu-size  1460
   timeout       30
   max-retry     3
```

```
   max-cdrs      5
   wait-time     30
   echo-interval 60
   deadtime      120
   cgf address 10.10.10.80 port 3386 max 100 priority 1 node-alive disable
   cgf address 10.10.10.90 port 3386 max 100 priority 2 node-alive disable
  exit
 exit
exit
```

Configuring the GTPP Endpoint

Note

- GTPP-EP pod uses this configuration.
- GTPP-EP pod always ignores nodes configuration.
- When the **k8s single-node** is set to **`false`**, it spawns two replicas of a GTPP-EP pod in active or standby mode, which is independent of replicas and nodes configuration.
- When the **k8s single-node** is set to **`true`**, the configured replicas have its impact.
- When the **k8s use-volume-claim** is set to **`true`**, endpoint GTP prime is used to set the storage size limit. Default value of storage size limit is one GB.
- When the system is up and running, we can't change the storage size.

To configure a GTPP endpoint, use the following commands:

```
config
 instance instance-id instance_id
  endpoint gtpprime
     storage storage_capacity
     replicas replicas_count
     nodes nodes_count
     interface Gz
       vip-ip   vip_ip vip-port vip-port vip-interface vip-interface vrf vrf
     end
```

NOTES:

- **endpoint gtpprime** : Specifiy the following parameters to configure an endpoint:
  - **storage** *storage_capacity*—Specify the storage size of persistent volume in GB. Must be an integer in the range of 1-100.

Note CLI doesn't allow changing storage size while the system is running. To change the storage size, bring the system down first.

  - **replicas** *replicas_count*—Specify the number of replicas per node. Must be an integer.
  - **nodes** *nodes_count*—This property is ignored. You may skip configuring it.

- **interface Gz** : Configure the Gz interface details, such as vip IPv4 address, vip port, vip interface, and virtual routing and forwarding details.

Note When the system is active and under the Gz Interface, if there are any add or update **vip** configurations to use new values, ensure to restart the **udp-proxy**.

Configuration Example

The following is an example configuration for the endpoint gtppprime configuration:

```
instance instance-id 1
 endpoint gtpprime
  replicas 1
  nodes    1
  storage  1
  interface gz
   vip-ip 10.10.10.205 vip-port 7202 vip-interface v303 vrf GTPP-VRF
  exit
 exit
exit
```

Verifying GTPP Endpoints

Use the **show gtpp-ep endpoints** command to verify the GTPP Enpoints.

The following is an example output of the show gtpp-ep endpoints command.

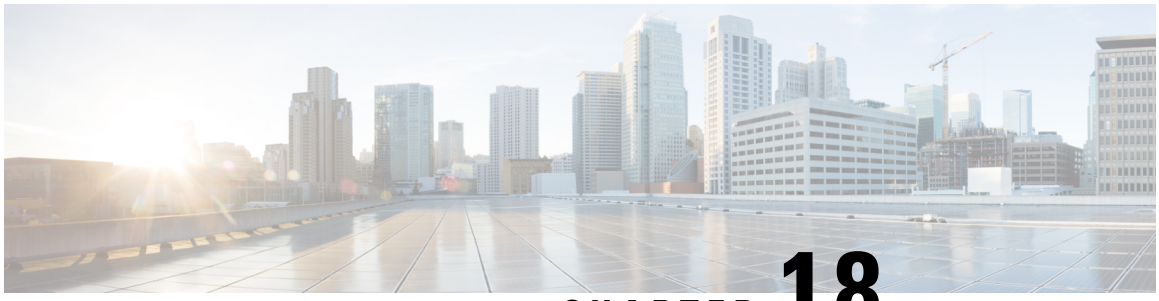
```
result List of gtpp pods with their names and IPs
gtpp-ep-0  192.168.42.116
gtpp-ep-1  192.168.42.126
```

Verifying GTP Prime Configuration

Use the **show running-config instance instance-id 1 endpoint gtpprime** command to verify the GTP Prime configuration.

The following is an example output of the show running-config instance instance-id 1 endpoint gtpprime command.

```
instance instance-id 1
 endpoint gtpprime
  replicas 1
  nodes    1
  storage  1
  interface gz
   vip-ip 10.10.10.205 vip-port 7202 vip-interface v303 vrf GTPP-VRF
  exit
 exit
exit
```



CHAPTER 18

Handover Procedures

- Feature Summary and Revision History, on page 431
- Feature Description, on page 432
- 4G to 5G Data Session Handover, on page 432
- CHF and PCF Integration for Access and Mobility Procedures, on page 447
- Inter gNodeB Handover, on page 457
- Wi-Fi Handover, on page 470

Feature Summary and Revision History

Summary Data

Table 152: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 153: Revision History

Revision Details	Release
Added support for an alternate RAT tunnel creation for 5G and Wi-Fi.	2023.03.0
FB Call Continuity Cause Code Expansion	2021.02.2

Revision Details	Release
Added support for: • Configuring calls with handover indication. • UE Local IP Address and UE UDP Port IEs in GTPC messages. • User Location Information (ULI) reporting.	2021.02.0
TFT Handling for Wi-Fi Handovers is supported.	2021.01.0
The Wi-Fi to 5GS Handover with EPS Fallback feature is fully qualified in this release.	2020.02.2
The Wi-Fi to 5GS Handover with EPS Fallback feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

This chapter describes the different handover procedures performed by SMF compliant to the 3GPP specifications.

4G to 5G Data Session Handover

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

For UEs, the SMF supports both 5G and 4G NAS to connect to E-UTRAN and 5G core network. The SMF includes the EPS interworking support and acts as PGW-C+SMF. The SMF uses the S5/S8 interface to receive the 4G Session Creation Request. Gx, Gy, or Gz interfaces, used for 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the NPCF and NCHF.

After a PDU session creation on PGW-C+SMF through E-UTRAN, MME, and S-GW, the SMF performs the 4G to 5G data session handover.

Alternate RAT Tunnel Creation for 5G

SMF creates an alternate RAT tunnel during 5G sessions for the 5G PDU establishment scenarios. This tunnel is reused when a subscriber moves to another RAT during handover.

Note Creation of an alternate RAT tunnel is a prerequisite for the inter-PLMN handover support.

How it Works

To interwork with EPS, a UE that supports both 5GC and EPS NAS works in one of the following modes:

- Single-registration Mode—In this mode, the UE has only one active MM state, which is either the RM state in 5GC or EMM state in EPS. In addition, this state is either in 5GC NAS mode or in EPS NAS mode when connected to 5GC or EPS, respectively.
- Dual-registration Mode—In this mode, the UE handles independent registrations for 5GC and EPS using separate RRC connections. The UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

Alternate RAT Tunnel Creation for 4G, 5G, and Wi-Fi

SMF creates an alternate RAT tunnel when the inter-PLMN handover CLI is enabled under the DNN profile. In addition, SMF creates this tunnel based on meeting the specific conditions. The following table lists the conditions for creation and non-creation of this tunnel.

Table 154: Conditions for Alternate RAT Tunnel Creation and Non-Creation

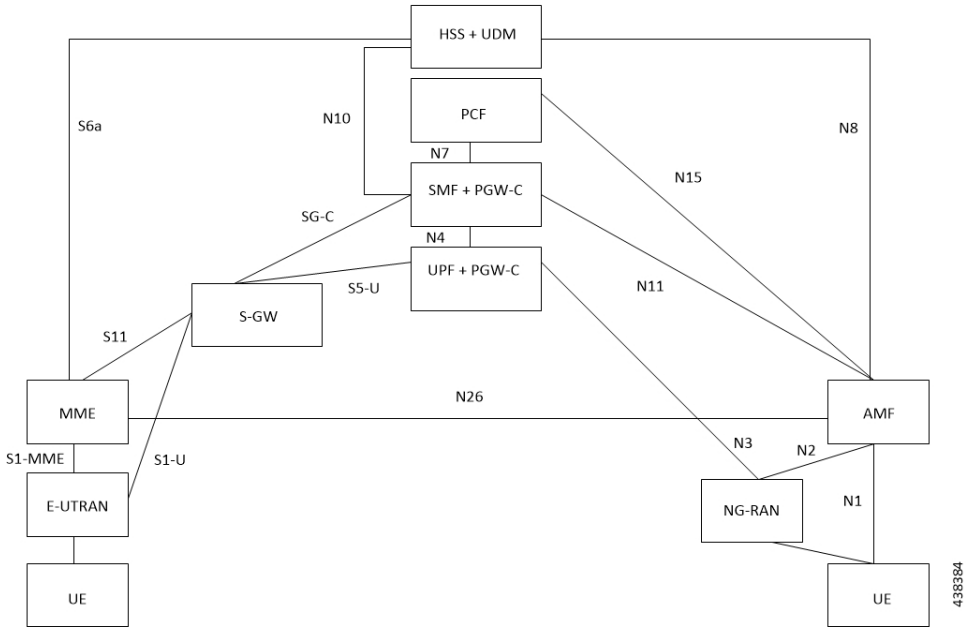
Create Session Request	N11 SMContext Create	Subscription Data	Alternate RAT Tunnel Creation
	epsInterworkingInd’: ‘WITH_N26’	dnnInfo->IwkEpsInd=true	Yes
	epsInterworkingInd’: ‘WITH_N26’	dnnInfo->IwkEpsInd=false	No
	epsInterworkingInd’: ‘WITHOUT_N26’	dnnInfo->IwkEpsInd=false	No
	epsInterworkingInd’: ‘WITHOUT_N26’	dnnInfo->IwkEpsInd=true	No
IWK_5GS indication flag=true, pduSessionId received from UE	Yes	dnnInfo->IwkEpsInd=true	Yes
IWK_5GS indication flag=true, pduSessionId received from UE	No	dnnInfo->IwkEpsInd=false	No
IWK_5GS indication flag=false, pduSessionId not received from UE	Yes	dnnInfo->IwkEpsInd=false	No

Create Session Request	N11 SMContext Create	Subscription Data	Alternate RAT Tunnel Creation
IWK_5GS indication flag=false, pduSessionId not received from UE	No	dnnInfo->IwkEpsInd=true	No

Architecture

This section describes the network architecture for the EPS-5G Core interworking.

Figure 90: Network Architecture for the EPS-5G Core Interworking



Call Flows

This section describes the following call flows.

- EPS to 5G Handover with N26 Interface – Preparation Call Flow
- EPS to 5G Handover with N26 Interface – Execution Call Flow
- UE Idle Mode Mobility from EPS to 5GS using N26 Interface

EPS to 5G Handover with N26 Interface – Preparation Call Flow

This section describes the call flow of the preparation of the EPS to 5G Handover with the N26 interface.

Figure 91: Preparation Call Flow for the EPS to 5G Handover with the N26 Interface

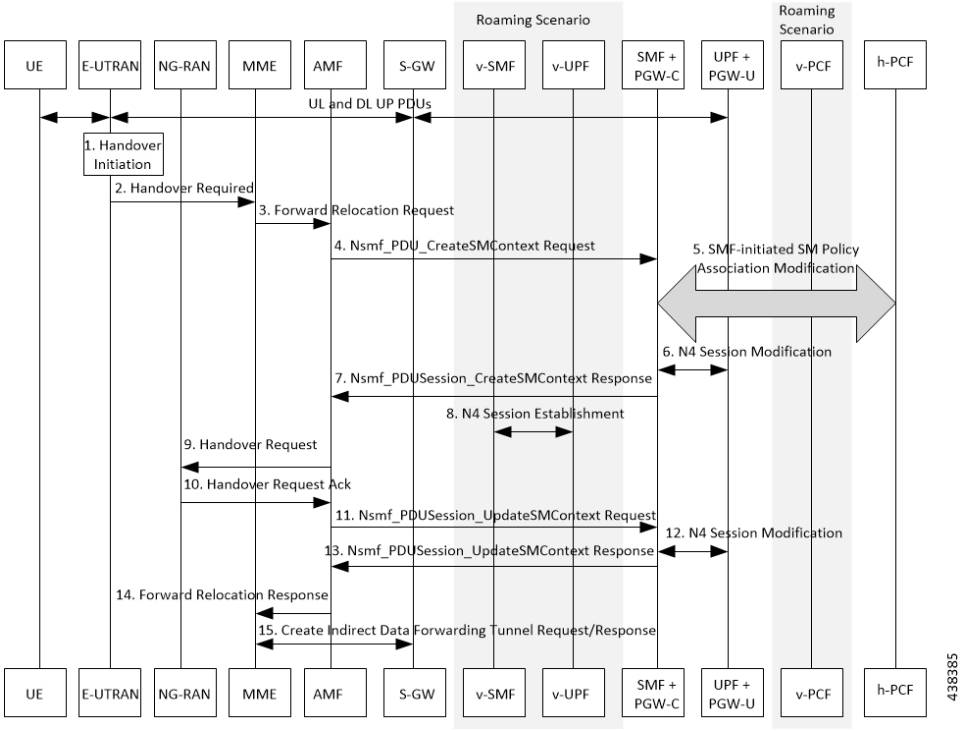


Table 155: Preparation Call Flow Description for the EPS to 5G Handover with the N26 Interface

Step	Description
1	Call handover initiation starts from UE and E-UTRAN toward each other, proceeds from E-UTRAN to the S-GW. Then for roaming calls, call handover initiation proceeds from S-GW to the UPF+PGW-C-U.
2	The E-UTRAN sends the Handover Call Request to the MME.
3	The MME forwards the Relocation Request to the AMF.
4	The AMF invokes the NsmfPDUSessionCreateSMContext service operation on SMF. The PGW-C+SMF address identifies this service operation. The service operations can be UE EPS PDN Connection, AMF ID, or Direct Forwarding Flag. The AMF then indicates the handover preparation to avoid switching the UP path. The SMF searches for the corresponding PDU session that is based on EPS Bearer Contexts. The AMF includes Direct Forwarding Flag to inform the SMF of the applicability of indirect data forwarding.
5	If you have deployed the dynamic PCC, the SMF+PGW-C initiates the SMF-initiated SM Policy Modification toward the PCF. **Important** Cisco SMF does not support this step
6	The PGW-C+SMF sends the N4 Session Modification to PGW-U+UPF to establish the CN tunnel for a PDU Session. The PGW-U+UPF receives the uplink packets from NG-RAN. This step involves creating uplink PDRs and FARs for the 5G session along with the QFIs that are mapped from the existing 4G bearers.

Step	Description
7	The PGW-C+SMF sends a NsmfPDUSessionCreateSMContext Response to the AMF. This response includes PDU Session ID, S-NSSAI, and N2 SM Information. The N2 SM Information includes PDU Session ID, S-NSSAI, QFIs, QoS Profiles, EPS Bearer Setup List, mapping between EBIs and QFIs, CN Tunnel information, and cause code details. The SMF includes mapping between EBIs and QFIs as the N2 SM Information container. If the PGW-C-C+SMF determines that session continuity from EPS to 5GS is not supported for the PDU session, then the PGW-C-C+SMF does not provide the Session Manager information for the corresponding PDU session. However, the PGW-C-C+SMF includes the cause code details for rejecting the PDU session transfer in the N2 SM information.
8	The V-SMF and V-UPF establish an N4 session with each other.
9	The AMF sends the Handover Request to NG-RAN.
10	The NG-RAN sends an acknowledgment for the received Handover Request to the AMF.
11	The AMF sends a NsmfPDUSessionUpdateSMContext Request, T-RAN SM N3 forwarding information list message to the SMF for updating the N3 tunnel information. The NsmfPDUSessionUpdateSMContext request includes a PDU Session ID, S-NSSAI, and N2 SM Information. The tunnel information exists in the NGAP IE DL Forwarding UP TNL Information of the Handoff Request Acknowledgment that is received from NG-RAN.
12	The SMF+PGW-C performs the N4 session modification toward UPF+PGW-U to create the indirect tunnel to forward the DL data from eNodeB to NG-RAN. This step includes creating UL PDRs for the redirected DL data and associating FARs with them to forward the FARs to NG-RAN. The mapping of these PDRs and FARs is based on QFI and the corresponding bearer ID.
13	The PGW-C+SMF sends the NsmfPDUSessionUpdateSMContext Response to the AMF. This response includes PDU Session ID, EPS Bearer Setup List, and CN tunnel information for data forwarding. At this point, the indirect tunnels are established for DL data forwarding.
14	The AMF sends the Forward Relocation Response to the MME.
15	The MME sends the creation request for the indirect data forwarding tunnel to the S-GW. The S-GW sends the response for the indirect data forwarding tunnel to the MME.

EPS to 5G Handover with N26 Interface – Execution Call Flow

This section describes the call flow of the execution of the EPS to 5G Handover with the N26 interface.

Figure 92: Execution Call Flow for the EPS to 5G Handover with the N26 Interface

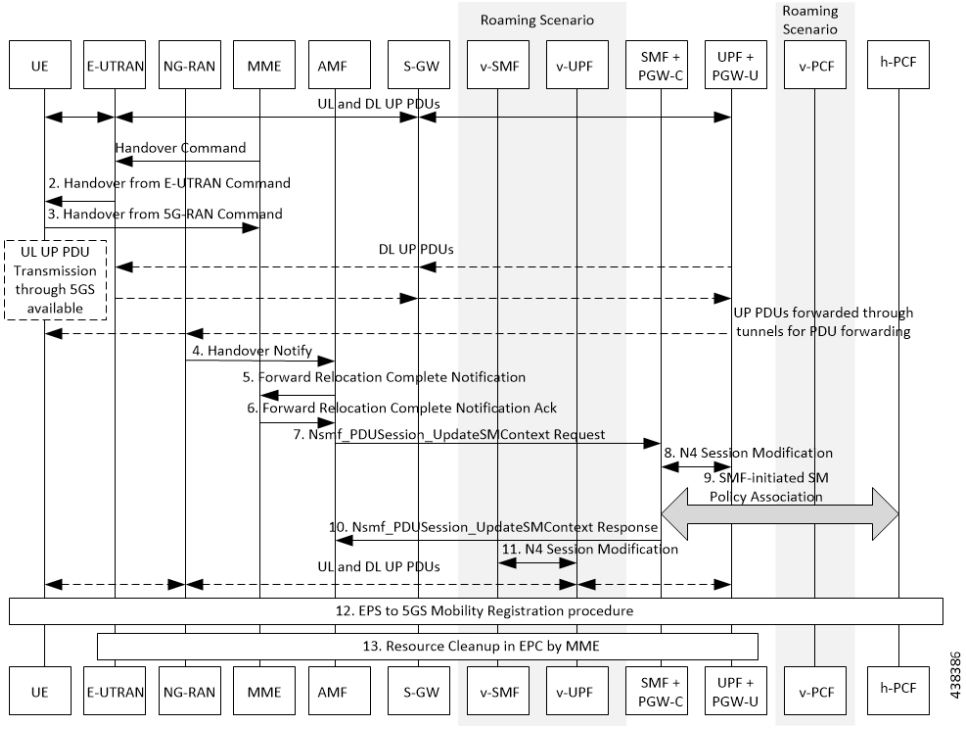


Table 156: Execution Call Flow Description for the EPS to 5G Handover with the N26 Interface

Step	Description
1	Call handover initiation starts from the UE and E-UTRAN toward each other, proceeds from E-UTRAN to S-GW. Then for roaming calls, call handover initiation proceeds from S-GW to the UPF+PGW-C-U. The MME sends the handover command to E-UTRAN.
2	The E-UTRAN sends the handover command to the UE.
3	The UE sends the confirmation message to NG-RAN for the received handover to 5G-RAN.
4	The NG-RAN sends the Handover Notification message to the AMF.
5	The AMF sends the Forward Relocation Complete Notification to the MME.
6	The MME sends the Acknowledgment Response for the received Forward Relocation Complete Notification.
7	The AMF sends NsmfPDUSessionUpdateSMContext Request to SMF +PGW-C. This request includes Handover Complete Indication for PDU Session ID details. For indirect forwarding, a timer in SMF+PGW-C starts to check when resources in UPF are to be released.
8	The SMF performs N4 Modification Request with UPF+PGW-U to update the DL tunnel information for the FARs that are associated with DL PDRs of the 5G session. The DL data path is activated. At this point, the indirect tunnel also exists.

Step	Description
9	The SMF sends NsmfPDUSessionUpdateSMContext Response, with PDU Session ID, to AMF. The SMF confirms the reception of Handover Complete.
10	After the timer that started in Step 7 expires, the SMF sends N4 Modification Request to UPF. This request is to remove the PDRs and FARs that are associated with the indirect data tunnel.
11	The UE starts the EPS to 5GS mobility registration procedure and sends it to H-PCF.
12	The E-UTRAN performs the resource cleanup in EPC by MME.

UE Idle Mode Mobility from EPS to 5GS using N26 Interface

The SMF and PGW-C support EPS to 5GS Idle Mode Mobility procedure. For Idle Mode Mobility from EPS to 5GS, the UE performs Mobility Registration Update Procedure with AMF. The AMF and SMF retrieve MM and SM contexts from EPS and move UE context from EPS to 5GS by interacting with other core NFs.

This feature enables the EPS and 5GS core network elements to support the following use cases during EPS to 5GS Idle Mode Mobility procedure.

- UE idle mode mobility from EPS to 5GS using N26 interface - PDU session in inactive state
- UE idle mode mobility from EPS to 5GS using N26 interface - User Plane connection reactivation request

PDU Session is in Inactive State

The following call flows captures information on UE Idle Mode Mobility from EPS to 5GS using N26 Interface when PDU session is in inactive state.

Figure 93: PDU Session in Inactive State

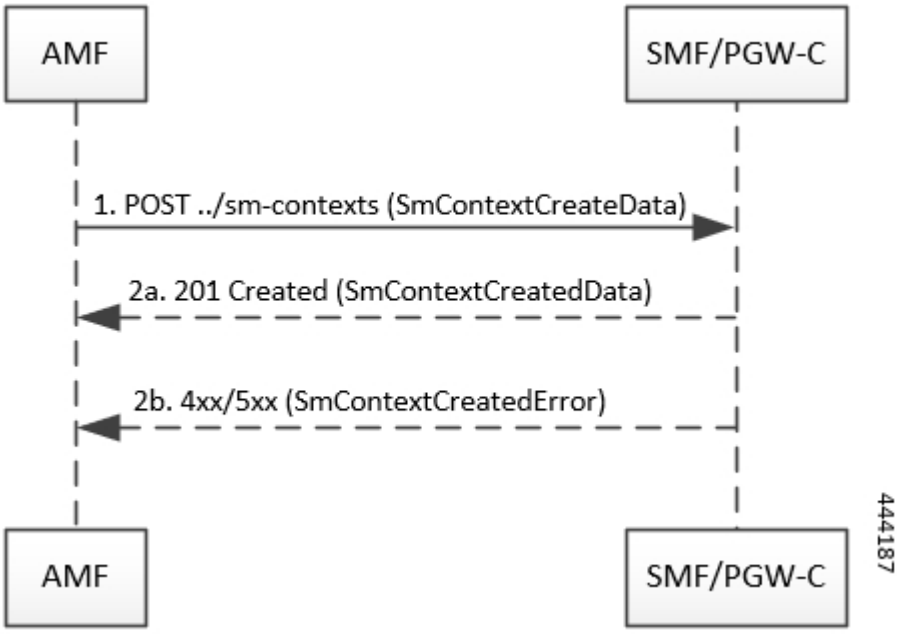


Table 157: PDU Session in Inactive State

Step	Description
1	AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information: • UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created. • EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.
2	Upon receipt of such a request, if: • a corresponding PDU session is found based on the EPS bearer contexts. • the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Connection Status attribute, if received; and • it is possible to proceed with moving the PDN connection to 5GS.
2a	SMF returns a 201 Created response including the following information: • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • Allocated EBI List, containing the EBI(s) allocated to the PDU session. The Location header present in the POST response contains the URI of the created SM context resource. AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID. If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.
2b	SMF returns 4xx/5xx failure response if: • SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to `NO_EPS_5GS_CONTINUITY`. • The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to `DEFAULT_EPS_BEARER_INACTIVE`.

User Plane Connection Reactivation Request

The following call flows captures information on UE idle mode mobility from EPS to 5GS with UP (User Plane) connection reactivation using N26 interface.

Figure 94: User Plane Connection Reactivation Request

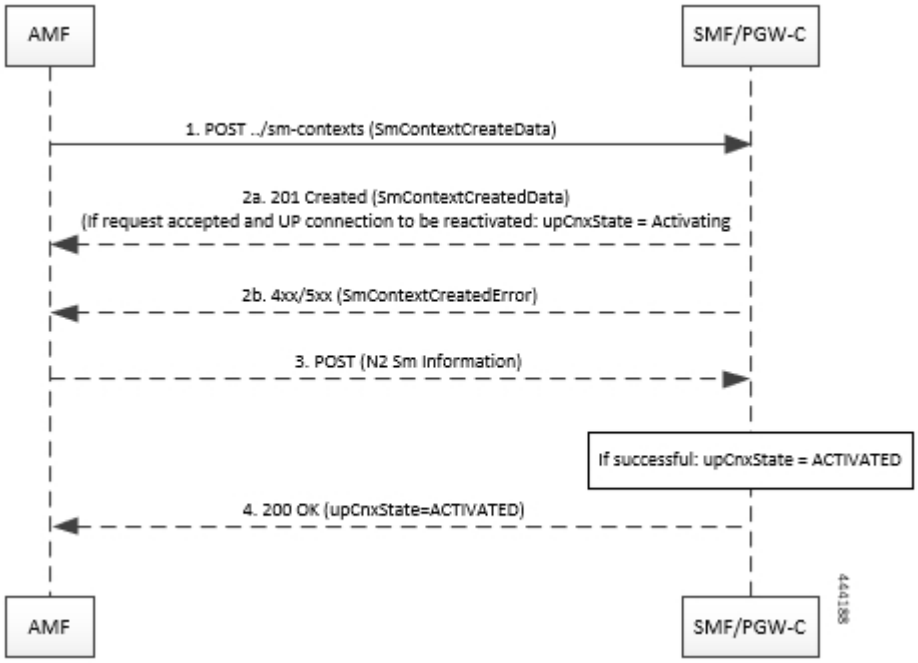


Table 158: User Plane Connection Reactivation Request

Step	Description
1	AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information: • UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created. • the PDU Sessions Activate List attribute, including the PDU Session ID of all the PDU session(s) to be re-activated. • EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.
2	Upon receipt of such a request, if: • a corresponding PDU session is found based on the EPS bearer contexts. • the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Context attribute, if received; and • it is possible to proceed with moving the PDN connection to 5GS.

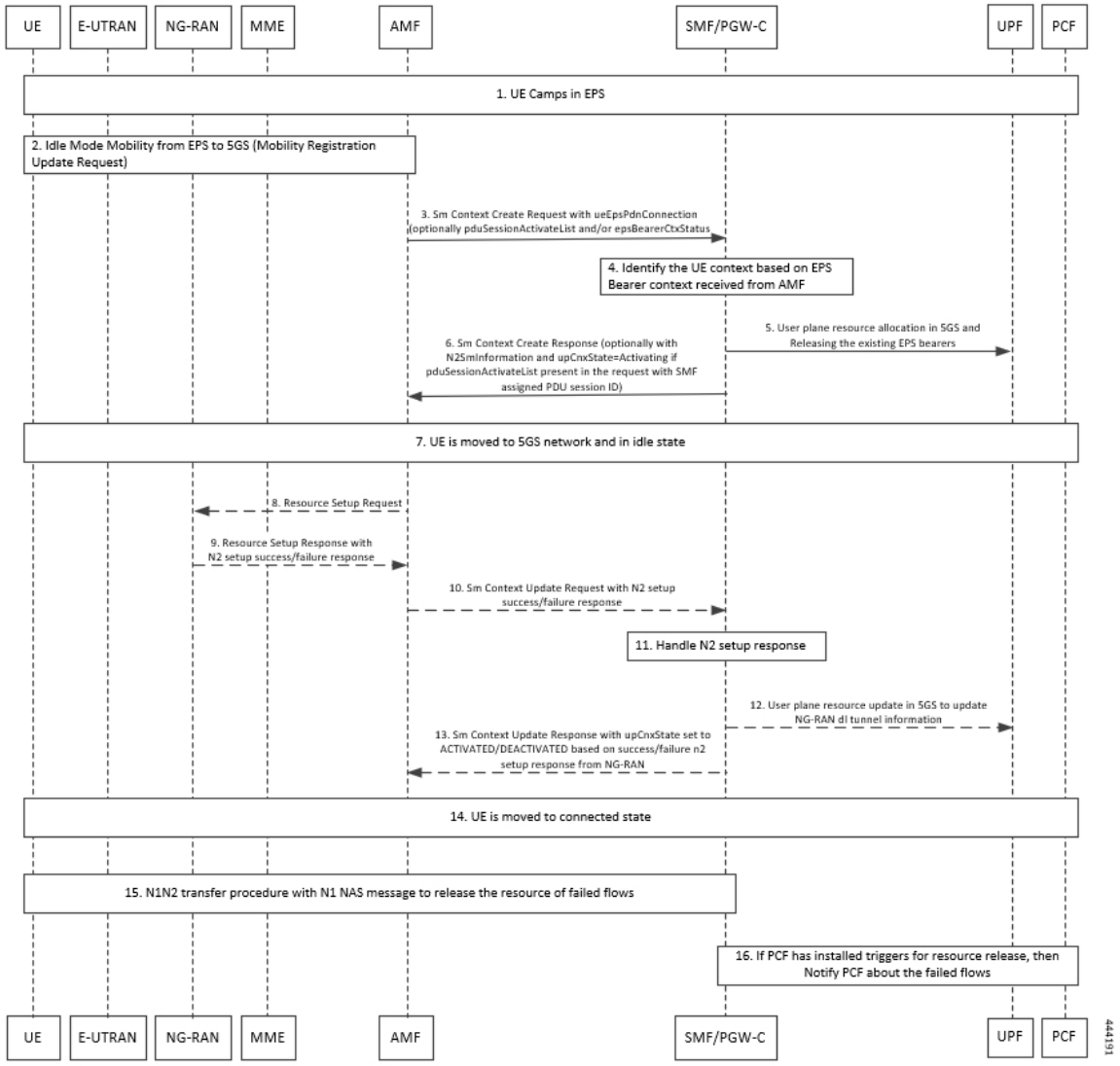
Step	Description
2a	SMF returns a 201 Created response including the following information: • PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection. • Allocated EBI List, containing the EBI(s) allocated to the PDU session. and, if the PDU session that is derived by the SMF based on the EPS bearer contexts was requested to be re-activated, i.e. if the PDU Session ID was present in the PDU Sessions Activate List, • the User Plane Connection State attribute is set to ACTIVATING. • N2 SM information to request the 5G-AN to assign resources to the PDU session (PDU Session Resource Setup Request Transfer), including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session (i.e. UPF's GTP-U F-TEID for uplink traffic). The Location header present in the POST response contains the URI of the created SM context resource. AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID. If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.
2b	SMF returns 4xx/5xx failure response if: • SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to `NO_EPS_5GS_CONTINUITY`. • The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to `DEFAULT_EPS_BEARER_INACTIVE`.

Step	Description
3	If the SMF returns a 200 OK response, the AMF subsequently updates the SM context in the SMF by sending POST request with the following information: • N2 SM information received from the 5G-AN (PDU Session Resource Setup Response Transfer IE), including the transport layer address and tunnel endpoint of one or two downlink termination point(s). It also includes the associated list of QoS flows for this PDU session (i.e. 5G-AN's GTP-U F-TEID(s) for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions; or • N2 SM information received from the 5G-AN (PDU Session Resource Setup Unsuccessful Transfer IE), including the Cause of the failure, if resources failed to be established for the PDU session. Upon receipt of this request, the SMF: • Updates the UPF with the 5G-AN's F-TEID(s) and sets the User Plane Connection State attribute to ACTIVATED, if the 5G-AN succeeds in establishing resources for the PDU sessions; or • Considers that the activation of the User Plane connection has failed and sets the User Plane Connection State attribute to DEACTIVATED.
4	SMF returns a 200 OK response including the User Plane Connection State attribute representing the final state of the user plane connection.

Message Flows

The following message flow describes the different scenarios of idle mode mobility procedure across 5GS network elements and subscriber.

Figure 95: Message Flow across 5GS NEs and Subscriber



Non-roaming 5GS to EPS Handover with Alternate RAT Tunnel Creation Call Flow

This section describes the call flow of the non-roaming 5GS to EPS handover with alternate RAT tunnel creation.

Figure 96: Non-roaming 5GS to EPS Handover with Alternate RAT Tunnel Creation Call Flow

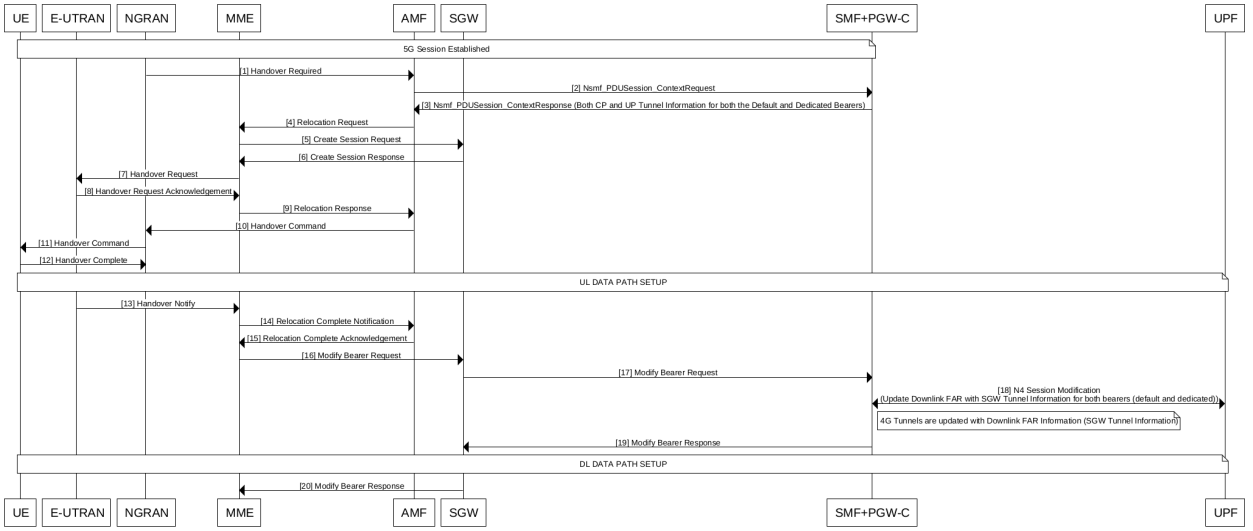


Table 159: Non-roaming 5GS to EPS Handover with Alternate RAT Tunnel Creation Call Flow Description

Step	Description
1	A 5G session is established among UE, E-UTRAN, NGRAN, MME, AMF, S-GW, and SMF+PGW-C. NG-RAN initiates handover towards AMF.
2	AMF sends the Nsmf PDU Session Context Request to SMF+PGW-C.
3	SMF+PGW-C sends the Nsmf PDU Session CreateSMContext Response to AMF. This response includes details on the CP and UP tunnels for both the default and dedicated bearers.
4	AMF sends the Relocation Request to MME.
5	MME sends the Create Session Request to S-GW.
6	S-GW sends the Create Session Response to MME.
7	MME sends the Handover Request to E-UTRAN.
8	E-UTRAN sends the acknowledgment of the Handover Request to MME.
9	MME sends the Relocation Response to AMF.
10	AMF sends the handover command to NG-RAN.
11	NG-RAN sends the handover command to UE.
12	UE sends the handover completion message to NG-RAN.
13	The UL data path is set up among UE, E-UTRAN, NG-RAN, MME, AMF, S-GW, SMF+PGW-C, and UPF. E-UTRAN sends the Handover Notify message to MME.

Step	Description
14	MME sends the notification on the relocation completion to AMF.
15	AMF sends the acknowledgment message of relocation completion to MME.
16	MME sends the Modify Bearer Request to S-GW.
17	S-GW sends the Modify Bearer Request to SMF+PGW-C.
18	SMF+PGW-C sends the N4 Session Modification Request to UPF. This request includes details for updating DL FAR with S-GW tunnel for both the default and dedicated bearers.
19	The 4G Tunnels are updated with DL FAR information (S-GW tunnel information). SMF+PGW-C sends the Modify Bearer Response to S-GW.
20	The DL data path is set up among UE, E-UTRAN, NG-RAN, MME, AMF, S-GW, SMF+PGW-C, and UPF. S-GW sends the Modify Bearer Response to MME.

Non-roaming EPS to 5GS Handover with Alternate RAT Tunnel Creation Call Flow

This section describes the call flow of non-roaming EPS to 5GS handover with an alternate RAT tunnel creation.

Figure 97: Non-roaming EPS to 5GS Handover with Alternate RAT Tunnel Creation Call Flow

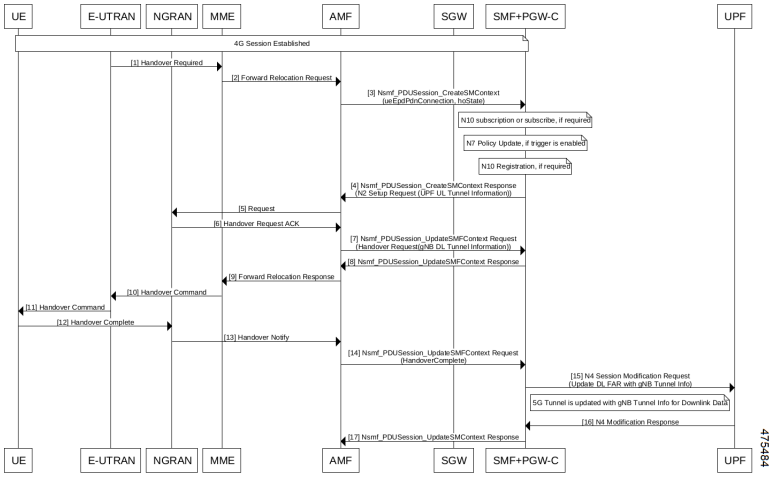


Table 160: Non-roaming EPS to 5GS Handover with Alternate RAT Tunnel Creation Call Flow Description

Step	Description
1	A 5G session is established among UE, E-UTRAN, NG-RAN, MME, AMF, S-GW, and SMF+PGW-C. E-UTRAN initiates handover towards MME.
2	MME sends the Forward Relocation Request to AMF.

Step	Description
3	AMF sends the Nsmf PDU Session CreateSMContext request to SMF+PGW-C. This request includes details on the UE PDN connection and handover state.
4	SMF+PGW-C checks for the following procedures: • N10 subscription or you can subscribe, if required. • N7 Policy Update, if trigger is enabled. • N10 Registration, if required. SMF+PGW-C sends the Nsmf PDUSession CreateSMContext Response to AMF. This response includes the N2 Setup Request with the UPF UL tunnel information.
5	AMF sends the handover request to NG-RAN.
6	NG-RAN sends the acknowledgment of the handover request to AMF.
7	AMF sends the Nsmf PDU Session Update SMF Context Request to SMF+PGW-C. This request includes the handover request with the gNB DL tunnel information.
8	SMF+PGW-C sends the Nsmf PDU Session Update SMF Context Response to AMF.
9	AMF sends the Forward Relocation Response to MME.
10	MME sends the Handover Command to E-UTRAN.
11	E-UTRAN sends the Handover Command to UE.
12	UE sends the message on handover completion to NG-RAN.
13	NG-RAN sends the Handover Notify message to AMF.
14	AMF sends the Nsmf PDU Session Update SMF Context Request to SMF+PGW-C after the completion of the handover.
15	SMF+PGW-C sends the N4 Session Modification Request to UPF. This request is for updating the DL FAR with the gNB tunnel information.
16	The 5G Tunnel is updated with gNB tunnel information for the DL data. UPF sends the N4 Modification Response to SMF+PGW-C.
17	SMF+PGW-C sends the Nsmf PDU Session Update SMContext Response to AMF.

Standards Compliance

The SMF Support for 4G to 5G Data Session Handover feature complies with 3GPP TS 23.502 V15.2.0 (2018-09) standard.

Limitations

The 4G to 5G Data Session Handover feature has the following limitation:

- SMF supports N26 4G to 5G handoff with single UPF, which implies that UPF selection and UPF modification are not supported.

CHF and PCF Integration for Access and Mobility Procedures

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

For the access and mobility procedures, SMF integrates Charging Function (CHF) and Policy Control Function (PCF) for the following procedures:

- Intra-AMF and Inter-AMF N2-based Handovers—SMF supports this function when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases.
- N26 4G to 5G Handover—SMF supports the EPS to 5GS procedures with the N26 interface. SMF establishes Uplink (UL) Packet Detection Rule (PDR) or Downlink (DL) PDR toward with the qualified EPS Bearer Identity (EBI) list in 5GS and replicates EBIs to the respective flows. SMF also creates IDFT to support the Downlink forwarding traffic between SGW-U to NR over UPF.
- N26 5G to 4G Handover—SMF supports 5GS to EPS procedures with the N26 interface. PGW-C establishes UL PDRs or DL PDRs toward SGW-U with qualified flows in 5GS and replicates EBIs to respective flows. PGW-C also creates an IDFT tunnel to support Downlink forwarding traffic between NR to SGW-U over UPF. Session-Level or Rating-Group level Charging Triggers are received during PDU Session establishment or in response to SMF-initiated Charging Update Request or CHF-initiated Charging Update Notify response in EPS procedures.
- Xn Handover—SMF supports the Xn-based inter NG-RAN handover with and without UPF reallocation. The SMF supports Xn handovers for intra-AMF mobility only. SMF processes the received SM context update request that includes the path switch request N2-based message and the access-side parameters. These parameters identify the CHF and PCF triggers that are received during PDU session establishment.
- Service Request Procedures—SMF supports the service requests from both the UE and network-initiated procedures. Either a UE in CM-Idle state or the 5GC uses the Service Request procedure to request the establishment of a secure connection to an AMF. The UE in both the CM-Idle and in CM-Connected state use the Service Request procedure to activate a User Plane connection for an established PDU Session. The UE does not initiate a Service Request procedure if an ongoing Service Request procedure exists.

SMF saves the CHF and PCF triggers that it receives as part of session creation or PCF or UE-initiated modifications. When a UE triggers access and mobility procedures for the preceding functions, SMF identifies the triggers from CHF and PCF against the received access parameters. Then, SMF sends an update toward CHF and PCF.

How it Works

The SMF integrates the CHF and PCF functions based on the following information:

- Policy control request triggers, which are received in the SM policy decision during PDU session establishment or PCF or UE-initiated modification.
- Session-level or rating-group-level charging triggers, which are received during PDU session establishment or in response to SMF-initiated Charging Update Request or CHF-initiated Charging Update Notify Request.

The SMF supports the following access-side information to detect the PCF and CHF triggers. The SMF sends the trigger information to the CHF and PCF during the N2-based handover.

Table 161: Access-Side Information for PCF and CHF Triggers

Access Side Information	CHF Triggers	PCF Triggers
UserLocation	USER_LOCATION_CHANGE	SAREA_CH
UeTimeZone	UE_TIMEZONE_CHANGE	SAREA_CH
ServingNetwork	PLMN_CHANGE	PLMN_CH
TargetServingNfId	SERVING_NODE_CHANGE	

For a change in the subscriber location, the SMF sends USER_LOCATION_CHANGE trigger towards CHF and SAREA_CH trigger towards PCF.

The SMF generates the usage report whenever a change in the subscriber location is detected in the following messages:

- Delete Bearer Command
- Delete Bearer Response
- Modify Bearer Request

For example, when a Delete Bearer Command is received with a new ULI, a CDR event is triggered with new ULI. If PCF or CHF has armed notification for ULI modifications, the SMF sends a notification to the PCF and CHF respectively.

This feature is compliant with the 3GPP TS 32.291, version 15.4.0.

Call Flows

This section describes the following call flows:

- CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow
- CHF and PCF Integration for N26 4G to 5G Handover Call Flow
- CHF and PCF Integration for N26 5G to 4G Handover Call Flow
- CHF and PCF Integration for Xn Handover Call Flow

- CHF and PCF Integration for Service Request Procedures

Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

This section describes the intra-AMF and inter-AMF N2-based handover call flow to support CHF and PCF integration.

Figure 98: Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

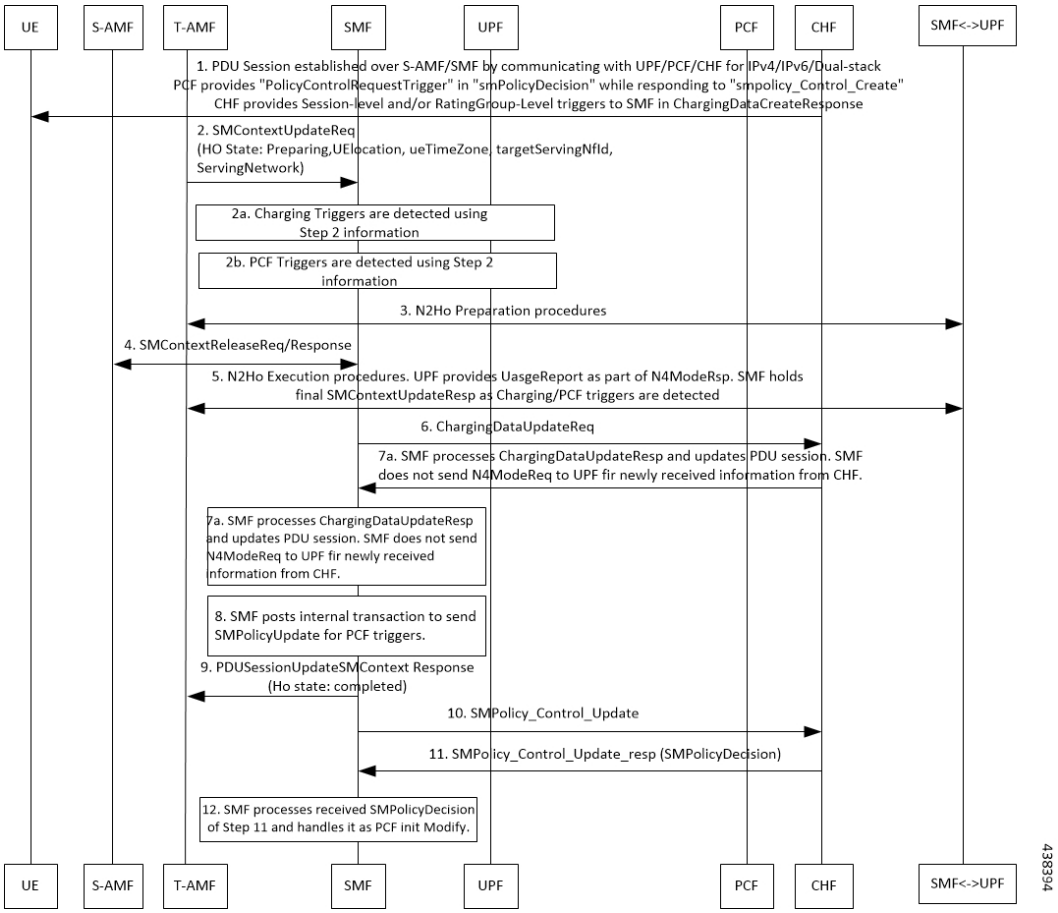


Table 162: CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow Description

Step	Description
1	The PDU session establishes over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF sends session-level and rating-group-level triggers to SMF as the Charging Data Create Response.

Step	Description
2	The T-AMF sends SM Context Update Request by including handover state to the SMF. The handover state includes the information on preparation, UE location, UE time zone, target serving NFID, and serving network. The AMF includes target serving NFID information for inter-AMF handoff.
2a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.
3	The N2-based Handover Preparation procedure starts from T-AMF towards the SMF and CHF and the opposite direction.
4	In the N2-based Handover Execution procedure, in case of inter-AMF handoff, the SMF receives SM Context Release Request from S-AMF and responds with the SM Context Release Response to the S-AMF.
5	In N2-based Handover Execution procedure, the UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Release Response when the SMF detects the CHF or PCF triggers.
6	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-information (with rating-group-level triggers with usage report), customer identification, and PDU session charging information.
7	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
7a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
8	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
9	The SMF sends the SM Context Update Response, for which the handover state is complete, to the T-AMF.
10	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update information includes details, such as the user location information, UE time zone, and serving network.
11	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
12	The SMF processes the SM policy decision that is received as response and triggers the PCF-initiated modification procedure..

CHF and PCF Integration for N26 4G to 5G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 4G to 5G handovers.

Figure 99: CHF and PCF Integration for N26 4G to 5G Handover Call Flow

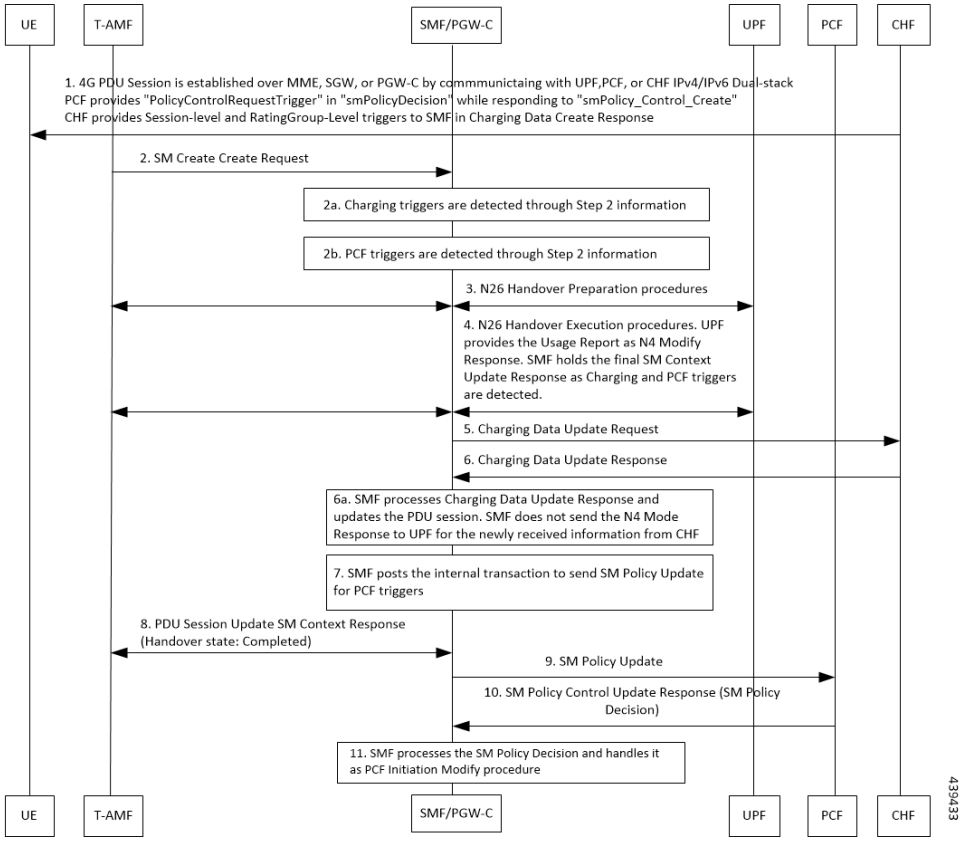


Table 163: CHF and PCF Integration for N26 4G to 5G Handover Call Flow Description

Step	Description
1	The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The T-AMF sends SM Context Create Request to the SMF. This request includes information on handover state as preparing, UE location, UE time zone, serving NFID, serving network, and RAT type.
2a	The SMF detects access-side changes that are received in the SM Context Create Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.
3	The N26-based Handover Preparation procedure starts from T-AMF toward the SMF or PGW-C and UHF and the opposite way, as defined in *3GPP TS 23.502, section 4.1.9.3*.

Step	Description
4	In the N26 Handover Execution procedure, the UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in *3GPP TS 23.502, section 4.3.3.2*.

CHF and PCF Integration for N26 5G to 4G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 5G to 4G handovers.

Figure 100: CHF and PCF Integration for N26 5G to 4G Handover Call Flow

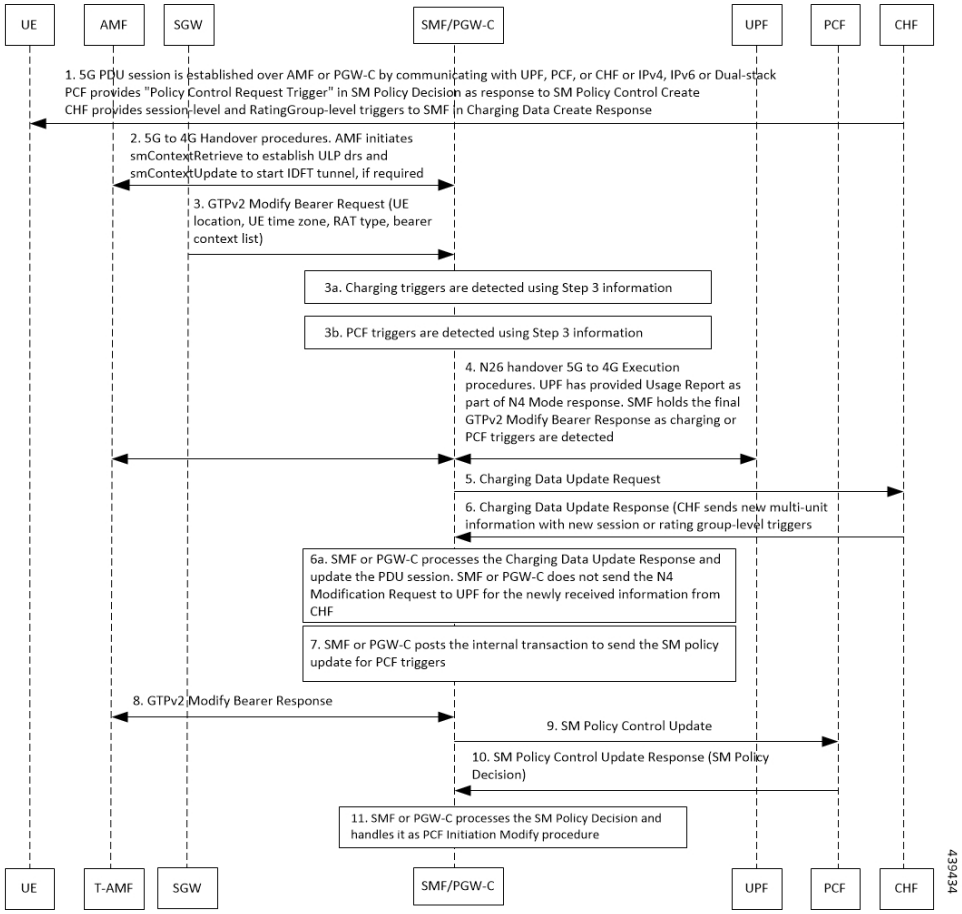


Table 164: CHF and PCF Integration for N26 5G to 4G Handover Call Flow Description

Step	Description
1	The PDU session is established over S-AMF or SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The 5G to 4G Handover procedure starts from AMF toward the SMF or PGW-C and the opposite way. AMF initiates the SM Context Retrieve Request to establish the UL PDRs and send SM Context Update Response to start the IDFT tunnel, if necessary.
3	In the N26 5G to 4G Handover Execution procedure, the SGW sends the GTPv2 Modify Bearer Request to PGW-C. This request includes the information on UE location, UE time zone, RAT type, and Bearer Context List.
3a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 3.

Step	Description
3b	The SMF detects the PCF triggers with the information that is available in Step 3.
4	In the N26 Handover 5G to 4G Execution procedure, the PGW-C requests UPF to create a GTP-U tunnel for each flow. This tunnel is for the EBIs received in the Bearer Context List of GTPv2 Modify Bearer Request. After the DL PDRs are established, UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final GTPv2 Modify Bearer Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF or PGW-C processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF or PGW-C posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF or PGW-C sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF or PGW-C sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in *3GPP TS 23.502, section 4.3.3.2*.

CHF and PCF Integration for Xn Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for the Xn handover.

Figure 101: CHF and PCF Integration for Xn Handover Call Flow

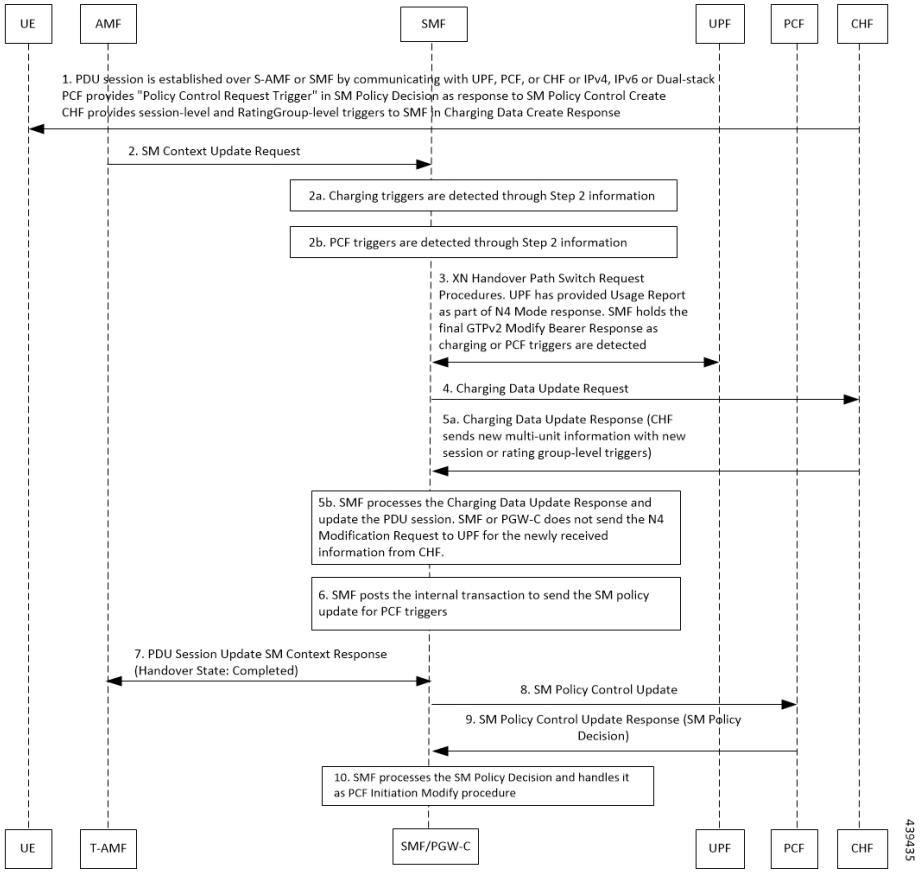


Table 165: CHF and PCF Integration for Xn Handover Call Flow Description

Step	Description
1	The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack. The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control. The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The AMF sends SM Context Update Request to the SMF. The SM Context Update Request includes the information on UE location, UE time zone, and path switch request N2 message.
2a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.

Step	Description
3	The Xn Handover Preparation procedure starts from SMF toward UPF and the opposite way, as defined in *3GPP TS 23.502, section 4.9.1.2*. SMF sends the N4 Modification Request to UPF and updates the received DL tunnel information of T-gNB. After the tunnel information is updated, UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
5	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
6	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
7	The SMF sends the SM Context Update Response to the AMF. This response includes the path switch request acknowledgment N2 message.
8	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information and UE time zone.
9	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
10	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in *3GPP TS 23.502, section 4.3.3.2*.

CHF and PCF Integration for Service Request Procedures

This section describes the CHF and PCF integration for service request procedures.

SMF processes the received SM Context Update Request to update N3 tunnel path state from Idle to Active or Active to Idle. SMF performs the following steps:

1. When UE is in CM-Idle state at AMF, which is Active to Idle mode—Based on the configuration, SMF updates UPF for N3 tunnel state to drop or buffer by sending the N4 session mode request. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.
2. When UE is in CM-Connected state at AMF, which implies SMF receives UE-requested Procedures to change the subscriber N3 Tunnel Path from Idle to Active State—SMF receives the updated user location and UE time zone in the SM Context Update Request. SMF sends the N4 Session Modification Request to UPF to update the DL tunnel details of gNB. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.
3. When the N3 Tunnel is unavailable for the Network Service Request Triggers, which implies that UE is in CM-Idle state at AMF—SMF initiates the Network Service Request Procedures for AMF to initiate

Paging toward the end user. Then, AMF begins the UE Service Request Procedures to configure the N3 Tunnel as specified in Step 2.

Standards Compliance

The CHF and PCF integration for access and mobility procedures feature complies with the following standards:

- *3GPP TS 23.502 version 15.4.0 Release 15 (sections 4.9.1.3, 4.11.1.2, 4.9.1.2, and 4.2.3)—5G; Procedures for the 5G System*

Inter gNodeB Handover

Feature Description

The SMF supports the Xn-based and N2-based handover procedures to hand over a UE from a source NG-RAN node to a target NG-RAN node using the Xn or N2 reference points. Initiation of this procedure can be due to new radio conditions, load balancing or due to a specific service.

The SMF releases the QoS flows that failed to set up on the target NG-RAN during Xn and N2 handovers on the respective interfaces N4 (UPF) and N1 (UE). The SMF sends appropriate notification to N7 (PCF) based on the triggers if armed. The SMF also sends the usage report to N40 (CHF) for the released QoS flows.

How it Works

Call Flows

The following sections explain the execution of Xn-based and N2-based handover procedures.

Xn-based Inter NG-RAN Handover

This section provides details regarding the Xn-based inter NG-RAN handover without UPF reallocation.

The handover preparation and the execution stages are implemented as specified in *3GPP TS 38.300*. When performing the handover in a shared network, the source NG-RAN determines a PLMN to be used in the target network as specified in *3GPP TS 23.501*. If the serving PLMN changes during the Xn handover, the source NG-RAN node indicates the selected PLMN ID to the target NG-RAN node.

If the AMF generates the N2 downlink signalling and receives a rejection to an N2 interface procedure due to the ongoing Xn handover procedure, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. The failure is known by expiry of the timer guarding the N2 interface procedure.

Upon reception of an SMF-initiated N1 and/or N2 request(s) with an indication that the request has been temporarily rejected due to the ongoing Xn handover procedure, the SMF starts a locally configured guard timer. The SMF holds signalling messages targeted towards the AMF during the handover preparation phase unless it detects that the handover is completed or the handover has failed or cancelled. The SMF reattempts, up to a pre-configured number of times, when either it detects that the handover is completed or has failed using message reception or at expiry of the guard timer.

The Xn-based inter NG-RAN handover is used to hand over a UE from a source NG-RAN to target NG-RAN using Xn when the AMF is unchanged and the SMF decides to keep the existing UPF.

The following figure depicts the call flow of the Xn-based inter NG-RAN handover without the UPF reallocation.

Figure 102: Xn-based Inter NG-RAN Handover without UPF Reallocation

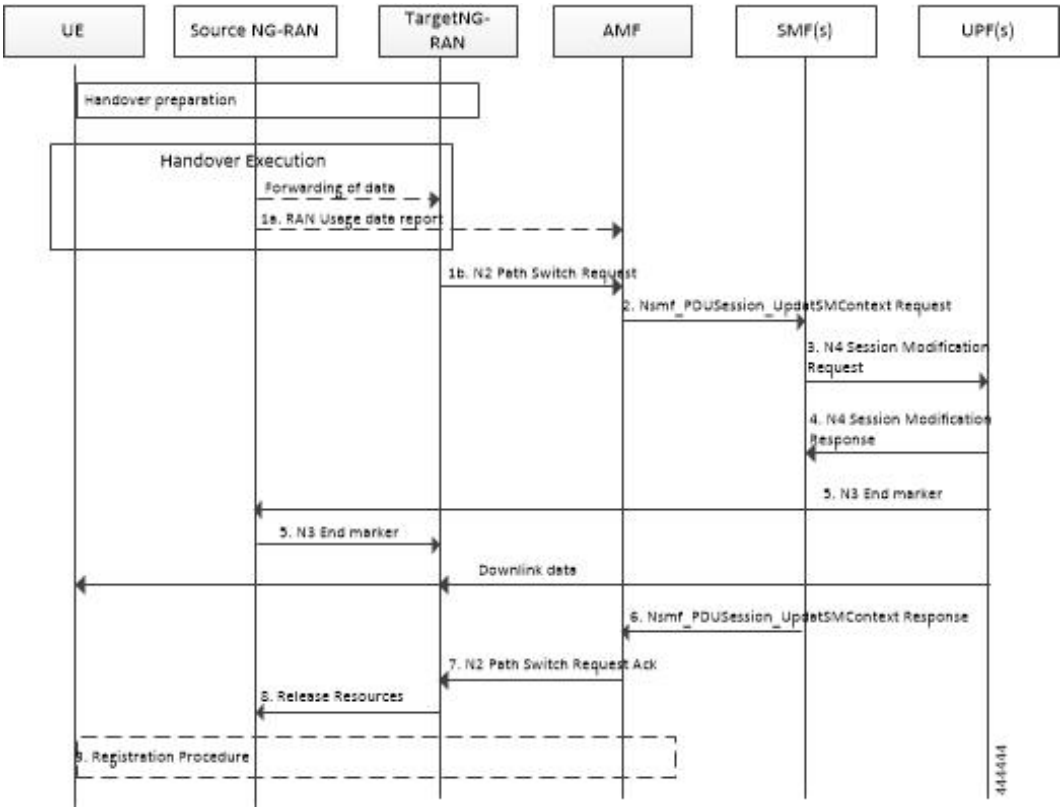


Table 166: Xn-based Inter NG-RAN Handover Call Flow Description (Without UPF Reallocation)

Step	Description
1a	During the handover execution, the source NG-RAN node provides RAN usage data Report to the AMF. The source NG-RAN node provides this report only when the target NG-RAN has confirmed handover over Xn interface. This report includes N2 SM Information (Secondary RAT usage data), Handover Flag, and Source to Target transparent container. The Handover Flag indicates that the report needs to be buffered by the SMF.
1b	The target NG-RAN sends an N2 Path Switch Request message to the AMF to inform that the UE has moved to a new target cell. The NG-RAN provides a List Of PDU Sessions To Be Switched. The N2 SM Information includes the AN Tunnel Info for each PDU Session to be switched.
2	The AMF sends N2 SM information by invoking the Nsmf_PDUSession_UpdateSMContext request service operation for each PDU session in the lists of PDU Sessions received in the N2 Path Switch Request.

Step	Description
3	The SMF sends an N4 Session Modification Request message to the UPF. The SMF may notify the UPF that originated the Data Notification to discard downlink data for the PDU Sessions and/or to not provide further Data Notification messages.
4	The UPF returns an N4 Session Modification Response message to the SMF after the requested PDU sessions are switched.
5	The UPF sends one or more "end marker" packets for each N3 tunnel on the old path immediately after switching the path. The UPF starts sending downlink packets to the target NG-RAN.
6	The SMF sends an Nsmf_PDUSession_UpdateSMContext response (CN Tunnel Info) to the AMF for PDU sessions which have been switched successfully. **Important** Step 6 can occur any time after the receipt of N4 Session Modification Response at the SMF.
7	Once the Nsmf_PDUSession_UpdateSMContext response is received from all the SMFs, the AMF aggregates the received CN Tunnel Info and sends this aggregated information as a part of N2 SM Information along with the Failed PDU Sessions in N2 Path Switch Request Ack to the target NG-RAN. If none of the requested PDU sessions have been switched successfully, the AMF sends an N2 Path Switch Request Failure message to the target NG-RAN.
8	The target NG-RAN confirms success of the handover by sending Release Resources message to the source NG-RAN.
9	The UE initiates Mobility Registration Update procedure if one of the triggers of registration procedure applies.

The following figure shows the detailed call flow of the Xn handover without UPF reallocation.

Figure 103: Xn Handover Without UPF Relocation Call Flow

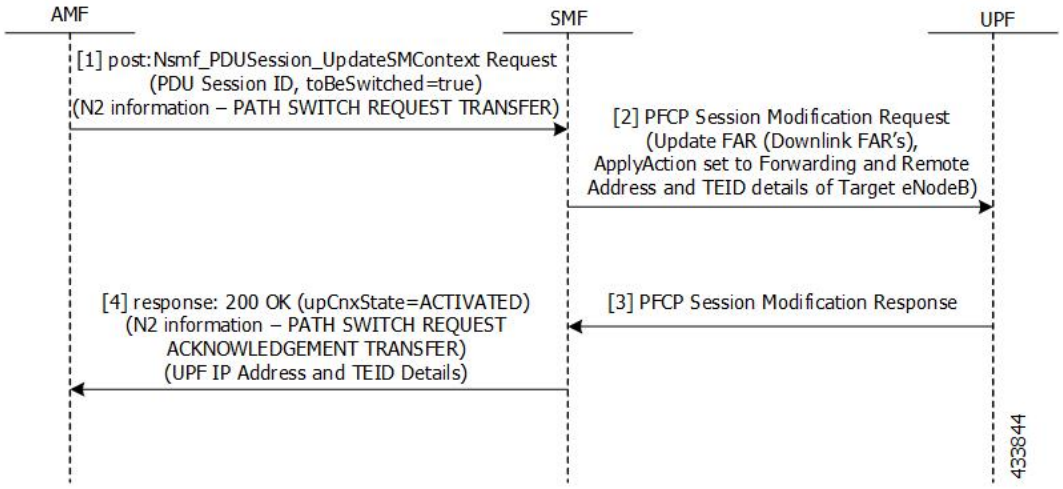


Table 167: Detailed Call Flow Description for the Xn Handover Without UPF Relocation

Step	Description
1	The NF Service Consumer (AMF) requests the SMF to switch the user plane connection of the PDU session. The AMF sends a POST request with the following information: • The toBeSwitched indication. • N2 SM information received from the 5G-AN (PDU session path switch request transfer IE), including the new transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session. • User location and user location timestamp. • Other information, if necessary.
2	The SMF switches the N3 tunnel of the PDU session after receiving the request. The SMF initiates PFCP session modification procedure toward the UPF with downlink FAR updated with the following option: • Forwarding Action is enabled with the remote node “forwarding parameters” details, such as the IP address and GTP-U F-TEID.
3	The SMF marks the PDU handover as successful after receiving the successful response from the UPF node.
4	The SMF initiates the 200 OK response. This response includes the N2 SM information, which has the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session, that is UPFs GTP-U F-TEID for the uplink traffic.

N2-based Inter NG-RAN Handover

Table 168: Feature History

Feature Name	Release Information	Description
DRB Level Data Forwarding in IDFT for N2-based Handover	2023.04	SMF supports DRB level data forwarding, in case the Data forwarding response DRB List is present in the Handover Request Acknowledge message and it does not meet the criteria for Session Level Forwarding.

The source NG-RAN decides to initiate an N2-based handover (HO) to the target NG-RAN. Initiation of this procedure could be due to any of the following reasons:

- New radio conditions
- Load balancing
- If there is no Xn connectivity to the target NG-RAN

- An error indication from the target NG-RAN after an unsuccessful Xn-based handover (that is, no IP connectivity between Target RAN (T-RAN) and Source UPF (S-UPF)).
- Based on dynamic information learned by the Source RAN (S-RAN)

The source NG-RAN determines the availability of a direct forwarding path and indicates the same to the SMFs. If the IP connectivity is available between the source, target NG-RAN, and the security association is in place between them, a direct forwarding path is available. If a direct forwarding path is not available, use the indirect forwarding. The SMFs use the indication from the source NG-RAN to choose the data forwarding path.

When performing the handover in a shared network, the source NG-RAN determines a PLMN for use in the target network as specified by *3GPP TS 23.501*. The source NG-RAN indicates the selected PLMN ID to the AMF as part of the Tracking Area sent in the HO Required message.

If the AMF generates the N2 downlink signaling and receives a rejection to a N2 interface procedure due to the ongoing N2 handover, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. If the Inter NG-RAN node handover changes the serving AMF, the source AMF terminates any other ongoing N2 interface procedures except the handover procedure.

If the AMF is still the serving AMF, the AMF pauses non-handover related N2 interface procedures and resumes them after the N2 handover is complete.

If the AMF detects that it must be changed, the AMF rejects any SMF-initiated N2 request and includes an indication that the request has been temporarily rejected due to the ongoing N2 handover procedure.

The following figure depicts the call flow for the preparation phase of the N2-based inter NG-RAN handover procedure.

Figure 104: Inter NG-RAN Node N2-based Handover - Preparation Phase

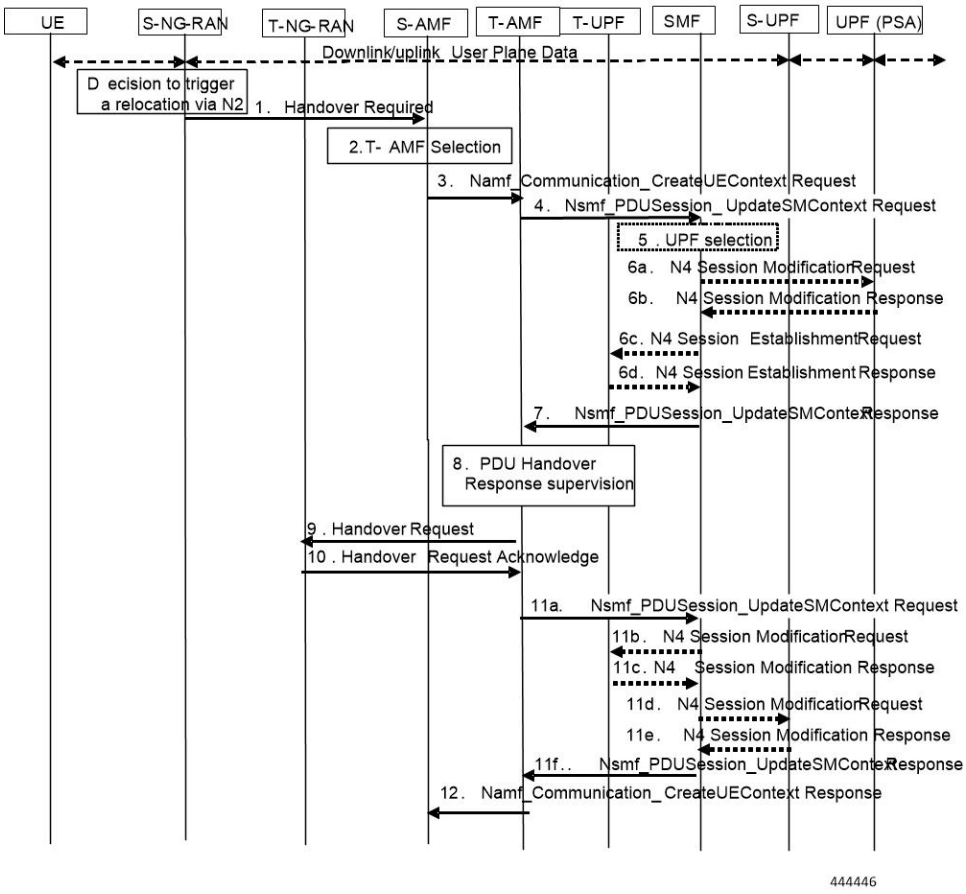


Table 169: Inter NG-RAN Node N2-based Handover Call Flow Description - Preparation Phase

Step	Description
1	The Source NG-RAN (S-RAN) sends the Handover Required message to the Source AMF (S-AMF). This message includes the following: • Target ID • Source to Target transparent container • SM N2 info list • PDU Session IDs • Intra-system handover indication The Source to Target transparent container includes NG-RAN information for use in Target RAN (T-RAN), and is transparent to 5GC. It also contains the corresponding User Plane Security Enforcement information, QoS flows/DRBs information subject to data forwarding. If direct data forwarding is available, the SM N2 info includes Direct Forwarding Path Availability. Direct Forwarding Path Availability indicates whether direct forwarding is available from the S-RAN to the T-RAN. This indication from S-RAN is based on the presence of IP connectivity and security association between the S-RAN and the T-RAN.
2	When the S-AMF cannot serve the UE anymore, the S-AMF selects the T-AMF as described in clause 6.3.5 on "AMF Selection Function" in *TS 23.501*.

3	The S-AMF initiates a Handover resource allocation procedure by invoking the Namf_Communication_CreateUEContext service operation toward the T-AMF.
	The Namf_Communication_CreateUEContext Request includes the following:
	• N2 Information
	  • Target ID
	  • Source to Target transparent container
	  • SM N2 information list
	  • PDU Session IDs
	• UE context information
	  • SUPI
	  • Service area restriction
	  • Allowed NSSAI for each Access Type if available
	  • Tracing Requirements
	  • The list of PDU Session IDs along with the corresponding SMF information and the corresponding S-NSSAI(s), PCF ID(s), and DNN
	When the S-AMF can still serve the UE, this step and step 12 are not needed.

Step	Description
4	For each PDU session indicated by S-RAN, the AMF invokes the Nsmf_PDUSession_UpdateSMContext Request to the associated SMF. However, if the S-NSSAI associated with PDU session is not available in the T-AMF, the T-AMF does not invoke Nsmf_PDUSession_UpdateSMContext for this PDU session. If the T-AMF detects that the UE moves into a restricted area based on Service area restrictions, the T-AMF notifies that the UE is only reachable for regulatory prioritized services to each NF consumer which has subscribed for the UE reachability event.
5	Based on the Target ID, the SMF checks the acceptance of N2 handover for the indicated PDU session. The SMF also checks the UPF Selection Criteria. If the UE has moved out of the service area of the UPF connecting to NG-RAN, the SMF selects a new intermediate UPF.
6a	If the SMF selects a new UPF to act as the intermediate UPF for the PDU session, and the different CN Tunnel Info must be used, the SMF sends an N4 Session Modification Request message to the UPF (PDU Session Anchor (PSA)). If the SMF allocates the CN Tunnel Info, it provides the CN Tunnel Info on N9, and the UPF (PSA) associates CN Tunnel Info with UL Packet detection rules.
6b	The UPF (PSA) sends an N4 Session Establishment Response message to the SMF. If the UPF (PSA) allocates CN Tunnel Info (on N9) of the UPF (PSA), it provides CN Tunnel Info (on N9) to the SMF. The UPF (PSA) associates the CN Tunnel Info (on N9) with UL Packet detection rules provided by the SMF.
6c	If the SMF selects a new intermediate UPF (T-UPF) and if the T-UPF allocates the CN Tunnel Info, the SMF sends an N4 Session Establishment Request message to the T-UPF. This request enables the Packet detection, enforcement, and reporting rules to be installed on the T-UPF. The T-UPF receives the CN Tunnel Info (on N9) of UPF (PSA) for this PDU session, which is used to set up the N9 tunnel.
6d	The T-UPF sends an N4 Session Establishment Response message to the SMF with DL CN Tunnel Info and UL CN Tunnel Info (that is, N3 tunnel info). The SMF starts a timer to release the resource of S-UPF, which is to be used in the step 13a of the Execution Phase.
7	If the N2 handover for the PDU session is accepted, the SMF includes the N2 SM Information in the Nsmf_PDUSession_UpdateSMContext response. The N2 SM Information contains the N3 UP address and the UL CN Tunnel ID of the UPF and the QoS parameters indicating that the N2 SM Information is for the Target NG-RAN. If the N2 SM information received at step 4, does not include the Direct Forwarding Path Availability and the SMF knows that there is no indirect data forwarding connectivity between source and target, the N2 SM Information includes a Data forwarding not possible indication. If the N2 handover for the PDU session is not accepted as described in step 5, the SMF does not include the N2 SM Information to avoid the establishment of radio resources at the target NG-RAN. The SMF provides a reason for non-acceptance. If the SMF receives notification from T-AMF that UE is only reachable for regulatory prioritized service, the SMF deactivates the PDU session.
8	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response messages from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the AMF continues with the N2 Handover procedure (Handover Request message in step 9).

Step	Description
9	If the subscription information includes Tracing Requirements, the target AMF provides the target RAN with Tracing Requirements in the Handover Request. The Handover request includes Source to Target transparent container, N2 MM Information, N2 SM Information list, and Tracing Requirements. The T-AMF determines T-RAN based on Target ID. T-AMF allocates a 5G-GUTI valid for the UE in the AMF and target TAI. N2 MM Information includes, for example, security information and Mobility Restriction List if available in the T-AMF. N2 SM Information list includes N2 SM Information for the T-RAN in the Nsmf_PDUSession_UpdateSMContext Response messages received within the allowed max delay supervised by the T-AMF in step 8.
10	The T-RAN sends a Handover Request Acknowledge to the T-AMF. The Acknowledge message includes Target to Source transparent container, List of PDU Sessions to Handover with N2 SM information, List of PDU Sessions that failed to establish with the failure cause given in the N2 SM information element.
11a	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID, N2 SM response) to the SMF. For each N2, SM response received from the T-RAN, the AMF sends the N2 SM response to the SMF indicated by the respective PDU Session ID. If no new T-UPF is selected, the SMF stores the N3 tunnel info of T-RAN from the N2 SM response if the N2 handover is accepted by T-RAN. The SMF/UPF allocates the N3 UP address and Tunnel IDs for indirect data forwarding corresponding to the data forwarding tunnel endpoints established by T-RAN. If a PDU session is indicated as a rejected PDU session by the Target NG-RAN, the SMF triggers the release of this PDU session. In all other cases of PDU Session rejection, the SMF decides whether to release the PDU session or to deactivate the UP connection of this PDU session. If some of the QoS Flows of a PDU Session are not accepted by the Target NG-RAN, SMF initiates the PDU Session Modification procedure to remove the non-accepted QoS Flows from the PDU Session(s) after the handover is completed. **Note** In N2 handover, if the direct path is not available between S-RAN and T-RAN, then SMF may decide to enable IDFT for data forwarding. So, if the SMF receives DL forwarding UP tunnel information from T-RAN for indirect data forwarding, it goes for session level data forwarding. If the SMF receives the Data forwarding response DRB List, it goes for DRB level data forwarding. If T-RAN does not provide the DL forwarding UP tunnel information, then SMF continues the HO without IDFT.
11b	The SMF sends the N4 Session Modification Request to the T-UPF. This request includes T-RAN SM N3 forwarding Information list, and an indication to allocate DL forwarding tunnel(s) for indirect forwarding.

Step	Description
11c	The T-UPF allocates Tunnel Info and returns an N4 Session Modification Response message to the SMF. The T-UPF SM N3 forwarding info list includes T-UPF N3 address, T-UPF N3 Tunnel identifiers for forwarding data.
11d	The SMF sends an N4 Session Modification Request to the S-UPF. This request includes T-RAN SM N3 forwarding Information list or T-UPF SM N3 forwarding Information list, and an indication to allocate DL forwarding tunnel(s) for indirect forwarding.
11e	The S-UPF allocates Tunnel Info and returns an N4 Session establishment Response message to the SMF. The S-UPF SM N3 forwarding Information list includes S-UPF N3 address and S-UPF N3 Tunnel identifiers for DL data forwarding.
11f	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response message per PDU session to the T-AMF. SMF does not fill the **qosFlowToBeForwardedList** for DRB level forwarding in the handover command. However, in case of Session level forwarding, the SMF sends **qosFlowToBeForwardedList** with the selected QFIs for forwarding (Based on the dataForwardingAccepted indication in the Handover Acknowledge).
12	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response message from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the T-AMF sends the Namf_Communication_CreateUEContext Response to the S-AMF.

Session Level Data Forwarding in IDFT

Upon getting the N2 setup response, SMF decodes the handover request acknowledge transfer and validates, if Data Forwarding Accepted IE is present in the message for existing flows. If the IE is present for at least one flow, SMF creates an uplink PDR to receive forwarded packets from source gNB and a FAR per flow with target gNB TEID received in DL Forwarding UP TNL Information IE to forward the packets to target gNB. Even if the SMF does not receive QoS Flow Setup Response List in the handover request acknowledgment, the SMF proceeds with session level forwarding, if the DL Forwarding UP TNL Information IE is present. SMF sends a handover command to the source gNB indicating the flows or which forwarding must be enabled (QoS flow to be forwarded item) and also the UPF TEID (DL Forwarding UP TNL Information IE) for forwarding the packets.

DRB Level Data Forwarding in IDFT

Upon receiving the Handover Request Acknowledgment, if SMF finds that the criteria for Session Level Forwarding is not met, and if the **Data Forwarding Response DRB List** IE is present, SMF proceeds with DRB Level Forwarding.

SMF triggers N4 Session Modification Request to create uplink PDRs (Packet Detection Rules) for each of the DRB (Data Radio Bearer) present in the DRB list. PDR is not associated to any QFI (QoS Flow Identifier). For each DRB, a tunnel is created to receive the data forwarded from the source gNB and each PDR is associated with an FAR (Forwarding Action Rules) to send those packets to the target gNB. Each FAR is associated to the target gNB TEID received the **DL Data Forwarding UP TNL Information** received for the corresponding DRB.

SMF includes the **Data Forwarding Response DRB List** IE with the UPF TEID for the corresponding DRB in Handover Command Transfer.

The following figure depicts the call flow for the execution phase of the N2-based inter NG-RAN handover procedure.

Figure 105: Inter NG-RAN Node N2-based Handover - Execution Phase

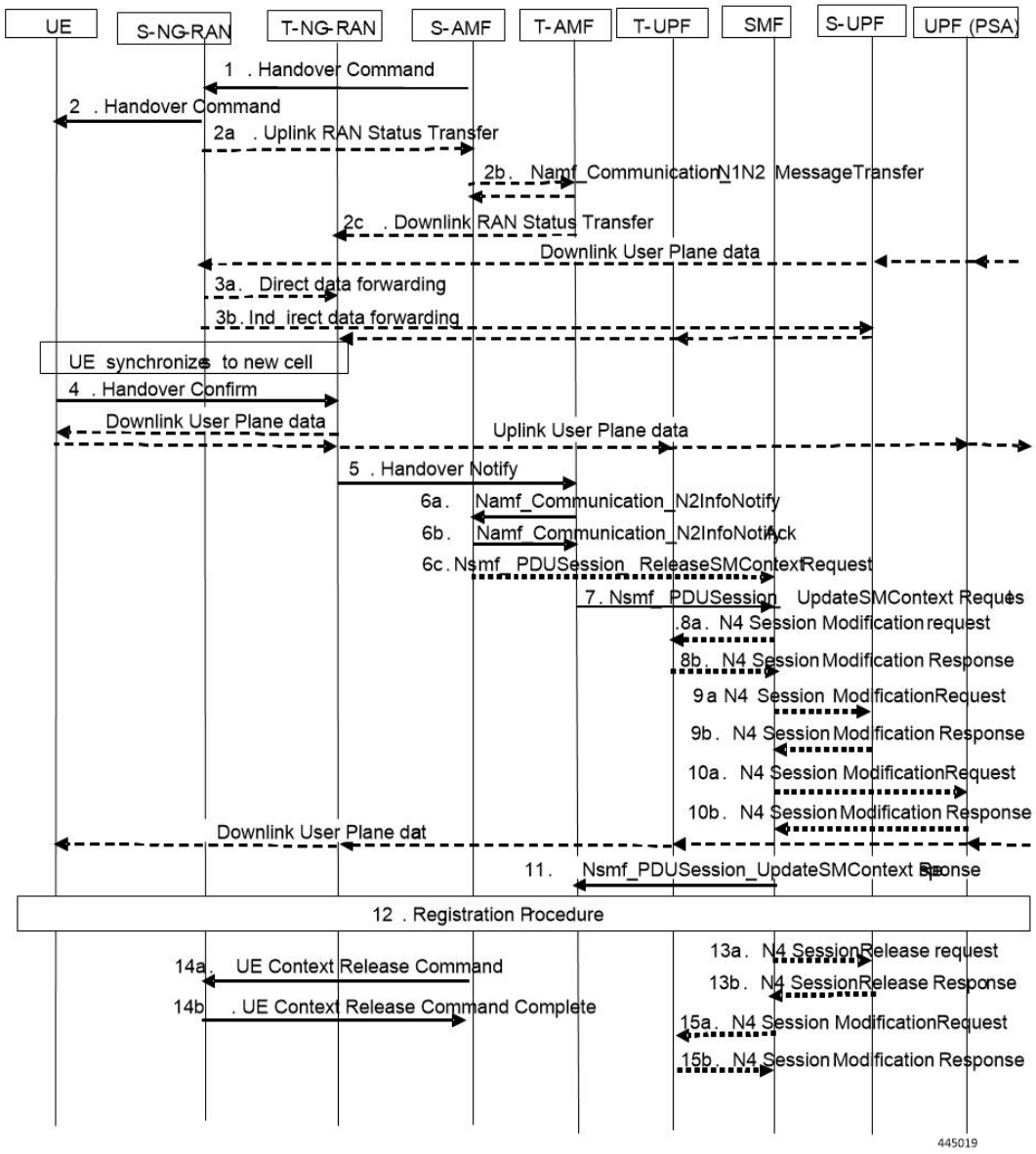


Table 170: Inter NG-RAN Node N2-based Handover Call Flow Description - Execution Phase

Step	Description
1	The Source AMF (S-AMF) sends the Handover Command to the Source NG-RAN (S-RAN). The Handover Command includes Target to Source transparent container, List Of PDU Sessions to be handed-over with N2 SM information containing information received from T-RAN during the handover preparation phase, and List Of PDU Sessions failed to set up. The SM forwarding info list includes T-RAN SM N3 forwarding info list for direct forwarding or S-UPF SM N3 forwarding info list for indirect data forwarding. The S-RAN uses the PDU Sessions failed to be setup list and the indicated reason for failure to decide whether to proceed with the N2 handover procedure.
2	The S-RAN sends a Handover Command (UE container) to the UE. The UE container is a UE part of the Target to Source transparent container, which is sent transparently from T-RAN via AMF to S-RAN and is provided to the UE by the S-RAN.
2a - 2c	The S-RAN sends the Uplink RAN Status Transfer message to the S-AMF. The S-RAN refrains from sending this message if none of the radio bearers of the UE are treated with Packet Data Convergence Protocol (PDCP) status preservation.
3	The T-RAN sends the uplink packets to the T-UPF and UPF (PSA). The UPF (PSA) sends the downlink packets to the S-RAN via S-UPF. The S-RAN forwards the downlink data toward the T-RAN for QoS flows or Data Radio Bearers (DRBs) subject to data forwarding. The data forwarding path is either direct (step 3a) or indirect forwarding (step 3b).
3a	Direct data forwarding is supported through Session Level and DRB level data forwarding.
3b	Indirect data forwarding is also supported through Session level and DRB level data forwarding.
4	After the UE has successfully synchronized to the target cell, it sends a Handover Confirm message to the T-RAN.
5	The T-RAN sends a Handover Notify message to the T-AMF. This message is sent to indicate that the handover is successful.
6a.	The T-AMF notifies to the S-AMF about the N2 handover notify received from the T-RAN by invoking the Namf_Communication_N2InfoNotify. The S-AMF uses a timer to supervise the release of resources in S-RAN.
6b	The S-AMF acknowledges by sending the Namf_Communication_N2InfoNotify ACK to the T-AMF.
6c	The S-AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the SMF. This request includes SUPI, PDU Session ID, and N2 SM Information (Secondary RAT Usage Data). If the PDU Session(s) is not accepted by the T-AMF, the S-AMF triggers the PDU Session Release procedure after the reception of N2 Handover Notify.

Step	Description
7	The T-AMF sends Nsmf_PDUSession_UpdateSMContext Request to the SMF. This request includes Handover Complete indication for PDU Session ID, UE presence in LADN service area, and N2 SM Information (Secondary RAT usage data). The T-AMF sends the Handover Complete indication per each PDU Session to the corresponding SMF to indicate the success of the N2 handover.
8a	If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF sends an N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the T-UPF.
8b	The T-UPF acknowledges by sending an N4 Session Modification Response message to the SMF.
9a	If the UPF is not reallocated, the SMF sends N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the S-UPF.
9b	The S-UPF acknowledges by sending the N4 Session Modification Response message to SMF.
10a	For non-roaming or local breakout roaming scenario, the SMF sends the N4 Session Modification Request message to PDU Session Anchor UPF, UPF (PSA). If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF provides the N3 AN Tunnel Info of T-RAN or the DL CN Tunnel Info of T-UPF. If the T-UPF is not inserted or an existing intermediate S-UPF is not reallocated, skip the step 10a and step 10b.
10b	The UPF (PSA) sends the N4 Session Modification Response message to the SMF. When there are multiple UPFs (PSA), perform step 10a and step 10b for each UPF (PSA).
11	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (PDU Session ID) to the T-AMF. The SMF confirms reception of Handover Complete.
12	The UE initiates the Mobility Registration Update procedure as defined in *3GPP TS 23.502*.
13a	If there is a source intermediate UPF, the SMF initiates resource release by sending an N4 Session Release Request (Release Cause) to the source UPF. This message is also used to release the indirect data forwarding resource in the S-UPF.
13b	The S-UPF acknowledges with an N4 Session Release Response message to confirm the release of resources. In case of indirect data forwarding, the resource of indirect data forwarding is also released.
14a	After the expiry of the timer (defined in step 6a), the AMF sends the UE Context Release Command.
14b	The source NG-RAN releases its resources related to the UE and responds with a UE Context Release Complete () message.
15a	If indirect forwarding applies and the UPF is reallocated, after the timer of indirect data forwarding expires, SMF sends the N4 Session Modification Request to the T-UPF. Then, the T-UPF releases the indirect data forwarding resources.
15b	The T-UPF acknowledges with an N4 Session Modification Response message to confirm the release of indirect data forwarding resources.

Limitations

The Xn-based handover with UPF reallocation is currently not supported.

OAM Support

This section describes the operations, administration, and maintenance information for this feature.

Statistics Support

The "smf_ran_failed_flows" metric is added to identify the number of QoS flows released by RAN as part of various call flow procedures including the Xn and N2 handover procedures.

The SMF uses the "xn_handover" label to account for Xn handovers. Similarly for the N2 handovers, the SMF uses the "n2_handover" label.

Wi-Fi Handover

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The SMF+PGW-C product supports Wi-Fi handovers. The cloud-based architecture supports the following Wi-Fi handovers in 5GS or EPS and non-3GPP untrusted access.

- EPC to non-3GPP untrusted Wi-Fi handover
- Non-3GPP untrusted Wi-Fi to EPC handover
- Non-3GPP untrusted Wi-Fi to 5GS handover with EPS fallback
- Non-3GPP untrusted Wi-Fi to 5GS handover
- 5GS to non-3GPP untrusted Wi-Fi handover

Handover Indication Support

The SMF+IWF rejects the Create Session Request received with handover (HO) indication even if the session does not exist. This support is applicable only to the 4G and Wi-Fi sessions.

The **gtpc message-handling create-session-request ho-ind new-call-reject** CLI command under access profile rejects the call with "Context Not Found".

For more information, see the Configuring Calls with Handover Indication, on page 500 section.

Alternate RAT Tunnel Creation for Wi-Fi

SMF creates an alternate RAT tunnel during the Wi-Fi attach procedure. This tunnel is reused when a subscriber moves to another RAT during handover.

Note Creation of an alternate RAT tunnel is prerequisite for the inter-PLMN handover support.

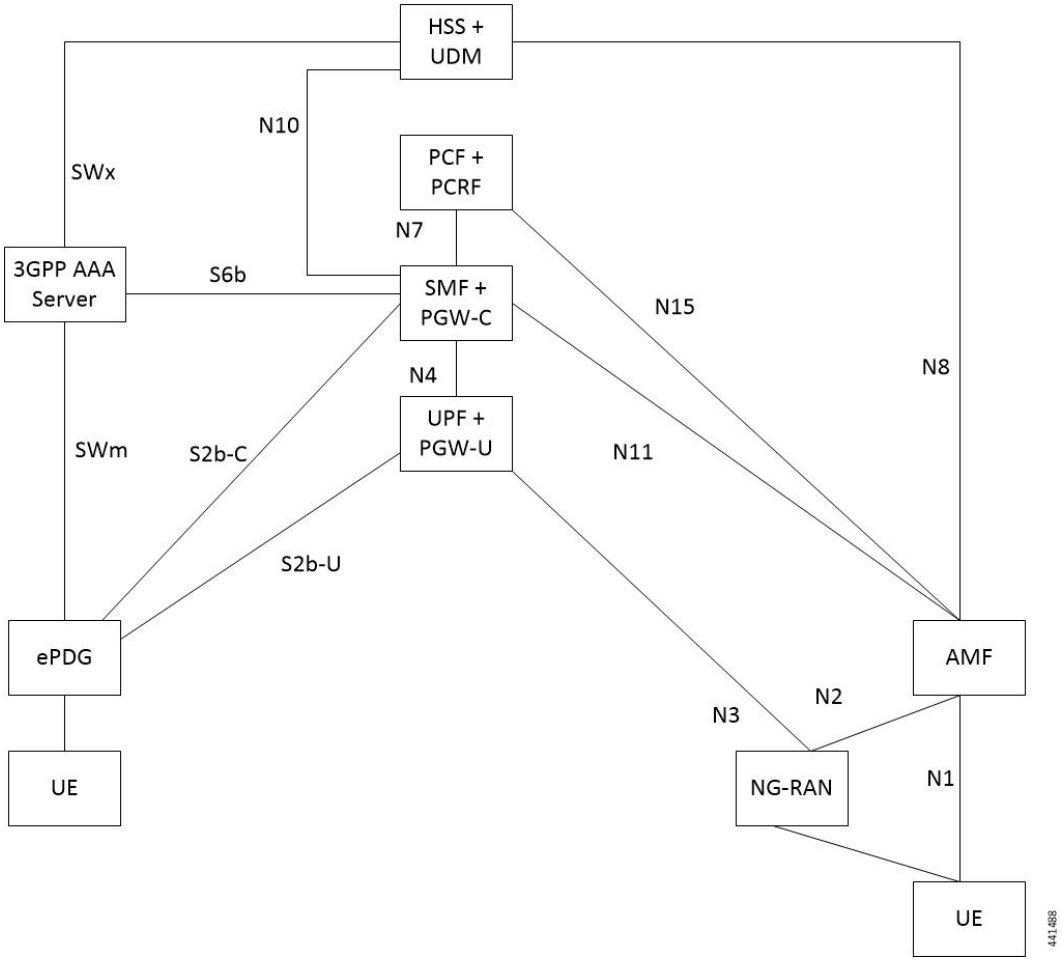
Architecture

The following sections describe the architecture for interworking between the ePDG or EPC and 5GS and the nonroaming architecture within the EPS using S5 and S2b interfaces.

ePDG and 5GS Interworking for Handover

The following figure illustrates the non-roaming architecture for interworking between the ePDG or EPC and 5GS.

Figure 106: Non-roaming Architecture for Interworking between ePDG or EPC and 5GS



The interworking between the ePDG and 5GS is similar to the interworking between the EPC and 5GS without the N26 interface. In this interworking, the IP address preservation occurs on the UEs on inter-system mobility. Fetching and saving the PGW-C and SMF and the corresponding APN and DNN information through the HSS and UDM makes interworking possible. In such networks, the AMF also supports interworking with UEs without the N26 interface during the initial registration in 5GC. The AMF may support interworking

with UEs without N26 in the Attach procedure in 5GS. In case of a non-3GPP untrusted Wi-Fi access, the ePDG does not communicate with the AMF because the N26 interface does not exist.

A 5GS supports network slicing and can interwork with the EPS in its PLMN or in other PLMNs. The SMF+PGW-C performs UDM registration for each UE with PGW-C FQDN and NSSAI values. With this registration, the AMF or ePDG identify the PGW-C IP-address from the UDM or HSS as part of the subscription information after the UE authorization is completed.

The mobility between 5GC to EPC does not ensure that all the active PDU sessions can be transferred to the EPC. During PDN connection establishment in the EPC, the UE allocates the PDU session ID and sends it to the PGW-C+SMF through the PCO.

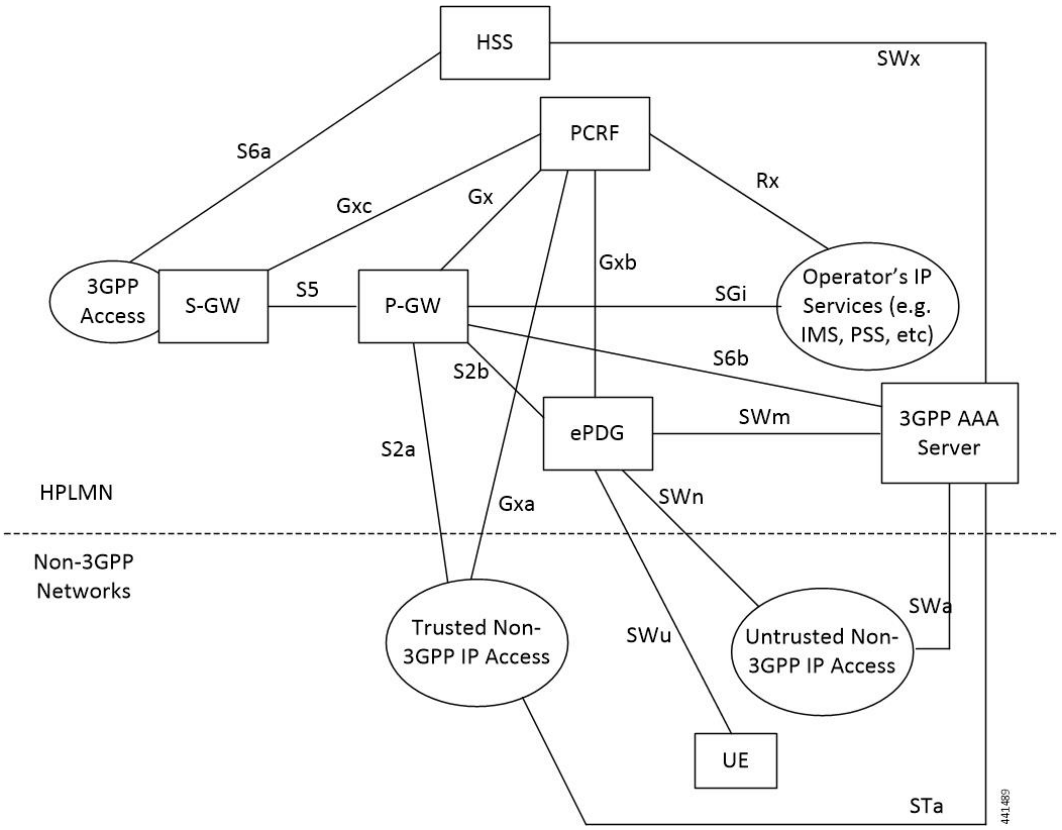
An S-NSSAI that is associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF. For example, the combination of PGW-C+SMF address and APN is sent to the UE in the PCO along with a PLMN ID to which the S-NSSAI relates. If the PGW-C+SMF supports multiple S-NSSAI and the APN is valid for multiple S-NSSAIs, the PGW-C+SMF selects only the S-NSSAI that is mapped to the subscribed S-NSSAIs of the UE.

The UE saves the S-NSSAI and the PLMN ID that is associated with the PDN connection. The UE derives the requested NSSAI through the received PLMN ID. The NAS registration request message includes the requested NSSAI. The RRC carries the registration request when the UE registers in 5GC. This scenario is applicable if the UE is non-roaming or the UE has configured NSSAI for the VPLMN in roaming case.

EPS and ePDG Interworking for Handover

The following figure illustrates the non-roaming architecture within the EPS using S5 and S2b interfaces.

Figure 107: Non-roaming Architecture Within EPS using S5, S2a, and S2b Interfaces



For 3GPP access to non-3GPP access untrusted Wi-Fi handover and for non-3GPP access untrusted Wi-Fi to 3GPP access handover, if a UE has multiple PDN connections to different APNs in the source access and the UE can route different simultaneously active PDN connections through different access networks, the UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them. This transfer can have the restriction that multiple PDN connections to the same APN have one access.

The transfer process can occur in the following scenarios:

- 3GPP access to non-3GPP access untrusted Wi-Fi handover
- Non-3GPP access untrusted Wi-Fi to 3GPP access handover

The UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them if the following conditions are met:

- The UE has multiple PDN connections to different APNs in the source access
- The UE can route different, but simultaneously active, PDN connections through different access networks."

The SMF supports untrusted Wi-Fi access for end-users over S2b interface with ePDG after establishment of IPSec connection between the end-user and ePDG.

For untrusted Wi-Fi to EPC handover, the SMF provides a PGW-C FQDN during UDM registration and fetches the subscription information.

During UE handover, the MME fetches PGW-C FQDN from the HSS. After authentication, the MME initiates GTPv2 create session request indicating handover. The SMF+PGW-C does not perform the UDM registration and subscription procedures while processing handover request. SMF+PGW-C ensures that GTPv2 MB request indicating handover is sent to perform data path switching from untrusted Wi-Fi to EPC.

For EPC to untrusted Wi-Fi handover, the HSS provides SMF+PGW-C FQDN after the subscriber authentication. When UE performs handover, after authentication HSS provides SMF+PGW-C FQDN. The ePDG initiates GTPv2 create session request indicating handover toward PGW after IPSec tunnel establishment. SMF+PGW-C performs the UDM registration and no subscription procedures exist while processing the handover request.

TFT Handling for Wi-Fi Handovers

In 4G and 5G deployment, the three-way audio or video multiparty call conference, and RCS message use cases, PGW-C ends up having more than four filters (it can go upto max 16 filters) for both UL and DL direction. SMF includes “EPS Bearer Level Traffic Flow Template (Bearer TFT)” is included in the GTPv2 CBReq or UBReq of BearerContextList. CBReq or UBReq carry maximum of 4 TFTs per bearer.

In case of three-way Audio/Video and multiparty call-conference, PCF tries to push the pccRules by adding different subscriber TFTs in multiple “N7 Policy Notify Req” messages. PGW-C handles the received “N7 Update Notify Req” in dedicated bearer establishment or update towards Wi-Fi or LTE by initiating GTPv2 CBReq or UBReq messages. SMF accommodates the received SDF Filters in TFT as it never crosses more than 256 Bytes (4 TFTs).

Note PGW-C don’t support more than 4TFTs received from PCF “N7 Policy Notify Req”.

PCF keeps pushing multiple pccRules for same bearer by sending “N7 Policy Notify Req” and over the period SMF ends up having 12-16 filters for case of multiparty call.

When subscriber moves from LTE to Wi-Fi or Wi-Fi to LTE or NR to Wi-Fi Handover call-model cases, SMF first establishes default bearer creation as part of HO. SMF then tries to send out CBReq for Dedicated bearer establishment by accommodating all 16 filters in “EPS Bearer Level Traffic Flow Template (Bearer TFT)” of bearer context list of the subscriber and if it fails to encode because of these restrictions. The SMF sends out CBReq without “EPS Bearer Level Traffic Flow Template (Bearer TFT)” IE based on HO type, SGW, MME, or ePDG rejects GTPv2 CBResp with Mandatory IE Incorrect with “TFT Semantic Errors”.

After receiving CBResp from SGW or ePDG, SMF doesn’t free up policy or charging resources for respective failed bearers and that leads to further stale entries on SMF and UPF which leads to system inconsistency for that subscriber with “EBI Mismatch – 408 Error Voice Call Failure Wi-Fi HOs”.

Standards Compliance

The Wi-Fi handovers feature complies with the following standards:

- 3GPP TS 23.502 V15.2.0 (2018-09)
- 3GPP TS 23.402 V15.3.0 (2018-03)
- 3GPP TS 29.214 V15.5.0 (2018-03)

How it Works

This section describes the Wi-Fi to LTE handover, Wi-Fi handover with EPS fallback, and Wi-Fi to 5GS handover.

EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the EPC to non-3GPP untrusted Wi-Fi handover call flow.

Figure 108: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

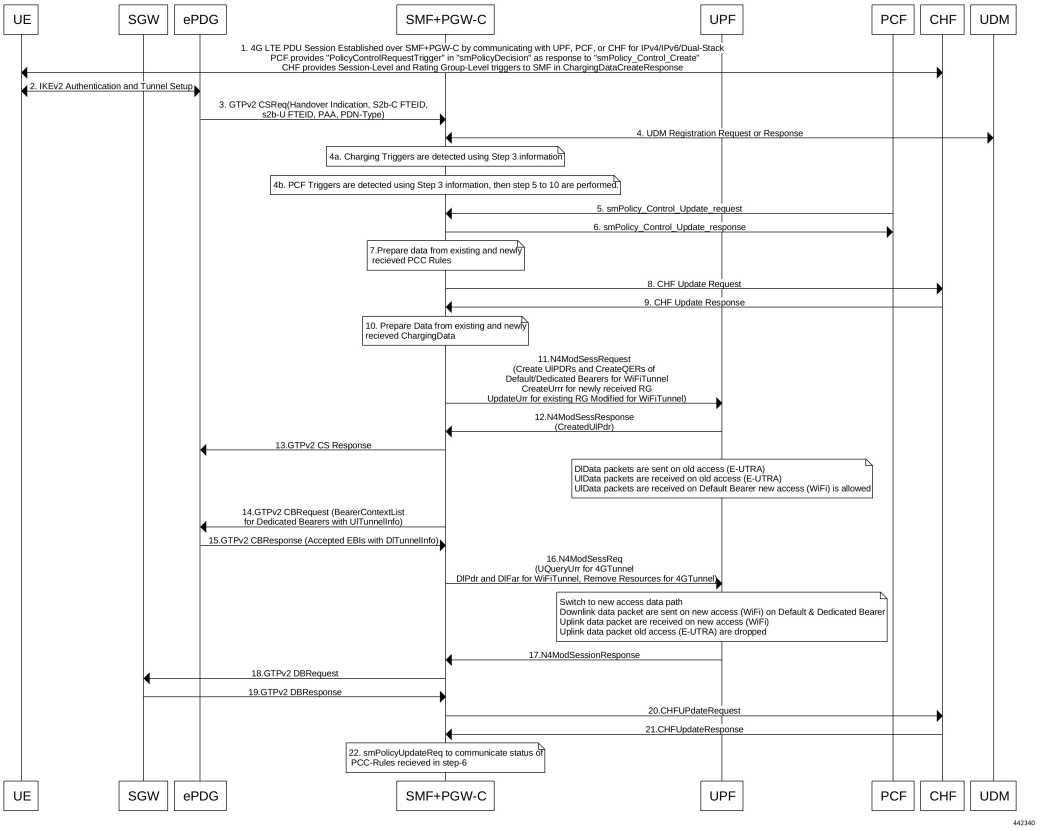


Table 171: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE is attached to the 3GPP access network. The SMF+PGW-C communicates with UPF, PCF, and CHF for IPv4, IPv6, or dual-stack to establish 4G LTE PDU session. The PCF sends the Policy Control Request trigger, which is the SM policy decision, in response to SM policy control create. The CHF provides session-level or rating-group-level triggers to the SMF in Charging Data Create response.
2	The UE connects to an untrusted non-3GPP access and an ePDG is selected through the ePDG selection process. Then, the UE initiates the handover attach procedure as defined in 3GPP TS 23.402, section 8.6.2.1. After the IKE tunnel is established between the UE and ePDG and after the UE is authenticated over SWm interface with AAA server, the UE initiates IKE authentication (IKE_AUTH). The IKE_AUTH includes configuration parameters of the earlier assigned IPv4 or IPv6 addresses in the EPC and P-CSCF and the DNS options.

Step	Description
3	The ePDG sends a Create Session Request to the PGW-C. This request includes the following details: • IMSI • APN • Handover indication • RAT type • ePDG TEID of the Control Plane • ePDG address for the User Plane • ePDG TEID of the User Plane • EPS bearer identity • User location The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and is included in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session Request to allow the PDN gateway to reallocate the same IP address or the prefix assigned to the UE. This IP address or prefix is assigned while UE is connected to the 3GPP IP access and initiates the policy modification procedure with PCF.
4a	The SMF performs UDM registration by updating the PGW-C FQDN with UDM. The UDM registration does not occur during the session establishment with EPC.
4b	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4c	The SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to the PCF.
6	The PCF includes new or updated PCC rules and sends the SM Policy Control Update response. The Update response includes information on the SM policy decision.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If new PCC rules are received in Step 6 with new Rating Group that requires quota information, SMF sends the Charging Update request to CHF. SMF also includes new access parameters for the PDU session information.
9	CHF sends the Charging Update Response with multi-unit information that contains quota information for the requested rating-group in Step 8 to SMF. CHF may also send the new quota information for the existing rating-group of EPC session.
10	SMF processes the information that is received as Charging Update response from CHF.

Step	Description
11	SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, and update on URR for modified quota information.
12	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, PGW-C S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SMF sends the GTPv2 Create Bearer request to S-GW. This request includes information on bearer context list, which contains DL tunnel information to end-user, to be created.
15	S-GW sends the GTPv2 Create Bearer response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
16	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to create the DL PDR and DL FAR with DL tunnel information for each bearer, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
17	UPF sends the usage report as N4 Session Modification response to SMF.
18	SMF+PGW-C sends the GTPv2 DB request to S-GW. This request includes EBI or list of EBIs.
19	S-GW sends the GTPv2 DB response to SMF+PGW-C.
20	SMF sends the Charging Update request to CHF. This request includes the PDU session information with the new access params and multi-usage report containing details on the access params and usage report that is received in Step 8
21	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information may include new quota information for the existing rating-groups.
22	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502, section 4.3.3.2.

Note The preceding call flow is based on the 3GPP specification and Cisco implementation has proprietary optimisations. For more information, contact your Cisco account representative.

Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to EPC handover call flow.

Figure 109: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

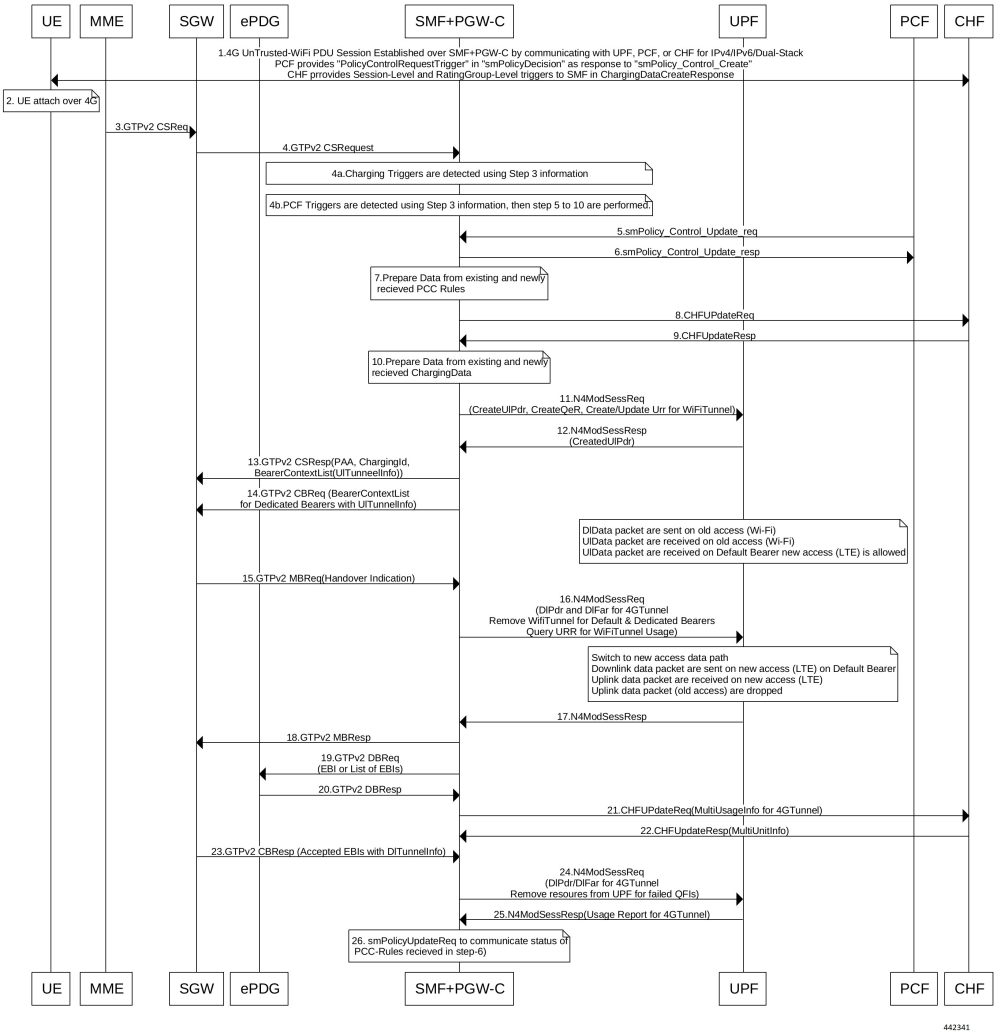


Table 172: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE discovers the E-UTRAN access and hands over the sessions from the currently used non-3GPP access system to E-UTRAN. For details on UE discovery of the 3GPP access system, see 3GPP TS 23.401, section 4.8. UE sends an Attach request to MME for the Handover Attach request type. E-UTRAN routes the messages received from UE to MME as defined in 3GPP TS 23.401. UE includes the one of the APNs which are corresponding to the PDN connections in the source non-3GPP access. The APN is provided as defined in 3GPP TS 23.401.

Step	Description
3	MME and HSS perform authentication, which is followed by location update procedure and subscriber data retrieval to receive the APN information. The MME selects an APN, an SGW and PDN gateway as defined in 3GPP TS 23.401. MME sends a Create Session Request message to SGW. This request includes information on IMSI, MME context ID, PDN-GW address, handover indication for the “handover” request type, and APN.
4	SGW sends a Create Session Request, which is handover indication, message to PDN-GW in the HPLMN as described in 3GPP TS 23.401. As the MME includes the handover indication information in the Create Session Request message, the SGW sends the GTPv2 Create Session Request message to PDN GW. This message includes details on IMSI, APN, handover indication, RAT type, S5-C TEID, S5-U TEID of the user plane, EBI, and user location information. The RAT type indicates the 3GPP IP access E-UTRAN technology type. If the UE supports IP address preservation and is included in PAA, the SGW configures the handover indication in the Creation Session Request. With this configuration, the PDN GW re-allocates the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access. With this configuration, SGW initiates the Policy Modification Procedure to the PCF. As the handover indication is includes, the PDN GW does not switch the tunnel from non-3GPP IP access to 3GPP access system at this point. SMF does not perform the UDM Registration as the registration happens during the Wi-Fi session establishment.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4b	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
6	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request, with the new rating-group having quota information, to CHF. This request includes the PDU session information with the new access params.
9	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the rating-group and the existing rating-group of EPC session, if any.
10	SMF prepares the charging data of the received Charging Update Response that CHF sent.
11	SMF sends the N4 Session Modification Request to UPF. This request includes the details on creation of UL and DL PDR, creation of QER, creation of URR for received new rating-group quota information, updated URR for modified quota information, and creation of FAR.
12	UPF sends the UL tunnel information in the created PDR as N4 Session Modification response to SMF.

Step	Description
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, PGW-C S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SGW sends the Modification Bearer request with handover indication to PGW for data path switching from Wi-Fi tunnel to 4G tunnel.
15	PGW sends the N4 Session Modification request to delete the Wi-Fi tunnel and to configure DL tunnel information that is received in GTPv2 Create Session request for 4G tunnel in Step 4.
16	UPF sends the N4 Session Modification response to SMF.
17	SMF sends the GTPv2 Create Session request, which includes the bearer context list, to SGW. This list includes the DL Tunnel information for the end-user.
18	SGW sends the GTPv2 Create Session response to SMF. This response includes details on request accepted or request accepted partially and bearer contexts.
19	ePDG sends the GTPv2 Create Bearer resp (accepted EBIs with DL tunnel info to SMF
20	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to update the DL FAR with the DL tunnel information, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
21	UPF sends the N4 Session Modification Response with usage report to SMF.
22	SMF sends the Charging Update request to CHF. This request includes the PDU session information with new access params and multi-usage report consisting of access-params and usage report that is received in Step 8.
23	CHF sends the Charging Update Response with multi-unit information that contains quota information for the existing rating-groups to SMF.
24	SMF+PGW-C initiates the GTPv2 DB Request toward SGW by including EBI or EBI list.
25	SGW sends the GTPv2 DB Response toward SMF+PGW-C.
26	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response. PCF sends the SM policy decision as SM Policy Control Update response. SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

Note The preceding call flow is based on the 3GPP specification and Cisco implementation has proprietary optimisations. For more information, contact your Cisco account representative.

Non-3GPP Untrusted Wi-Fi to 5GS Handover with EPS Fallback Call Flow

This section describes the non-3GPP untrusted Wi-Fi to 5GS handover with EPS fallback call flow.

Figure 110: Non-3GPP Untrusted Wi-Fi to 5GS Handover with EPS Fallback Call Flow

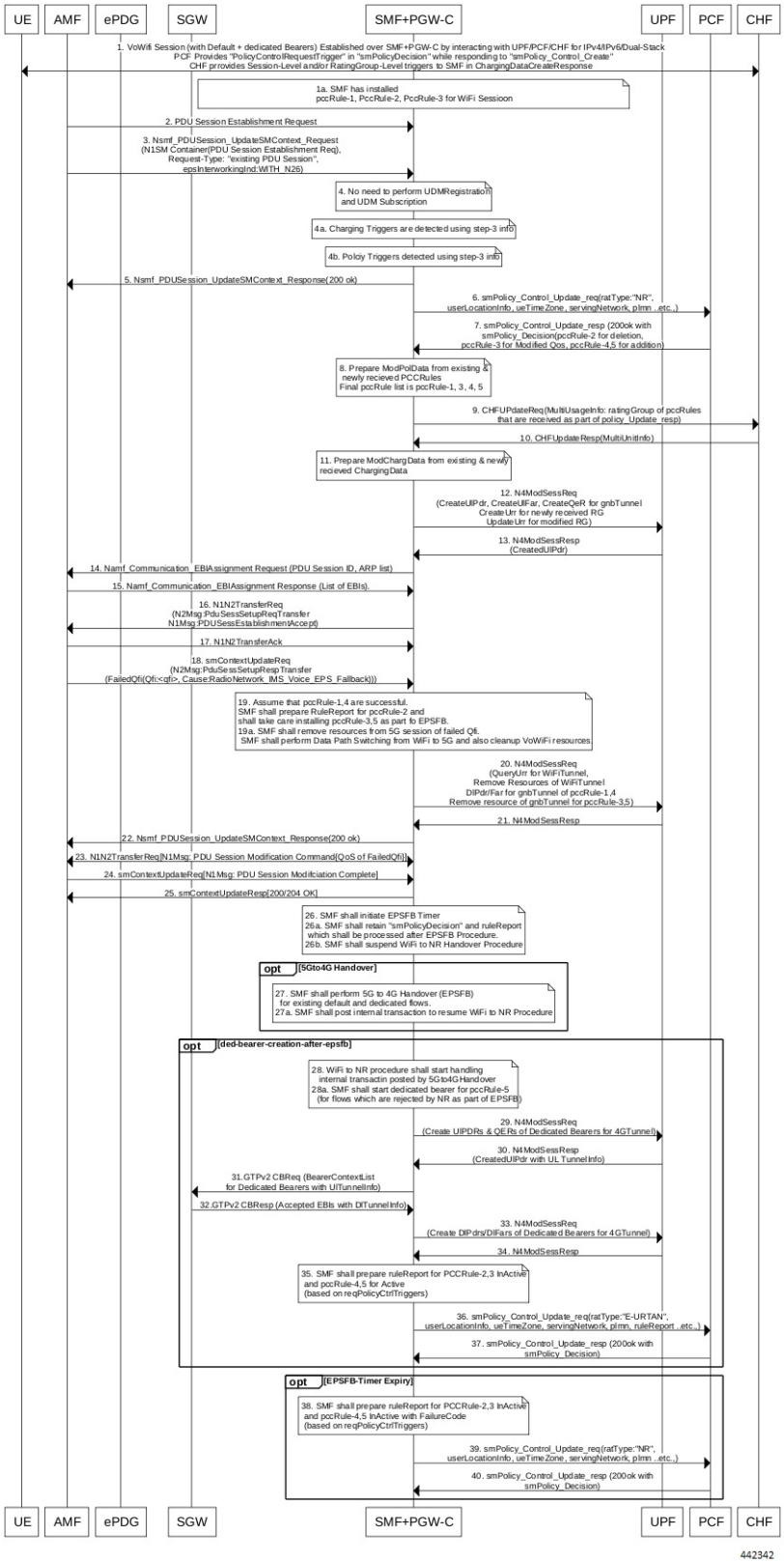

UE
AMF
ePDG
SGW
SMF+PGW-C
UPF
PCF
CHF
1. VoWifi Session (with Default + dedicated Bearers) Established over SMF+PGW-C by interacting with UPF/PCF/CHF for IPv4/IPv6/Dual-Stack
PCF Provides "PolicyControlRequestTrigger" in "smPolicyDecision" while responding to "smPolicy_Control_Create"
CHF provides Session-Level and/or RatingGroup-Level triggers to SMF in ChargingDataCreateResponse
1a. SMF has installed
pccRule-1, PccRule-2, PcRule-3 for WiFi Sessioon
2. PDU Session Establishment Request
3. Nsmf_PDUSession_UpdateSMContext_Request
(N1SM Container(PDU Session Establishment Req),
Request-Type: "existing PDU Session",
epsInterworkingInd:WITH_N26)
4. No need to perform UDMRegistration
and UDM Subscription
4a. Charging Triggers are detected using step-3 info
4b. Policy Triggers detected using step-3 info
5. Nsmf_PDUSession_UpdateSMContext_Response(200 ok)
6. smPolicy_Control_Update_req(ratType:"NR",
userLocationInfo, ueTimeZone, servingNetwork, plmn ..etc..)
7. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision(pccRule-2 for deletion,
pccRule-3 for Modified Qos, pccRule-4,5 for addition)
8. Prepare ModPolData from existing &
newly recieved PCCRules
Final pccRule list is pccRule-1, 3, 4, 5
9. CHFUPdateReq(MultiUsageInfo: ratingGroup of pccRules
that are received as part of policy_Update_resp)
10. CHFUpdateResp(MultiUnitInfo)
11. Prepare ModChargData from existing & newly
recieved ChargingData
12. N4ModSessReq
(CreateUlPdr, CreateUlFar, CreateQeR for gnbTunnel
CreateUrr for newly received RG
UpdateUrr for modified RG)
13. N4ModSessResp
(CreatedUlPdr)
14. Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list)
15. Namf_Communication_EBIAssignment Response (List of EBIs).
16. N1N2TransferReq
(N2Msg:PduSessSetupReqTransfer
N1Msg:PDUSessEstablishmentAccept)
17. N1N2TransferAck
18. smContextUpdateReq
(N2Msg:PduSessSetupRespTransfer
(FailedQfi(Qfi:<qfi>, Cause:RadioNetwork_IMS_Voice_EPS_Fallback)))
19. Assume that pccRule-1,4 are successful.
SMF shall prepare RuleReport for pccRule-2 and
shall take care installing pccRule-3,5 as part to EPSFB.
19a. SMF shall remove resources from 5G session of failed Qfi.
SMF shall perform Data Path Switching from WiFi to 5G and also cleanup VoWiFi resources
20. N4ModSessReq
(QueryUrr for WiFiTunnel,
Remove Resources of WiFiTunnel
DlPdr/Far for gnbTunnel of pccRule-1,4
Remove resource of gnbTunnel for pccRule-3,5)
21. N4ModSessResp
22. Nsmf_PDUSession_UpdateSMContext_Response(200 ok)
23. N1N2TransferReq[N1Msg: PDU Session Modification Command(QoS of FailedQfi)]
24. smContextUpdateReq[N1Msg: PDU Session Modificiation Complete]
25. smContextUpdateResp[200/204 OK]
26. SMF shall initiate EPSFB Timer
26a. SMF shall retain "smPolicyDecision" and ruleReport
which shall be processed after EPSFB Procedure.
26b. SMF shall suspend WiFi to NR Handover Procedure
opt
[5Gto4G Handover]
27. SMF shall perform 5G to 4G Handover (EPSFB)
for existing default and dedicated flows.
27a. SMF shall post internal transaction to resume WiFi to NR Procedure
opt
[ded-bearer-creation-after-epsfb]
28. WiFi to NR procedure shall start handling
internal transactin posted by 5Gto4GHandover
28a. SMF shall start dedicated bearer for pccRule-5
(for flows which are rejected by NR as part of EPSFB)
29. N4ModSessReq
(Create UlPDRs & QERs of Dedicated Bearers for 4GTunnel)
30. N4ModSessResp
(CreatedUlPdr with UL TunnelInfo)
31.GTPv2 CBReq (BearerContextList
for Dedicated Bearers with UlTunnelInfo)
32.GTPv2 CBResp (Accepted EBIs with DlTunnelInfo)
33. N4ModSessReq
(Create DlPdrs/DlFars of Dedicated Bearers for 4GTunnel)
34. N4ModSessResp
35. SMF shall prepare ruleReport for PCCRule-2,3 InActive
and pccRule-4,5 for Active
(based on reqPolicyCtrlTriggers)
36. smPolicy_Control_Update_req(ratType:"E-URTAN",
userLocationInfo, ueTimeZone, servingNetwork, plmn, ruleReport ,etc..)
37. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision)
opt
[EPSFB-Timer Expiry]
38. SMF shall prepare ruleReport for PCCRule-2,3 InActive
and pccRule-4,5 InActive with FailureCode
(based on reqPolicyCtrlTriggers)
39. smPolicy_Control_Update_req(ratType:"NR",
userLocationInfo, ueTimeZone, servingNetwork, plmn ..etc..)
40. smPolicy_Control_Update_resp (200ok with
smPolicy_Decision)
442342

Table 173: Non-3GPP Untrusted Wi-Fi to 5GS Handover with EPS Fallback Call Flow Description

Step	Description
1	The UE and the ePDG interact with each other through untrusted non-3GPP access to establish one or more PDU sessions. With the 5G NAS capability of UE, ePDG selects a combined PGW-C and SMF. The UE sends the PDU session ID to the combined PGW-C and SMF.
1a	The SMF installs the PccRule-1, PccRule-2, PccRule-3 for the WiFi session.
2	The AMF sends the PDU Session Establishment request through 3GPP access to the SMF. This request includes details on the following: • PDU session ID • Requested PDU session type • Requested SSC mode • 5GSM capability PCO • SM PDU DN request container • Number of packet filters • Optional requested always-on PDU session The request type with an existing PDU session indicates switching between 3GPP access and non-3GPP access or to a PDU session handover from an existing PDN connection in EPC.

Step	Description
3	If the request type is “Existing PDU Session”, the AMF selects the SMF based on SMF-ID that is received from the UDM. An error occurs for this request type on meeting any of the following conditions: • If the AMF does not identify the PDU Session ID or the subscription context that the AMF received from UDM during the registration. • If the subscription profile update notification procedure contains no SMF ID corresponding to the PDU Session ID. Then, the AMF updates the Access Type stored for the PDU session. If the request type with an existing PDU session refers to a PDU session that moved between 3GPP access and non-3GPP access and if the S-NSSAI of the PDU session is available in the Allowed NSSAI of the target access type, the PDU Session Establishment procedure begins when the SMF ID corresponding to the PDU Session ID and the AMF are part of the same PLMN. The AMF sends the NSMF PDU Session Create SM Context request with the request type “Existing PDU Session” to the SMF. This request includes information on the following: • SUPI • DNN • S-NSSAIs • PDU Session ID • AMF ID • Request Type • PCF ID • Priority Access • N1 SM container including the PDU Session Establishment Request • User location information • Access Type • PEI • GPSI • Subscription For PDU Session Status Notification • DNN Selection Mode The SMF analyzes the existing PDU session from the PDU Session Establishment request using SUPI+PDU-Session-ID. The SMF also compares the IPv4 or IPv6 addresses of the received UE against the retrieved PDU session IPv4 or IPv6 addresses. The SMF rejects the request if the session is not retrieved or the IPv4 or IPv6 addresses do not match.
4	The SMF does not perform UDM registration as it has already been registered with UDM during the WiFi session establishment.

Step	Description
4a	The SMF detects the Charging triggers with the information available in Step 3 against the chrgTriggers received during the WiFi session.
4b	The SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the earlier communication with PCF during the Wi-Fi session.
5	The SMF sends the NSMF PDU Session Create SM Context response to the AMF. This response includes the cause, SM Context ID, or N1 SM container with PDU session rejection cause.
6	Based on the detected armed Policy Control Triggers that are received in Step 4a, the SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to the PCF.
7	The PCF sends the SM policy decision through the SM Policy Control Update response by including new or updated PCC rules.
8	Based on the information received in Step 7 and the existing policy data of Wi-Fi session, the SMF prepares the ModPolData.
9	If the SMF receives new PCC rules in Step 7, the SMF sends the Charging Update request to the CHF with new rating-group for quota information. This request includes the PDU session information with the new access parameters.
10	The CHF sends the multi-unit information in the Charging Update response to the SMF. The multi-unit information includes quota information for the rating-groups received in Step 9 and for the existing rating-group of Wi-Fi session.
11	The SMF processes the ModChargingData that is received in the Charging Update response from the CHF.
12	The SMF sends the N4 session modification request to the UPF for gNB tunnel. This request includes details on the following: • Create uplink PDR. • Create QER. • Create URR (for new rating group quota information) • Update on URR (for modified quota information) • Create FAR
13	The UPF sends the UL tunnel information in the created PDR as the N4 Session Modification response to the SMF.
14	The SMF sends the EBI assignment request to the AMF. This request includes the ARP list for the PDU session ID.
15	The AMF sends the list of EBIs as the EBI Assignment response to the SMF.

Step	Description
16	The SMF sends the N1 N2 Transfer Request to the AMF. This request includes the N2 message as “PDU Session Resource Setup Request Transfer” with supported QFI list and UL Tunnel Information of gNB tunnel. This request also includes the N1 message as “PDU Session Establishment Accept” with authorized QoS rule, authorized QoS flow description, EPCO, PDN addresses, and session AMBR values.
17	The AMF sends the N1 N2 Transfer acknowledgment to the SMF.
18	The AMF sends the SM Context Update request to the SMF with one of the following: • “PDU Session Resource Set up Unsuccess Transfer” N2 message with “IMS voice EPS fallback or RAT fallback triggered” cause. • “PDU Session Resource Setup Response Transfer” with “QoS Flow Failed Setup List” cause as “IMS voice EPS fallback or RAT fallback triggered”.
19	With the assumption that the pccRule-1 and pccRule-4 are successful, the SMF prepares the rule report for pccRule-2 and installs the pccRule-3 and pccRule-5 as part of the EPS fallback.
19a	The SMF deletes the resources from 5G session of failed QFI, and the VoWiFi resources. Further, the SMF performs the data path switching from WiFi to 5G.
20	The SMF sends the N4 Session Modification request to the UPF by performing the following operations: • QueryUrr for WiFiTunnel • Remove the resources of WiFi tunnel. • Create DlPdr/Far for gNB tunnel of pccRule-1 and pccRule-4. • Remove the resources of gNB tunnel for failed QFI of pccRule-3 and pccRule-5.
21	The UPF sends the N4 Session Modification response along with Usage Report for WiFi session to the SMF.
22	The SMF sends the SM Context Update response to the AMF.
Note	The SMF performs the Step 23 through the Step 25 if there are any failed QFIs.
23	The SMF initiates the N1 N2 Transfer request with N1Msg: PDU Session Modification Command{QoS of FailedQfi}. The SMF receives the N1 N2 Transfer response from the AMF.
24	The SMF receives the SM Context Update request with N1Msg: PDU Session Modification Complete from the AMF.
25	The SMF sends the 204 OK in the SM Context Update response to the AMF.
26	The SMF initiates the EPS fallback timer by retaining the "smPolicyDecision" and ruleReport which are processed after the EPS fallback procedure. Also, the SMF suspends the WiFi to NR handover procedure until the EPS fallback procedure is executed or the EPS fallback timer is expired.

Step	Description
27	The SMF performs 5G to 4G handover (EPS fallback) for the existing default and dedicated flows. The SMF posts the internal transaction to resume the WiFi to NR procedure.
28	The WiFi to NR procedure starts handling the internal transaction.
28a	The SMF starts the dedicated bearer creation procedure for pccRule-5 (for flows which are rejected by NR as part of the EPS fallback).
29	The SMF initiates the N4 Modification request with Create UlPDRs, QERs, URRs (if any) for pccRules which are rejected as part of WiFi to NR handover with EPS fallback reason.
30	The SMF receives the N4 Modification response with CreatedUlPDR which contains the uplink tunnel information for the dedicated bearers.
31	The SMF initiates the GTPv2 Context Bearer request (bearer context list for dedicated bearers with uplink tunnel information).
32	The SMF receives the GTPv2 Context Bearer response (accepted EBIs with downlink tunnel information).
33	The SMF initiates the N4 Modification Session request (Create DlPdrs/DlFars of Dedicated Bearers for 4G tunnel) towards the UPF.
34	The SMF receives the N4 Modification Session response from the UPF.
35	The SMF prepares the ruleReport for PCCRule-2,3 InActive and pccRule-4,5 for Active based on the request Policy Control Triggers.
36	The SMF sends the SM Policy Control Update request with ratType:"E-URTAN", userLocationInfo, ueTimeZone, servingNetwork, plmn, ruleReport, and so on.
37	The SMF receives 200 OK with SM Policy Decision in the SM Policy Control Update response.
Note	The SMF performs Step 38 through Step 40 only when the Step 27 through Step 37 is not executed, that is, when the EPS fallback procedures are not triggered.
38	The SMF prepares the ruleReport for PCCRule-2,3 InActive and pccRule-4,5 InActive with FailureCode based on the request Policy Control Triggers.
39	The SMF sends the SM Policy Control Update with ratType:"NR", userLocationInfo, ueTimeZone, servingNetwork, PLMN, ruleReport, and so on.
40	The PCF sends the SM Policy Decision in the SM Policy Control Update response. The SMF processes the SM Policy Decision and handles it as PCF-initiated Modification procedure as defined in *3GPP TS 23.502, section 4.3.3.2*.

Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to 5GS handover call flow.

Figure 111: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

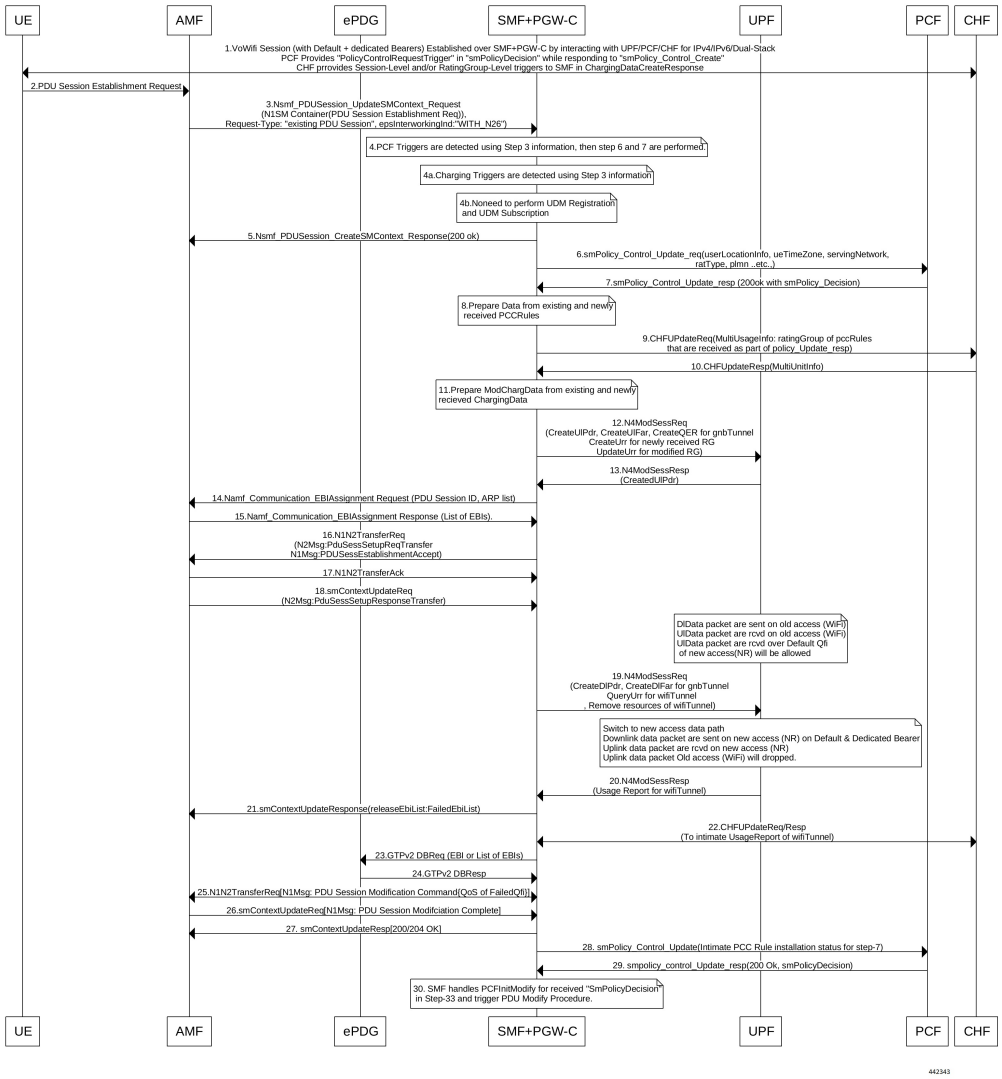


Table 174: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	UE sends the PDU Session Establishment request through 3GPP access to AMF. This request includes details on PDU session ID, requested PDU session type, requested SSC mode, 5GSM capability PCO, SM PDU DN request container, number of packet filters, and an optional requested always-on PDU session. The request type with an existing PDU session indicates switching between 3GPP access and non-3GPP access or to a PDU session handover from an existing PDN connection in EPC.

Step	Description
3	If the request type is “Existing PDU Session”, the AMF selects the SMF based on SMF-ID that is received from UDM. For this request type, if AMF does not identify the PDU Session ID or the subscription context that the AMF received from UDM during the Registration or if the subscription profile update notification procedure contains no SMF ID corresponding to the PDU Session ID, an error occurs. Then, AMF updates the Access Type stored for the PDU session. If the request type with an existing PDU session refers to a PDU session that moved between 3GPP access and non-3GPP access and if the S-NSSAI of the PDU session is available in the Allowed NSSAI of the target access type, the PDU Session Establishment procedure is performed when the SMF ID corresponding to the PDU Session ID and the AMF are part of the same PLMN. AMF sends the NSMF PDU Session Create SM Context Request with the request type “Existing PDU Session” to SMF. This request includes information on SUPI, DNN, S-NSSAIs, PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container including the PDU Session Establishment Request, User location information, Access Type, PEI, GPSI, Subscription For PDU Session Status Notification, DNN Selection Mode. SMF analyzes the existing PDU session from the PDU Session Establishment request using SUPI+PDU-Session-ID. SMF also compare the IPv4 or IPv6 addresses of the received UE against the retrieved PDU session IPv4 or IPv6 addresses. SMF reject the request if the session is not retrieved or IPv4 or IPv6 addresses do not match.
4	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the earlier communication with PCF during Wi-Fi session.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during Wi-Fi session.
4b	SMF does not perform the UDM registration as happens during Wi-Fi Session Establishment.
5	SMF sends the NSMF PDU Session Create SM Context response to AMF. This response includes the cause, SM Context ID or N1 SM container with PDU session rejection cause.
6	Based on the detected armed Policy Control Triggers that are received in Step 4a, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
7	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
8	Based on the information received in Step 7 and existing policy data of Wi-Fi session, SMF prepares the information.
9	If SMF receives new PCC rules in Step 7, the SMF sends the Charging Update request to CHF with new rating-group for quota information. This request includes the PDU session information with the new access params.
10	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes quota information for the rating-groups received in Step 9 and for the existing rating-group of Wi-Fi session.
11	SMF processes the data that is received Charging Update response from CHF.

Step	Description
12	SMF sends the N4 session modification request to UPF for gnb tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, update on URR for modified quota information, and creation of FAR.
13	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
14	SMF sends the EBI assignment request to AMF. This request includes the ARP list for the PDU session ID.
15	AMF sends the list of EBIs as response to SMF.
16	SMF sends the N1 N2 Transfer Request toward AMF. This request includes the N2 message as "PDU Session Resource Setup Request Transfer" with supported QFI list and UL Tunnel Information of gnb Tunnel. This request also includes the N1 message as "PDU Session Establishment Accept" with authorized QoS rule, authorized QoS flow description, EPCO, PDN addresses, and session AMBR values.
17	AMF sends the N1 N2 Transfer acknowledgement to SMF.
18	AMF sends the SM Context Update request to SMF with "PDU Session Resource Setup Response Transfer" containing the failed QFI list and the DL tunnel information.
19	SMF sends the N4 session modification request to UPF for the gnb tunnel resources. This request is to create the DL PDR, to create DL FAR with DL tunnel information, include details on RAT-change and delete resources for Wi-Fi tunnel. SMF also deletes the N4 resources of gnb tunnel for received failed QFI list.
20	UPF sends the N4 Session Modification Response with the usage report to SMF.
21	SMF sends the SM Context Update response to AMF.
22	SMF sends the Charging Update request to PCF. This request includes the PDU session information with new access params and multi-usage report with old access-params and usage report that is received in Step 18. SMF receives the Charging Update response that includes new quota information for existing rating-groups.
23	SMF+PGW-C initiates the GTPv2 DB request, which includes EBIs, to ePDG.
24	ePDG sends the GTPv2 DB response to SMF+PGW-C.
25	SMF receives the SM Context Update request with N1 message for PDU session modification completion from AMF.
26	SMF sends 200/204 OK as SM Context Update response to AMF.
27	SMF sends the SM policy decision as SM Policy Control Update response to AMF.
28	SMF sends the SM Policy Control Update request to PCF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of N2 message.

Step	Description
29	PCF sends the SM policy decision as SM Policy Control Update response to SMF.
30	SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the 5GS to non-3GPP untrusted Wi-Fi handover call flow.

Figure 112: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

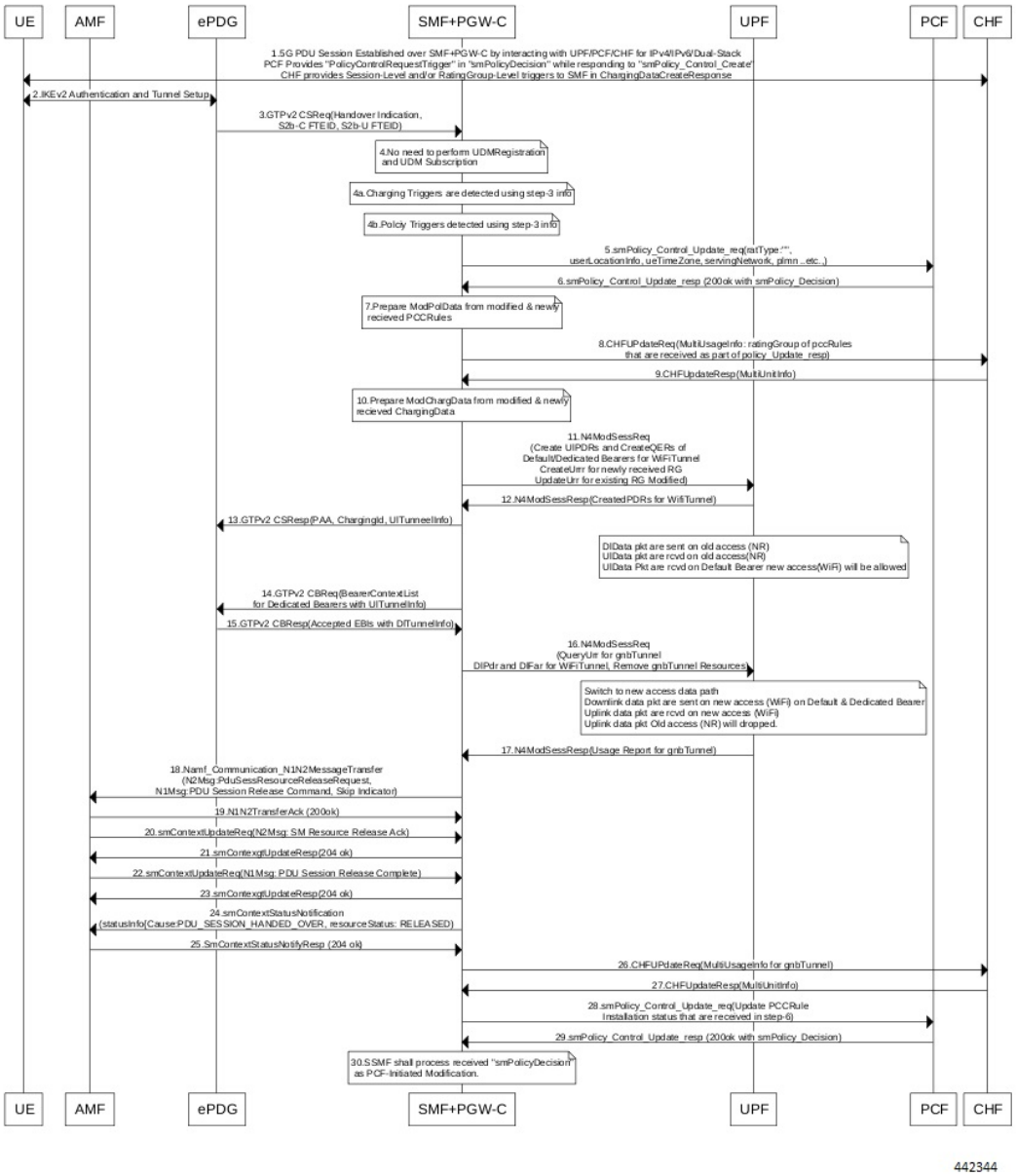


Table 175: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE and the SMF or the UPF communicate through the NG-RAN to establish one or more PDU sessions.
2	The UE connects to an untrusted non-3GPP access and selects an ePDG. Then, the UE initiates the handover attach procedure, as defined in 3GPP TS 23.402, section 8.6.2.1. After establishing the IKE tunnel between the UE and the ePDG, and authenticating the UE over SWm interface with the AAA server, the UE initiates IKE_AUH. The IKE_AUH includes cfg_params of the earlier assigned IPv4 or IPv6 addresses in 5GS and P-CSCF and DNS options.
3	The ePDG sends a Create Session request to the PGW-C. This request includes the following details: • IMSI • APN • Handover indication • RAT type • ePDG TEID of the control plane • ePDG address for the user plane • ePDG TEID of the user plane • EPS bearer identity • User location The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and includes it in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session request. This configuration allows the PGW-C to reallocate the same IP address or the prefix assigned to the UE. The IP address or prefix assignment occurs while the UE is connected to the 3GPP IP access. The policy modification procedure begins with the PCF.
4	The SMF does not perform the UDM registration as it has already been registered with UDM during the 5GS session establishment.
4a	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during the Wi-Fi session.
4b	The SMF detects the policy triggers with the information available in Step 3 against the requested policy control triggers that are received while communicating with PCF during the Wi-Fi session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters to the PCF.
6	The PCF sends the SM policy decision in the SM Policy Control Update response by including new or updated PCC rules.

Step	Description
7	Based on the information received in Step 6 and the existing policy data of 5GS session, the SMF prepares the “ModPolData” information.
8	If the SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request to the CHF with new rating-group for quota information. This request includes the PDU session information with the new access parameters.
9	The CHF sends the multi-unit information as Charging Update response to the SMF. The multi-unit information includes quota information for the rating-groups received in Step 8 and for the existing rating-group of 5GS session.
10	The SMF processes the ModChargingData in the Charging Update response that SMF receives from the CHF.
11	The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnels. This request includes details on creation of uplink FAR, creation of QER, creation of URR for the received new rating-group quota information, and update on URR for the modified quota information.
12	The UPF sends the N4 session modification response to the SMF with the UL tunnel information in the created PDR.
13	The SMF sends the GTPv2 Create Session response to the S-GW. The response includes details on accepted request or partially accepted request, PGW-C S2b F-TEID, PAA, APN-AMBR, creation of bearer context, charging gateway address, and APCO.
14	The SMF sends the GTPv2 Create Bearer request to the S-GW. This request includes information on bearer context list, which contains UL tunnel information for each dedicated bearer to end-user.
15	The S-GW sends the GTPv2 Create Bearer response to the SMF. The response includes details on accepted request or partially accepted request and bearer contexts.
16	The SMF processes the Create Bearer response and derives the DL tunnel information for the established bearer and the failed EBI list, if any. The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnel. This request is to create DL PDR and DL FAR with the DL tunnel information or list of charging description IDs for the detected charging triggers. The SMF deletes the gnb tunnel resources and the N4 resources of the Wi-Fi tunnel for the failed bearer context list.
17	The UPF sends the usage report in the N4 Session Modification response to the SMF.
18	The SMF initiates the NAMF communication N1 N2 message transfer, to the S-GW. This transfer message includes the PDU Session Resource Release Request N2 message.
19	The AMF sends N1 N2 Transfer Acknowledgement to the SMF.
20	The AMF sends the SM Context Update request to the SMF. This request includes the SM Resource Release Acknowledgement N2 message.
21	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
22	The AMF sends the SM Context Update request to the SMF. This request includes the PDU Session Release Complete N1 message.

Step	Description
23	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
24	If the SMF supports the June 2019 compliance version of 3GPP specification 23.502, the SMF indicates the release details to the AMF. The SMF achieves this functionality by sending the SM Context Status Notification message (statusInfo {Cause: PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED). The SMF sends this notification after a successful handover of 5GS to Non-3GPP Untrusted WiFi session. The SMF processes the message as per the compliance profile configured for the corresponding service. For information on the compliance profile configuration, see the Configuring Compliance Profile, on page 499 section. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
25	The AMF sends the 204 OK as SM Context Status Notify response to the SMF. **Important** If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.
26	The SMF sends the Charging Update request to the CHF. This request includes the PDU session information with the new access parameters and multi-usage report containing details on the old access parameters and the usage report that is received in Step 17.
27	The CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the existing rating-groups.
28	The SMF sends the SM Policy Control Update to PCF. This update includes the new access parameters and rule report for failed QFI list that are received from the AMF as part of Create Bearer response.
29	The PCF sends the SM policy decision through the SM Policy Control Update response to the SMF.
30	The SMF processes the SM policy decision and handles it as PCF-initiated modification procedure as defined in 3GPP TS 23.502, section 4.3.3.2.

Non 3GPP Untrusted LTE to WiFi Handover

This section describes the non-3GPP untrusted LTE to WiFi handover call flow.

Figure 113: Non-3GPP Untrusted LTE to WiFi Handover with TFTs more than 4 for a Dedicated Bearer

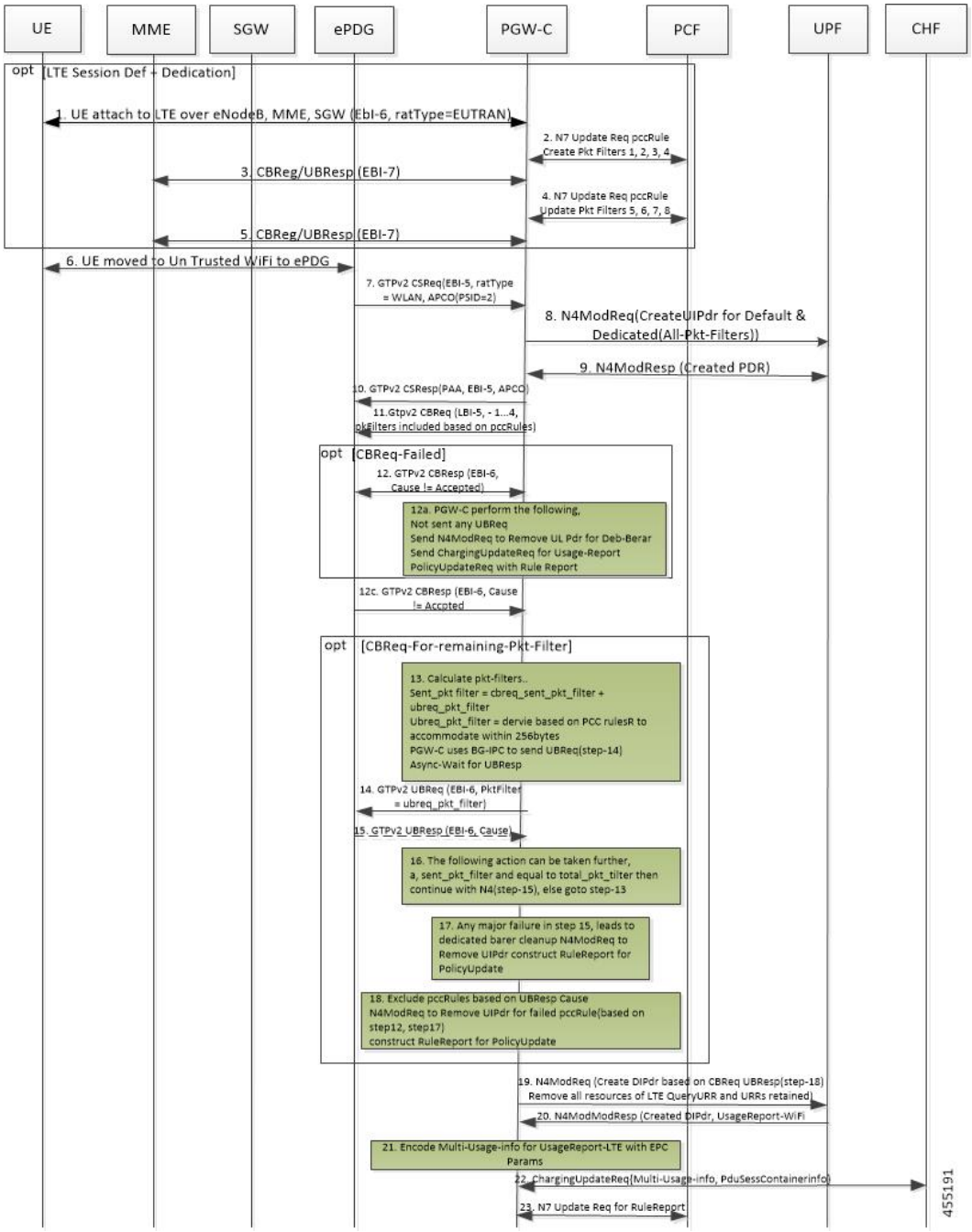


Table 176: Non-3GPP Untrusted LTE to WiFi Handover Call Flow Description

Step	Description
1	Session is established in LTE with a default bearer and dedicate bearer with 8 TFTs.
2	LTE to Wi-Fi Handover is triggered, when CSReq is received with hi flag configured from ePDG.

Step	Description
3	After successfully handling CSReq, CSResp is sent back to ePDG, indicating that the default bearer is successfully handed over.
4	For the dedicated bearer which has 8 TFT, since all TFTs cannot be sent in CBReq, the CBReq message is triggered with only 4 TFTs toward ePDG.
5	After successful CBResponse from ePDG, SMF sends the remaining TFTs in the UBReq message.
6	After successful UBResponse from ePDG, SMF continues with completion of establishing the bearer towards UPF.
7	In case of failure in CBResponse or failure in UBResponse at Step 5 or Step 6, the SMF deletes that bearer, and if armed, sends rule report to PCF with corresponding rules information as Inactive.

Important Steps 4-7 are applicable for LTE to Wi-Fi and NR to Wi-Fi if a dedicate bearer has more than 4 TFTs.

IE Support for GTPC

The SMF supports the following IEs in GTPC messages.

Table 177: Supported IEs in GTPC Messages

IE	Scenario
UE Local IP Address	If SMF receives UE Local IP Address from ePDG during Create Session Request, Create Bearer Response, Modify Bearer Request, or Delete Bearer Response procedure, then SMF sends the n3gaLocation attribute towards PCF and CHF if triggers are met.
UE UDP Port	If SMF receives UE UDP Port from ePDG during Create Session Request, Create Bearer Response, Modify Bearer Request, or Delete Bearer Response procedure, then SMF sends the n3gaLocation attribute towards PCF and CHF if triggers are met.

Example

The following example shows the n3GaLocation attribute in the output of the **show subscriber supi imsi-123456789012345 nf-service smf psid 5 full** command.

```
"n3GaLocation": {
"PortNumber": 4661,
"UeIpv4Addr": "209.165.200.227",
"ueLocationTimestamp": "2021-03-09T12:34:02Z"
}
```

Wi-Fi to 5G Handover with Alternate RAT Tunnel Creation Call Flow

This section describes the call flow of Wi-Fi to 5G handover with an alternate RAT tunnel creation.

Figure 114: Wi-Fi to 5G Handover with Alternate RAT Tunnel Creation Call Flow

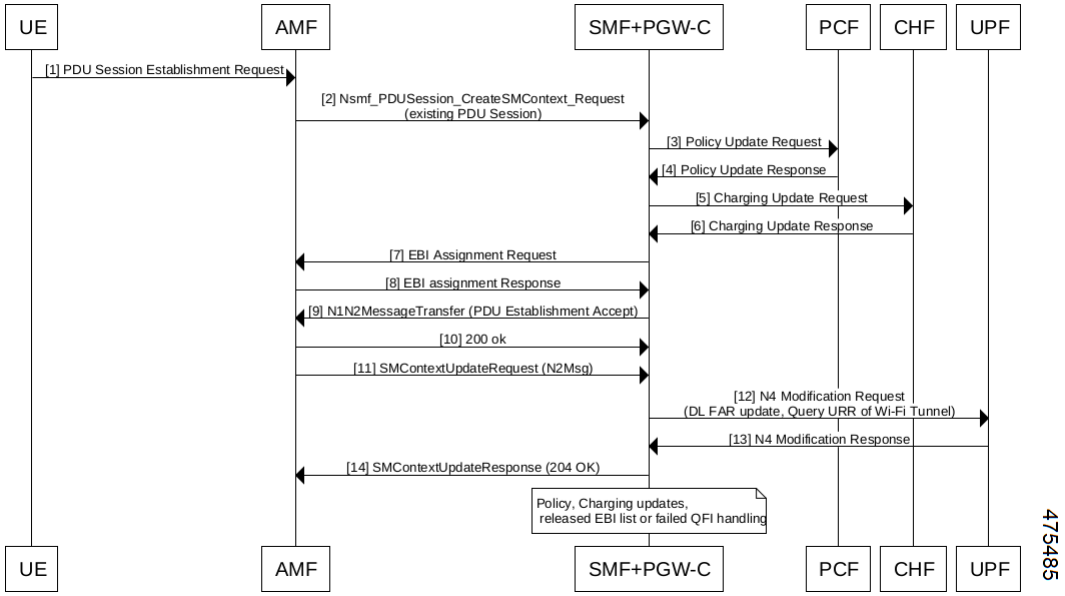


Table 178: Wi-Fi to 5G Handover with Alternate RAT Tunnel Creation Call Flow Description

Step	Description
1	UE sends the PDU Session Establishment Request to AMF.
2	AMF Nsmf PDU Session Create SMContext Request to SMF+PGW-C. This request is for the existing PDU session. The SMF+PGW-C sends the 200 OK message.
3	SMF+PGW-C sends the Policy Update Request to PCF.
4	PCF sends the Policy Update Response to SMF+PGW-C.
5	SMF+PGW-C sends the Charging Update Request to CHF.
6	CHF sends the Charging Update Response to SMF+PGW-C.
7	SMF+PGW-C sends the EBI assignment request to AMF.
8	AMF sends the EBI assignment Response to SMF+PGW-C.
9	SMF+PGW-C sends the N1N2Message Transfer (PDU Establishment Accept) message to AMF.
10	AMF sends the 200 OK response to SMF+PGW-C.
11	AMF sends the SMContext Update Request (N2 message) to SMF+PGW-C.

Step	Description
12	SMF+PGW-C sends the N4 Modification Request to UPF. This request includes details on DL FAR update and Query URR of the Wi-Fi tunnel.
13	UPF sends the N4 Modification Response to SMF+PGW-C.
14	SMF+PGW-C sends the SMContext Update Response, which is 204 OK to AMF. SMF+PGW-C SMF+PGW-C includes details on policy, charging updates, and the released EBI list or failed QFI handling information.

5G to Wi-Fi Handover with Alternate RAT Tunnel Creation Call Flow

This section describes the call flow of the 5G to Wi-Fi handover with an alternate RAT tunnel creation.

Figure 115: 5G to Wi-Fi Handover with Alternate RAT Tunnel Creation Call Flow

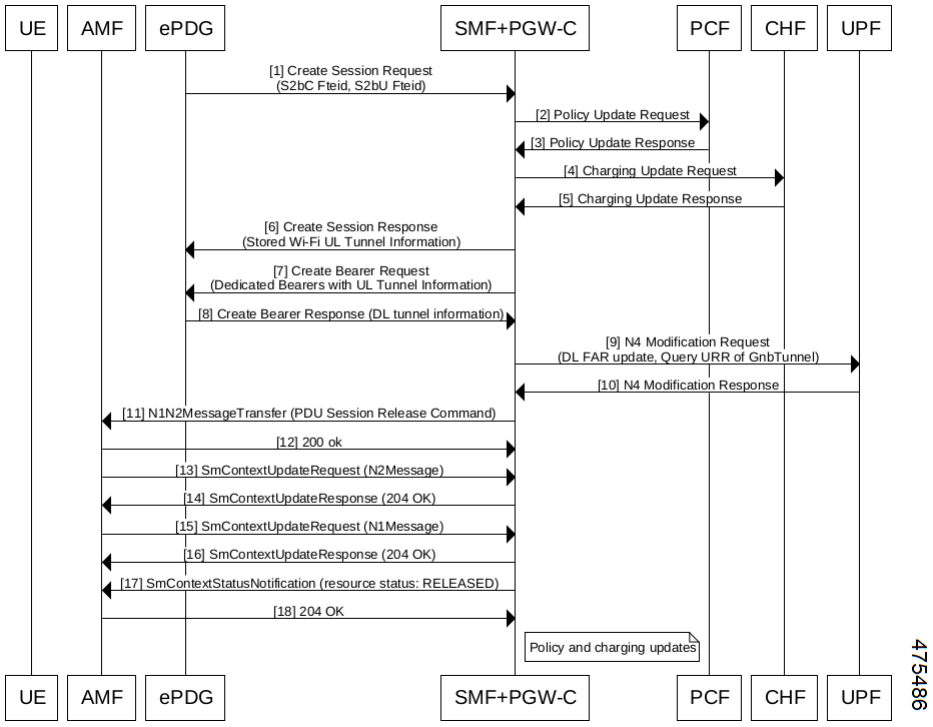


Table 179: 5G to Wi-Fi Handover with Alternate RAT Tunnel Creation Call Flow Description

Step	Description
1	ePDG sends the Create Session Request to SMF+PGW-C. This request includes details on S2bC F-TEID and S2bU F-TEID.
2	SMF+PGW-C sends the Policy Update Request to PCF.
3	PCF sends the Policy Update Response to SMF+PGW-C.
4	SMF+PGW-C sends the Charging Update Request to CHF.

Step	Description
5	CHF sends the Charging Update Response to SMF+PGW-C.
6	SMF+PGW-C sends the Create Session Response to ePDG. This response includes details on the stored Wi-Fi UL tunnel.
7	SMF+PGW-C sends the Create Bearer Request to ePDG. This request includes details on the dedicated bearers with UL tunnel.
8	ePDG sends the Create Bearer Response (DL tunnel information) to SMF+PGW-C.
9	SMF+PGW-C sends the N4 Modification Request to UPF. This request includes information on the DL FAR update and Query URR of gNB tunnel.
10	UPF sends the N4 Modification Response to SMF+PGW-C.
11	SMF+PGW-C sends the N1N2Message Transfer, which is the PDU Session Release Command to AMF.
12	AMF sends the 200 OK response to SMF+PGW-C.
13	AMF sends the SMContext Update Request (N2Message) to SMF+PGW-C.
14	SMF+PGW-C sends the SMContext Update Response (204 OK) to AMF.
15	AMF sends the SMContext Update Request (N1Message) to SMF+PGW-C.
16	SMF+PGW-C sends the SMContext Update Response (204 OK) to AMF.
17	SMF+PGW-C sends the SMContext Status Notification to AMF. This notification indicates the resource status as RELEASED.
18	AMF sends the 204 OK response to SMF+PGW-C. Then, on SMF+PGW-C, the policy and charging updates happen.

Configuring Wi-Fi Handovers

This section describes the configurations related to the Wi-Fi Handovers feature.

Configuring Compliance Profile

The SMF provides the compliance profile support for the 3GPP specification 23.502 through the CLI configuration. This compliance profile is in use during the 5GS to non-3GPP untrusted Wi-Fi handover procedure.

Use the following configuration to configure the SMF in compliance with the 3GPP specification.

```
config
   profile compliance profile_name
      service threegpp23502 version   spec  {  15.4.0 | 15.6.0 } spec_version
full version_format
      uri_version uri_version
         range
```

```
!
!
```

Important For more information on how to configure compliance profile, contact your Cisco Account representative.

NOTES:

- **full**: Specifies the full version in the format — <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]
- **spec**: Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.4.0
  - 15.6.0

  To support 3GPP December 2018 specification compliance, configure the specification version as 15.4.0. The default version is 15.4.0.

  To support 3GPP June 2019 specification compliance, configure the specification version as 15.6.0.
- **uri**: Specifies the URI version in the format — "v" concatenated with a number. The version can be both v1 and v2, or either v1 or v2.

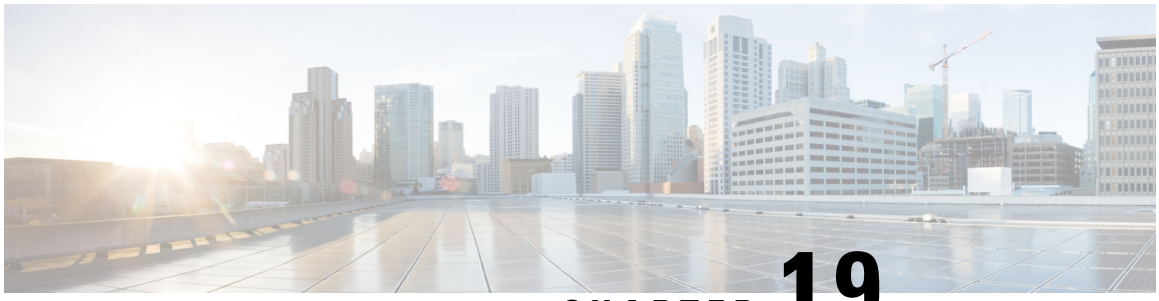
Configuring Calls with Handover Indication

Use the following sample configuration to handle calls coming with handover (HO) indication and no existing session.

```
config
  profile access access_profile_name
    gtpc message-handling create-session-request ho-ind new-call-reject
    exit
```

NOTES:

- **ho-ind**: Indicates that Create Session Request is received with handover.
- **new-call-reject**: If the session does not exist, SMF rejects Create Session Request received with HO indicator.



CHAPTER 19

IMS PDU Sessions for Voice

- Feature Summary and Revision History, on page 501
- Feature Description, on page 502
- Voice Over LTE Support, on page 502
- NPLI Support for VoLTE and VoNR, on page 513
- VoWi-Fi Support, on page 515
- Voice over New Radio, on page 521

Feature Summary and Revision History

Summary Data

Table 180: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 181: Revision History

Revision Details	Release
Added support for VoLTE and Emergency Call Prioritization	2021.02.03
Introduced NPLI support for VoLTE and VoNR	2021.02.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

This chapter provides an overview of the IMS procedures handeled by SMF.

Voice Over LTE Support

Feature Description

Important The PGW-C term used in this chapter denotes the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The SMF supports Voice over Long-Term Evolution or LTE (VoLTE). The VoLTE technology utilizes IP Multimedia Subsystem (IMS) to allow you to make cellular calls over the LTE access network.

SMF supports prioritization of emergency and VoLTE calls during ICSR switchover and recovery. The SMF tracks IMS sessions with active voice calls and communicates with UPF. Then, UPF prioritizes the Emergency and VoLTE calls during ICSR switchover and recovery. SMF supports only the Wireless Priority Services (WPS) call prioritization where the MP flag is configured in N4 and the GTP headers are based on the WPS configuration.

How it Works

A 5G mobile device with LTE access requests voice services to communicate with PGW-C over S-GW and MME resulting in the establishment of a PDU session. The PGW-C supports a non-GBR bearer with QCI flows as 5 for VoLTE sessions. This support allows IMS signaling along with P-CSCF, DNS IPv4, or DNS IPv6 addresses for end users. For mobile-originated (MO) or mobile-terminated (MT) calls, the Application Function (AF) provides policy authorization details to the PCF. The PCF then converts these details to GBR flows and PCC rules and sends them to PGW-C. The PGW-C then converts the GBR-flows to dedicated bearers by establishing the dedicated bearer creation procedure with UE (User Equipment). The PGW-C provisions the GBR with the QCI flow as 1 to UPF. By this provisioning, the UPF supports voice communication between the calling and called devices over IMS network elements.

As per the E-UTRAN Attach procedure, the MME triggers the GTPv2 Create Session Request to PGW-C over S-GW. This request includes the EPS Bearer Identity (EBI) value, ePCO options for P-CSCF and DNS IPv4 or DNS IPv6 containers, PDN-Type, and PAA options for IPv4 or IPv6 allocated address for end users. The PGW-C then processes the received Create Session Request and communicates with various SBI interfaces to receive the following information:

- Subscription data from UDM by including PGW-C FQDN in the subscription request.
- Policy information from PCF by sending SM policy create request. Policy information includes details, such as PCC rules and Session-AMBR.

- Online and offline charging information from CHF by sending the charging create data request.

After communication with SBI interfaces, which are based on the local SMF profile configuration, the PGW-C sends the GTPv2 Create Session Response to the end user over S-GW and MME. This response includes:

- PAA with IPv4 or IPv6 addresses that PGW-C IPAM module allocates
- ePCO option with P-CSCF
- DNS IPv4 or DNS IPv6 address based on DNN-Profile configuration
- Non-GRB with the QCI flow as 5 for IMS signaling

For an MO or MT call, if the PCF is provisioned for GBR with the QCI flow as 1 for end users, the PGW-C converts these GBR flows to the dedicated bearer creation. The GBR flows include the flow information and the PCC rules in the SM Policy Update Notify Request. The dedicated bearer is created by sending GTPv2 Create Bearer Request to UE over S-GW or MME. Another S5-U tunnel is created between S-GW and PGW-C to allow GBE flow packets for the voice communication between the calling and called devices.

For prioritization of emergency and VoLTE calls during ICSR switchover and recovery, SMF includes the MP flag value in N4 and GTP messages. The flag values are listed in the following table.

Table 182: MP Flag Values

Call Type	MP Flag Value
Emergency	1
IMS-Active	2
IMS-Inactive	3
WPS	1

Note

- If **message-priority gtpc** is configured in WPS profile, then SMF sends the MP flag value as 1 for the WPS sessions. Earlier SMF used to send MP value as 0 in N4 and GTP header for WPS sessions.
- If a call matches multiple call types, then SMF sends better priority, which is the lowest value. If the call matches with WPS and the **message-priority** is not configured, then message priority is not sent.
- SMF marks session as IMS-inactive when dedicated bearer or modify procedure starts for establishment of QCI configured as IMS in DNN profile and the session is not marked as IMS-active.
- SMF updates the session as IMS-active session after the IMS QCI bearer or flow is established.
- SMF updates the session as IMS-inactive session after last IMS QCI bearer or flow is deleted.
- SMF marks session as WPS session when dedicated bearer or modify procedure starts for an ARP that is configured in WPS profile.
- SMF updates the session as WPS session after WPS bearer or flow is established.
- SMF updates the session as IMS-active or IMS-inactive if an IMS QCI bearer exists when the last WPS bearer was deleted.
- SMF updates the session as IMS-inactive, if an IMS flow is removed during handover, path-switch, or any other procedure.
- Clear subscriber non-VoLTE CLI implementation is modified to use the QCI that is configured as IMS. If QCI is not configured, the earlier behavior of detecting non-VoLTE session is used. This behaviour implies that the session does not having bearer or flows with QCI as 1 or 2.

Call Flows

This section describes the following call flows:

- VoLTE PDU Session Creation Call Flow
- VoLTE Mobile-Originated (MO) Call Creation Call Flow
- VoLTE Mobile-Terminated (MT) Call Creation Call Flow

VoLTE PDU Session Creation Call Flow

To enable the connectivity through a 5G core, the initial attach on the E-UTRAN or EPS deviates from the defined 3GPP procedures in the following ways:

- An SMF+PGW-C replaces the PGW-C in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN Session Establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.

Note Depending on the mapped PCC rules, the SMF+PGW-C can initiate the dedicated bearer creation.

The following call flow depicts the creation of a VoLTE PDU session.

Figure 116: VoLTE PDU Session Creation Call Flow

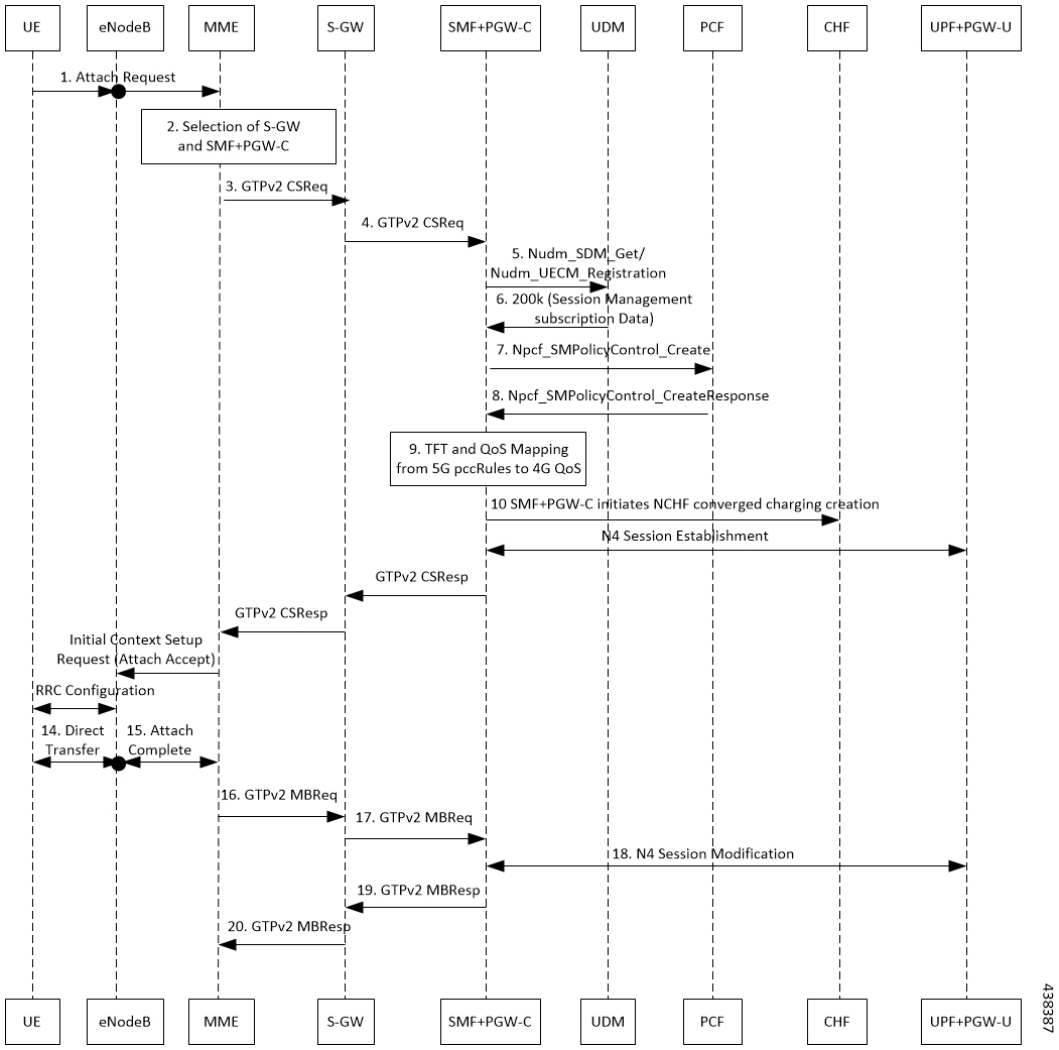


Table 183: VoLTE PDU Session Creation Call Flow Description

Step	Description
1	UE sends the attach request to MME through eNodeB.
2	MME determines if the UE is active and subscribed for the handoff to NR. Then, MME selects a SMF+PGW-C node as the PGW-C for the PDU session.
3	MME sends the create session request to the selected S-GW and includes the selected SMF+PGW-C address in the request.

Step	Description
4	S-GW initiates the create session request toward SMF+PGW-C by including the “P-CSCF IPv4 or IPv6 request” container identifier in the extended PCO IE options. SMF+PGW-C extracts and saves the PDU session ID that UE sends in the PCO option. Then, SMF+PGW-C performs a UDM registration and sends both the N11 and S5 or S8 interface ID to UDM. Based on the local configuration or the session management subscription data, which is received from UDM for respective DNN, SMF+PGW-C determines to support “IMS Voice over PS”.
5	SMF+PGW-C sends the NPCF SM policy control creation request to PCF to initiate the SM policy association establishment procedure. In this procedure, PGW-C+SMF includes the information elements that are received in the create session request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information: • SUPI contains the IMSI. • DNN contains the APN. • PEI contains the IMEI-SV. • Session AMBR contains the APN-AMBR. • Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.
6	PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. Then, SMF+PGW-C associates them with the corresponding default and dedicated bearers.
7	Based on the charging policies received from the PCF, the SMF+PGW-C initiates the NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.
8	The SMF+PGW-C starts the UPF+PGW-U selection and N4 session establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
9	The SMF+PGW-C sends create session response to the S-GW. This response includes the bearer information and the TEID for the default bearer. The SMF+PGW-C also includes the 5G QoS parameters in PCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime), and 001FH (QoS flow descriptions) to the UE.
10	Based on the charging policies received from PCF, the SMF+PGW-C initiates NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from PCF.
11	S-GW sends create session response to MME.
12	MME sends the Initial Context Setup Request to eNodeB with the N1 Attach Accept message.
13	eNodeB and UE perform the RRC configuration.
14	UE sends the direct transfer message to eNodeB.

Step	Description
15	eNodeB sends the attach completion message in the Initial Context Setup Response and the TEID of eNodeB to MME.
16	MME sends a modify bearer request to S-GW with eNodeB TEID.
17	S-GW sends the modify bearer request to SMF+PGW-C with eNodeB TEID.
18	SMF+PGW-C performs the N4 session modification to update the eNodeB TEID on the data path to the UPF+PGW-U.
19	SMF+PGW-C sends the modify bearer response to the S-GW.
20	S-GW sends the modify bearer response to MME.

VoLTE Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoLTE MO call creation call flow.

Figure 117: VoLTE MO Call Creation Call Flow

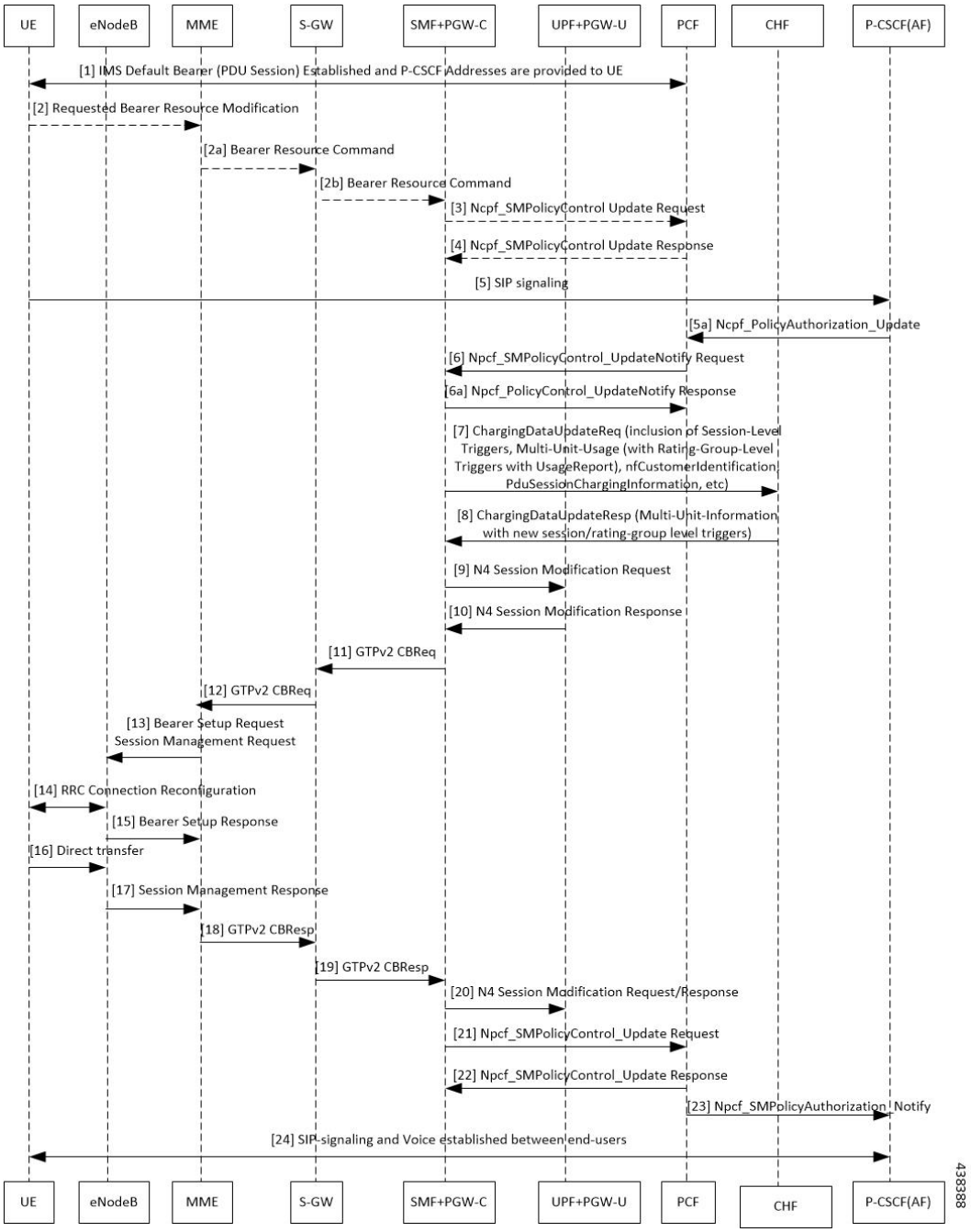


Table 184: VoLTE MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	UE sends the requested bearer resource modification information to MME.

Step	Description
2a	MME sends the bearer resource command to S-GW.
2b	S-GW sends the bearer resource command to SMF+PGW-C.
3	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
4	PCF sends the NPCF SM Policy control update response back to SMF+PGW-C.
5	UE initiates SIP signaling toward P-CSCF (AF).
5a	P-CSCF sends NPCF Policy Authorization Update message to PCF through CHF.
6	PCF sends the NPCF SM policy control update notify request to SMF+PGW-C.
6a	SMF+PGW-C sends the NPCF SM Policy control update notify response back to PCF.
7	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
8	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
9	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
10	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
11	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
12	S-GW sends the GTPv2 create bearer request to MME.
13	MME sends the bearer setup request and session management request to eNodeB.
14	RRC connection reconfiguration starts between UE and eNodeB.
15	The eNodeB sends the bearer setup response to MME.
16	UE initiates a direct transfer toward eNodeB.
17	eNodeB sends the session management response to MME.
18	MME sends the GTPv2 create bearer response to S-GW.
19	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
20	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
21	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
22	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
23	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
24	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

Note

- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
- The NCHF Converged Charging Update service procedures replace all the Gy and Gz interface messages.
- The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
- SMF+PGW-C saves the EBI for the dedicated bearer that is received in the create bearer response.

VoLTE Mobile-Terminated (MT) Call Creation Call Flow

This section describes the VoLTE MT call creation call flow.

Figure 118: VoLTE MT Call Creation Call Flow

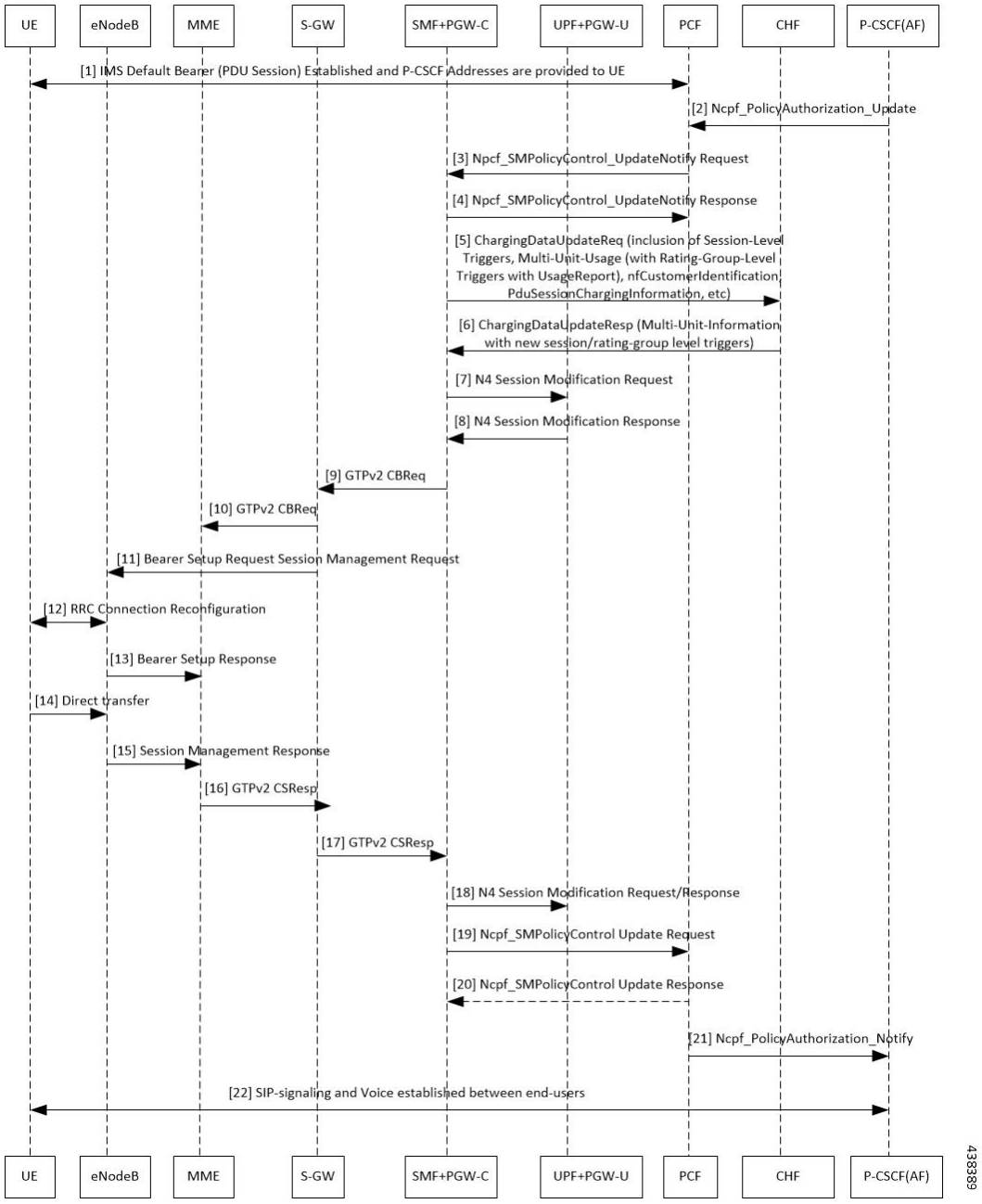


Table 185: VoLTE MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	P-CSCF (AF) sends the NPCF policy authorization update to PCF.
3	PCF sends the NPCF SM Policy control update notify request to SMF+PGW-C.

Step	Description
4	SMF+PGW-C sends the NPCF SM Policy control update notify response to PCF.
5	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
6	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
7	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
8	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
9	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
10	S-GW sends the GTPv2 create bearer request to MME.
11	MME sends the bearer setup request and session management request to eNodeB.
12	RRC connection reconfiguration starts between UE and eNodeB.
13	eNodeB sends the bearer setup response to MME.
14	UE initiates a direct transfer toward eNodeB.
15	eNodeB sends the session management response to MME.
16	MME sends the GTPv2 create bearer response to S-GW.
17	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
18	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
19	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
20	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
21	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
22	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

VoLTE and Emergency Call Prioritization Configuration

To configure VoLTE and emergency call prioritization, use the following configuration:

```
config
  profile dnn dnn_profile_name ims mark qci qci_value
  end
```

NOTES:

- **mark**: Specify the value for marking standard QCI value as IMS media.

- **qci** *qci_value*: Specify the standard QoS Class Identifier. The identifier value must be in range of 1 to 9. By default, SMF considers QCI value as 1,2 as IMS. Configuration with these values overrides the default behavior.

Configuration Example

The following is an example configuration:

```
config
  profile dnn dnn1 ims mark qci [1 2]
  end
```

Configuration Verification

To verify the configuration for IMS sessions, use the following show running-config command.

```
show running-config profile dnn dnn1 ims mark qci
```

Standards Compliance

The VoLTE support feature complies with the following standards:

- *3GPP TS 23.502 version 15.2.0 (2018-09)—5G; Procedures for the 5G System*

Limitations

The VoLTE support feature does not support UE-initiated dedicated bearer creation.

NPLI Support for VoLTE and VoNR

Feature Description

SMF provides NetLoc User location information, Access Type, UE time zone towards PCF for VoNR and VoLTE support with this 2021.02.0 release.

In roaming scenarios, the hSMF provides the preceding functionality and supports associated call flows.

SMF informs support of Access Network Information Reporting to PCF by sending the NetLoc bit to PCF in SmPolicyContextData.

If PCF learns that NetLoc feature is supported, it performs the PCC rule provisioning and also provides the requested access network information indication (e.g. user location and/or user timezone information) to the SMF as follows:

1. PCF includes the "lastReqRuleData" attribute to contain the "reqData" attribute with one or more values MS_TIME_ZONE and/or USER_LOC_INFO and the "refPccRuleIds" attribute to contain one or more related installed/modified/removed PCC rule identifiers.
2. Provides the AN_INFO policy control request rigger within the "policyCtrlReqTriggers" attribute (if not yet set)
3. For those PCC Rules based on preliminary service information as described in 3GPP TS 29.514 [17] or in 3GPP TS 29.214 [18], the PCF may assign the 5QI and ARP of the default QoS flow to avoid signalling

to the UE. These PCC Rules are not included in the "packetFilterUsage" attribute set to true within the "flowInfos" attribute.

If PCF sets the AN_INFO policy control request trigger to receive the "lastReqRuleData" attribute with the "reqData" attribute with one or more values MS_TIME_ZONE and/or USER_LOC_INFO and the "refPccRuleIds" attribute containing one or more PCC rule identifiers corresponding to one or more PCC rules which are installed, modified, or removed together.

- If the user location information is requested by the PCF and provided to the SMF, then the SMF provides the user location information within the "userLocationInfo" attribute and the time when it was last known within "userLocationInfoTime" attribute (if available).
- If the user location information was requested by the PCF and if it’s not provided to the SMF, the SMF provides the serving PLMN identifier within the "servingNetwork" attribute.
- If the time zone is requested by the PCF, the SMF provides "ueTimeZone" attribute. In addition, the SMF also provides the AN_INFO policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.
- If SMF does not have time zone information and PCF only requests MS TIME ZONE in reqData and AN INFO is the sole trigger activated in policyCtrlReqTriggers, then the SMF does not start the PCF update.

The SMF doesn’t report any subsequent access network information updates received from the RAN without any further provisioning or removal of related PCC rules. SMF requests the access network information unless the associated QoS flow or PDU session is released.

Architecture

Call Flows

This section describes the following call flows:

- VoLTE PDU Session Creation Call Flow
- VoLTE Mobile-Originated (MO) Call Creation Call Flow
- VoLTE Mobile-Terminated (MT) Call Creation Call Flow

Standards Compliance

VoNR/VoLTE NPLI Support feature complies with the following standards:

- 3GPP TS 29.518
- 3GPP TS 29.512
- 3GPP TS 29.502
- 3GPP TS 23.502

VoWi-Fi Support

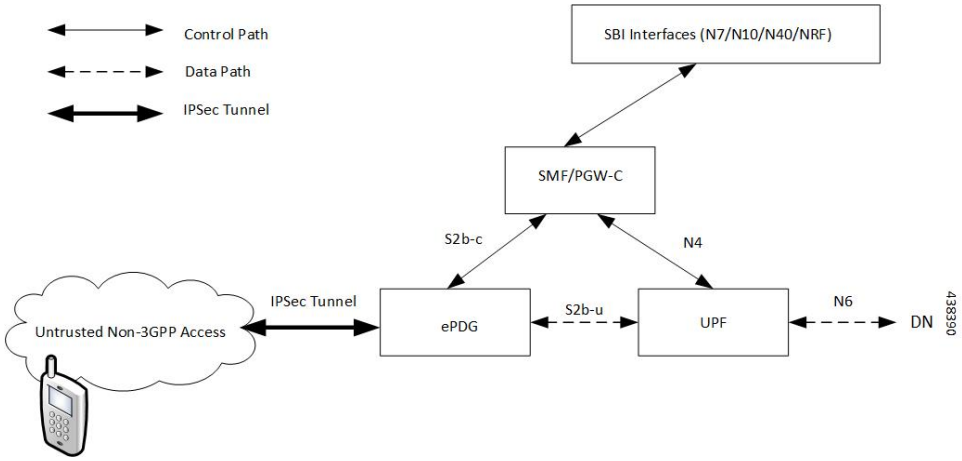
Feature Description

The SMF supports Voice over Wi-Fi (VoWi-Fi). The VoWi-Fi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

Architecture

This section describes the VoWi-Fi architecture.

Figure 119: VoWi-Fi Architecture



How it Works

A 5G mobile device connects through an untrusted Wi-Fi network for voice services to establish a PDN connection with PGW-C. This connection is established through Internet Key Exchange Protocol version 2 (IKEv2) protocol between the UE and enhanced Packet Data Gateway (ePDG). The PGW-C receives the GTPv2 Create Session Request from an untrusted Wi-Fi ePDG over the S2b interface. The PGW-C then communicates with the SBI interfaces for creating the default and dedicated bearers. The SBI interfaces can be an N7, N10, N40, or an NRF interface.

Call Flows

This section describes the following call flows:

- VoWi-Fi PDU Session Creation Call Flow
- VoWi-Fi Mobile-Originated (MO) Call Creation Call Flow
- VoWi-Fi Mobile-Terminated (MT) Call Creation Call Flow

VoWi-Fi PDU Session Creation Call Flow

To enable connectivity through a 5G core, the initial attach on the ePDG or EPS deviates from the defined 3GPP procedures in the following ways:

- An SMF+PGW-C replaces the PGW-C in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN session establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.

The following call flow depicts the creation of a VoWi-Fi PDU session.

Figure 120: VoWi-Fi PDU Session Creation Call Flow

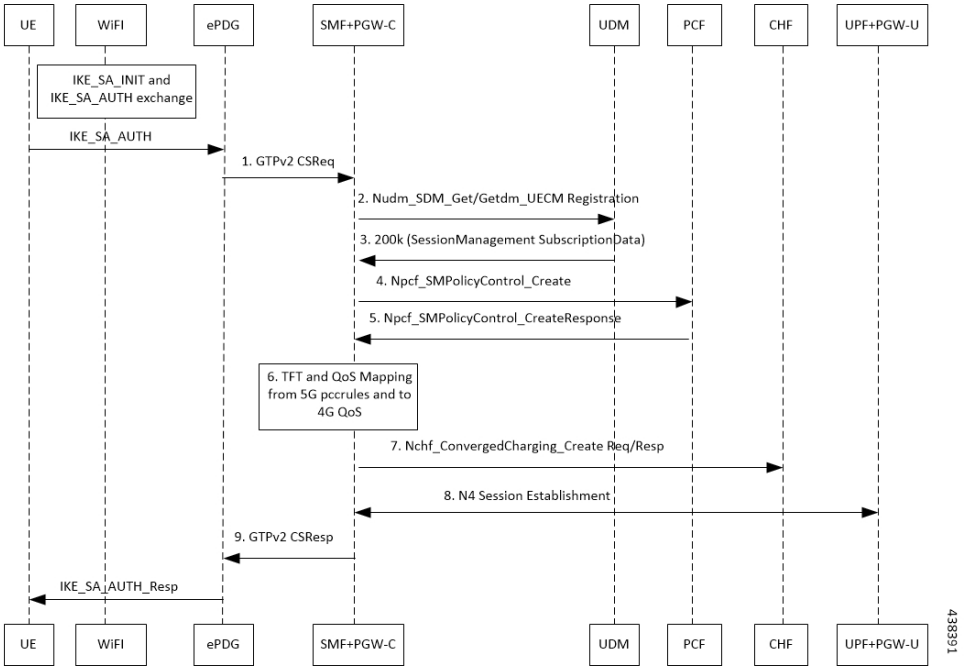


Table 186: VoWi-Fi PDU Session Creation Call Flow Description

Step	Description
1	The UE initiates the IKE_SA_INIT and IKE_SA_AUTH exchange. The UE then sends the IKE_SA_AUTH exchange message to ePDG to create the IPSec tunnel.
2	The UE sends the IKE_SA_AUTH exchange message to the SMF+PGW-C as a GTP Create Session Request by including the “P-CSCF IPv4 or IPv6 request and DNS IPv4 or IPv6” container identifier in APCO IE Options.

Step	Description
3	The SMF+PGW-C extracts and saves the PDU Session ID that the UE sent in the APCO IE option. The SMF+PGW-C then performs a UDM registration and sends both the N11 and S2b interface IDs to UDM. Based on the local configuration or session management subscription data that is received from UDM for respective DNN, SMF+PGW-C determines to support “IMS Voice over PS”.
4	The SMF+PGW-C sends the NPCF SM Policy Control Creation Request to the PCF to initiate the SM Policy Association Establishment procedure. In this procedure, the PGW-C+SMF includes the information elements that are received in the Create Session Request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information: • SUPI contains the IMSI. • DNN contains the APN. • PEI contains the IMEI-SV. • Session AMBR contains the APN-AMBR. • Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.
5	The PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. The SMF+PGW-C then associates them with the corresponding default and dedicated bearers.
6	Based on the charging policies received from the PCF, the SMF+PGW-C initiates Nchf_ConvergedCharging_Create procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.
7	The SMF+PGW-C starts the UPF+PGW-U selection and N4 Session Establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
8	Th eSMF+PGW-C sends Create Session Response to the ePDG. This response includes the bearer information and the TEID for the default bearer.
9	The ePDG sends IKE_SA_AUTH Response to the UE. Then, depending on the mapped PCC rules, the SMF+PGW-C initiates the dedicated bearer creation.

VoWi-Fi Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoWi-Fi MO call creation call flow.

Figure 121: VoWi-Fi MO Call Creation Call Flow

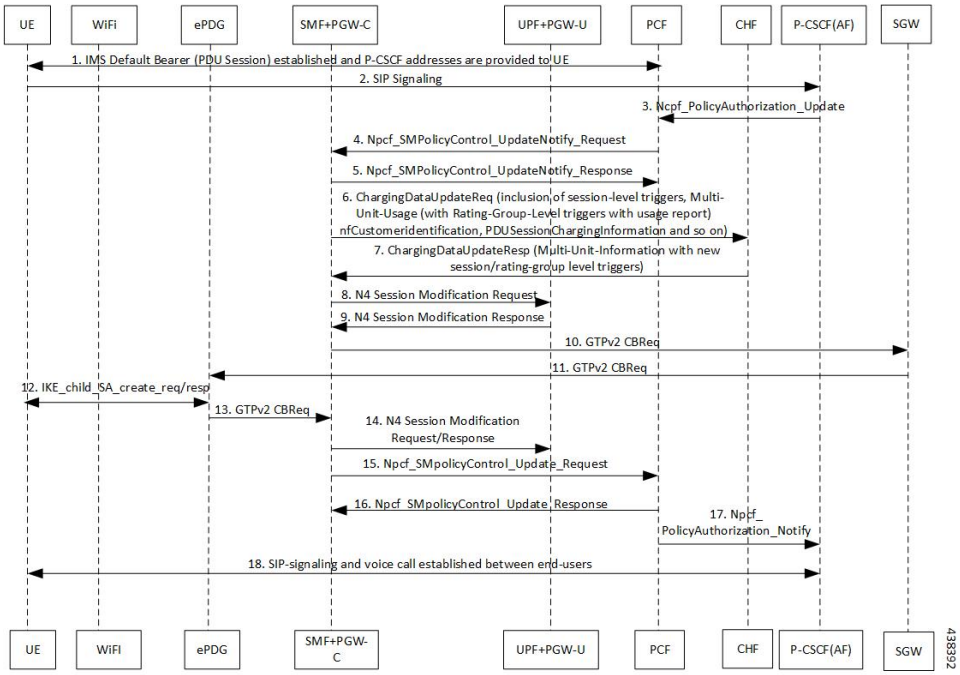


Table 187: VoWi-Fi MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE initiates the SIP signaling toward P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of SM Policy Control UpdateNotify Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER information which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.

Step	Description
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

Note

- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
- The NCHF Converged Charging Update Service procedures replace all the Gy and Gz interface messages.
- The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
- The SMF+PGW-C saves the EBI for the dedicated bearer that is received in the Create Bearer Response.

VoWi-Fi Mobile-Terminated (MT) Call Creation Call Flow

This section describes the Mobile-Terminated (MT) call flow.

Figure 122: VoWi-Fi MT Call Creation Call Flow

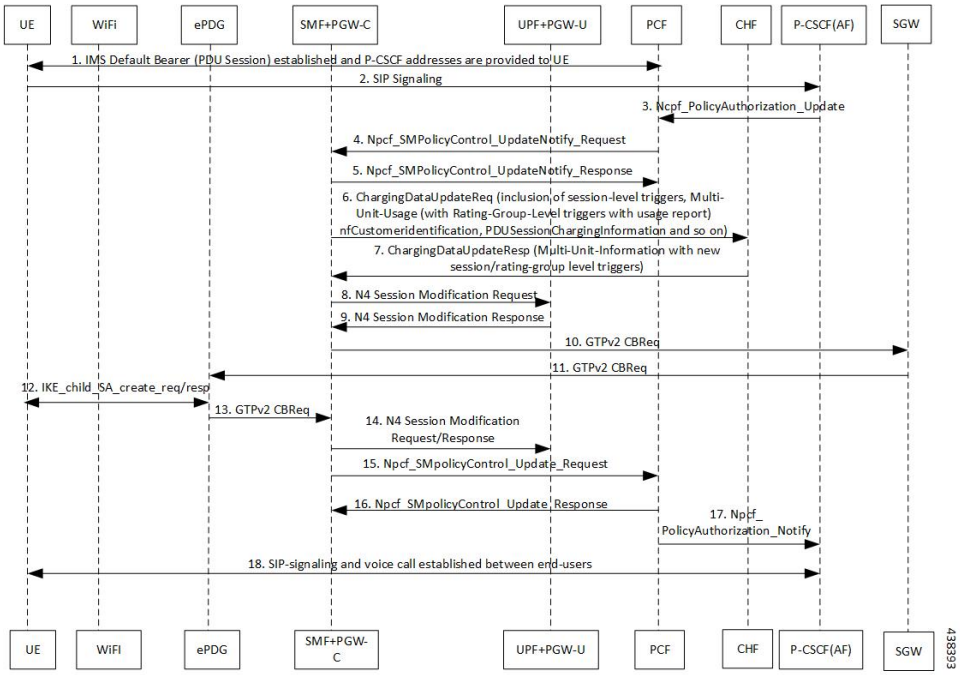


Table 188: VoWi-Fi MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE-initiates the SIP signaling towards the P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of SM Policy Control UpdateNotify Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.

Step	Description
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

Standards Compliance

The VoWi-Fi support feature complies with the following standard:

- 3GPP TS 23.502 V15.2.0 (2018-09)

Limitations

The VoWi-Fi support feature has the following limitation:

- UE-initiated Dedicated Bearer Creation is not supported.

Voice over New Radio

Feature Description

New Radio (NR) is the 5G radio access technology, and Voice over NR (VoNR) is the voice or video over the 5G network. VoNR is the target voice or video communication solution for 5G networks.

Voice services in 5GS over NG-RAN continue to be based on IP Multimedia Subsystem (IMS), such as Voice over LTE (VoLTE). VoNR is supported only when 5GS is connected to the IMS core.

Resolution of P-CSCF Server Address

The SMF uses either the **DNS proxy** or the **local configuration** defined in P-CSCF profile to resolve the address of P-CSCF server. SMF uses one of the options to resolve the domain name, receive the IP address from the remote DNS servers, and send the IP address to the subscribers.

Note Local configuration is applicable to both 4G and 5G.

Standards Compliance

The VoNR feature complies with the following standards:

- *3GPP TS 23.228, Release 15.3.0*
- *3GPP TS 23.501, Release 15.4.0*
- *3GPP TS 23.502, Release 15.4.0*

Address Resolution Using DNS Proxy

Feature Description

The Domain Name System (DNS) is a network of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice-versa. The DNS proxy allows you to configure one or more proxy servers for resolving the host names to their IP address. The DNS proxy resides within the SMF.

When you query for the host name, the SMF sends the DNS queries to the configured DNS server through the DNS proxy server to fetch a maximum of two P-CSCF IP addresses. The resolved IP addresses are then sent back to the DNS client. This operation helps in resolving the Fully Qualified Domain Name (FQDN) of the P-CSCF. The SMF allows configuration of FQDN within the P-CSCF profile.

Configuring the DNS Proxy for Address Resolution

This section describes how to configure the DNS Proxy for P-CSCF address resolution.

Configuring the DNS Proxy involves the following steps:

1. Configuring the P-CSCF FQDN, on page 522
2. Configuring DNS Proxy Replica
3. Configuring DNS Proxy

Configuring the P-CSCF FQDN

The SMF allows configuration of domain name under P-CSCF profile. The DNS is used to resolve the domain name, fetch the IP address from the remote DNS servers, and provide the IP address to the subscribers.

To define the FQDN of the P-CSCF, use the following sample configuration:

```
config
   profile pcscf pcscf_profile_name
      fqdn domain_name
      end
```

NOTES:

- **pcscf-profile** *pcscf_profile_name*: Specify the P-CSCF profile name, and enters into the P-CSCF Profile Configuration mode. *pcscf_profile_name* must be an alphanumeric string.
- **fqdn** *domain_name*: Specify the FQDN of the P-CSCF server. *domain_name* must be an alphanumeric string.

Verifying the Feature Configuration

Use the following show command to verify the P-CSCF FQDN feature configuration.

show running-config

The following is an example of the output of this show command:

```
profile pcscf pcscf1
 fqdn cisco.com
exit
```

Configuring DNS Proxy Replica

Use the following sample configuration to configure the DNS proxy replica.

```
config
   instance instance-id gr_instance_id
      endpoint dns-proxy replicas replica_value
      commit
```

NOTES:

- **endpoint dns-proxy replicas** *replica_value*: Specify the number of replicas of the DNS proxy pod per node.

  replica_value must be an integer.

- **commit**: Saves the configuration.

Configuring DNS Proxy

Use the following sample configuration to configure the DNS Proxy feature for SMF.

```
config
   profile dns-proxy
      cache-ttl dns_response_ttl_value
      query-type { ipv4v6 | ipv4 | ipv6 }
      servers dns_server_name
         ip server_ip_address
         port server_port
         priority server_priority
         protocol { tcp | udp }
      timeout dns_timeout_value
      commit
```

NOTES:

- **profile dns-proxy**: Enter the DNS Proxy Configuration mode.
- **cache-ttl** *dns_response_ttl_value*: Specify the TTL value of DNS responses in cache, in seconds. *dns_response_ttl_value* must be an integer in the range of 60-86400.
- **query-type**: Specify the DNS query type.
- **servers** *dns_server_name*: Specify the name of the DNS server. For example, serv1.
  - **ip** *server_ip_address*: Specify the IP address of the DNS server.
  - **port** *server_port*: Specify the port of the DNS server.

    server_port must be an integer in the range of 1-65535.
  - **priority** *server_priority*: Specify the priority of the DNS server.

server_priority must be an integer in the range of 1-100.

- **protocol**: Specify the protocol type for the DNS server as TCP or UDP.

- **timeout** *dns_timeout_value*: Specify the DNS timeout value, in milliseconds. *dns_timeout_value* must be an integer in the range of 200-10000.

  dns_timeout_value must be an integer.

- **commit**: Saves the configuration.

Verifying DNS Proxy Configuration

This section describes how to verify the DNS Proxy feature configuration.

Use the **show running-config profile dns-proxy** command to confirm the configuration of DNS Proxy feature.

The following is an example output of **show running-config profile dns-proxy** command with configuration for two DNS servers, serv1 and serv2.

```
query-type ipv4
timeout 205
servers serv1
round-robin-answers
randomise-answers

servers serv1
 ip 209.165.200.240
 port 53
 protocol tcp
 priority 1
exit
servers serv2
 ip 209.165.200.241
 port 20
 protocol udp
 priority 2
exit
```

Randomization of P-CSCF Addresses from DNS

The SMF service supports random selection of resolved hosts. If a DNS resolution yielded a set of IP addresses for a host and if the **randomize-answers** CLI is enabled in the DNS Proxy profile configuration, the DNS lookup selects IP addresses randomly. The selection of addresses is based on pseudo-random permutation of integers that ensure randomization.

Every DNS query for a particular host gives different sets of IP addresses when the **randomize-answers** CLI is enabled. This is applicable for both IPv4 and IPv6 addresses.

The selection method is either round-robin or randomized for the DNS Proxy profile.

Example:

For a DNS lookup to get a subset of five IP addresses with **randomize-answers** enabled.

Host1 = *{ "209.165.200.226", "209.165.201.2", "209.165.201.3", "209.165.201.4", "209.165.201.5", "209.165.201.6", "209.165.201.7", "209.165.201.8", "209.165.201.9", "209.165.201.10" }*

First lookup: *[209.165.201.5 209.165.200.226 209.165.201.9 209.165.201.2 209.165.201.7]*

Second lookup: *[209.165.201.8 209.165.201.6 209.165.201.2 209.165.201.3 209.165.201.9]*

Third lookup: *[209.165.201.7 209.165.201.5 209.165.201.2 209.165.201.4 209.165.201.9]*

Configuring DNS for Random Selection of P-CSCF Addresses

The SMF supports selection of resolved hosts either in randomized or round-robin manner.

To configure the DNS for selection of P-CSCF address, use the following sample configuration:

```
config
   profile dns-proxy
      randomize-answers
      round-robin-answers
      end
```

NOTES:

- **randomize-answers**: Enable DNS for fetching addresses by the randomized selection method.
- **round-robin-answers**: Enable DNS for fetching addresses by the round-robin selection method.

DNS Test Query

Feature Description

SMF supports DNS Test client to query and check the P-CSCF IP address using the Fully Qualified Domain Name (FQDN). The DNS Test client can be used as a debug utility for VoNR launch. The SMF supports DNS test query execution from the SMF Ops Center CLI. The DNS Test client interacts with the DNS server through DNS proxy to retrieve the test query results. The DNS client then displays the fetched results to the user.

The Test DNS client manages the following error scenarios and provides the appropriate IPv4 or IPv6 responses to the user.

- Query timeouts
- DNS proxy failures/errors
- Invalid response handling

How it Works

The DNS proxy sends DNS request to DNS servers. The DNS proxy server receives the response from DNS server and sends it to DNS Test client running from OAM pod. The CLI shows the response.

The timeout values are used while interacting with DNS proxy. The basic validation of data is performed in the DNS client before sending to the SMF Ops Center CLI.

The DNS response contains primary and secondary IPv4 or IPv6 address for any given FQDN. The DNS client handles the response data accordingly.

Important DNS client does not support sending DNS query with no cache (direct hit DNS server). The support is not available with DNS proxy.

Configuring DNS Test Query

DNS Test client queries and checks the P-CSCF IP address using the FQDN.

To configure the DNS test query, use the following command:

test dns-query [fqdn *fqdn_name* **| num-ipv4** *ipv4_address_num* **| num-ipv4v6** *ipv4v6_address_num* **| num-ipv6** *ipv6_address_num* **]**

NOTES:

- **test dns-query**: Perform test FQDN resolution.
- **fqdn** *fqdn_name*: Specify the FQDN of the node for which DNS query has to be sent.

  fqdn_name must be an alphanumeric string from 1 through 255 characters.
- **num-ipv4** *ipv4_address_num*: Specify the number of IPv4 addresses to be used for DNS query.

  ipv4_address_num must be an integer in the range of 1-9.
- **num-ipv4v6** *ipv4v6_address_num*: Specify the number of IPv4v6 addresses to be used for DNS query.

  ipv4v6_address_num must be an integer in the range of 1-9.
- **num-ipv6** *ipv6_address_num*: Specify the number of IPv6 addresses to be used for DNS query.

  ipv6_address_num must be an integer in the range of 1-9.

Configuration Verification

This section describes how to verify the DNS test query configuration.

Use the **show dns query** command to verify the DNS Test Query configuration.

The following is an example output of the **show dns query** command.

```
smf# show dns-query fqdn smf.com
dns-summary
Hostname : smf.com,
IPv4Addr : [209.165.200.228,
209.165.200.229,
209.165.200.230],
IPv6Addr : [::1,
::3,
::2]

smf# show dns-query fqdn smf.comnum-ipv4 1

dns-summary
Hostname : smf.com,
IPv4Addr : [209.165.200.228],
IPv6Addr : []

[smf] smf# show dns-query fqdn hello.comnum-ipv4v6 4
dns-summary
Hostname : hello.com,
IPv4Addr : [209.165.200.235,
209.165.200.236,
209.165.200.237,
209.165.200.238],
IPv6Addr : [2001:DB8::1,
2001:DB8::2,
```

```
2001:DB8::3,
2001:DB8::4]
```

Address Resolution Using Local Configuration

If the UE requests P-CSCF discovery, then the SMF fetches the P-CSCF addresses from the DNN configuration, which are locally provisioned under DNN with IMS-Support and list of P-CSCF addresses or P-CSCF FQDN.

Currently, only up to 64 address lists can be configured for both P-CSCF IPv4 and IPv6 addresses.

P-CSCF Address Selection Mechanism

The local configuration consists of P-CSCF address sets that contain primary, secondary, and tertiary P-CSCF server IP addresses. You can configure multiple such IPv4, IPv6, or mixed IP address sets. Each address set has a precedence value.

SMF supports only round-robin method for selecting P-CSCF addresses. You can define the number of addresses to be selected based on normal or emergency calls.

When choosing the address from the local configuration, SMF picks the P-CSCF server addresses according to the precedence value from the address set and sends them to the UE.

If the defined number of P-CSCF server addresses are not configured in the selected address set or some are marked as down, the SMF then selects as many addresses as are configured and working in that set. SMF does not select the remaining number of addresses from the subsequent set.

If the addresses in the selected set are not configured or marked as down, only then SMF moves to the address set with next address set.

How SMF Performs P-CSCF Address Selection

The serving PLMN AMF sends an indication toward the UE during the registration procedure to indicate whether an IMS voice over PS session is supported in the 3GPP access network. A UE with "IMS voice over PS" voice capability over 3GPP access takes this indication into account when performing voice domain selection.

The UE includes extended Protocol Configuration Options (ePCO) IE in PDU Session Establishment Request by setting P-CSCF container options in the AMF. Further, the AMF forwards these ePCO IE options in SM Context Create Request toward the SMF. The SMF fetches the P-CSCF addresses based on the DNN profile, which maintains IMS-related data. The SMF includes P-CSCF IPv4 and IPv6 addresses in N1N2 Message Transfer toward the AMF as per the PDN types and requested P-CSCF container values.

Important The SMF does not include the P-CSCF address if the UE does not set the P-CSCF container options in the ePCO IE.

P-CSCF Address Selection During Normal Calls

During normal calls, SMF fetches P-CSCF addresses from the IMS DNN. SMF by default sends 3 P-CSCF addresses from the local configuration to the UE.

Configure the P-CSCF Servers for Address Resolution

Configuring the P-CSCF server involves the following steps:

Step 1 Create the P-CSCF Profile

Step 2 Define the P-CSCF Servers Parameters

Step 3 Define the P-CSCF Profile in DNN Profile Configuration, on page 529

Create the P-CSCF Profile

This task helps you create a P-CSCF profile for configuring the P-CSCF servers.

Create a P-CSCF profile instance using **profile pcscf** *pcscf_profile_name* command.

Example:

```
[smf] smf# config
[smf] (config)# profile pcscf pcscf1
[smf] (config-pcscf-pcscf1)#
```

What to do next

After creating the P-CSCF profile, you need to perform following tasks:

- Define the P-CSCF Server Parameters such as FQDN, server selection method, count of addresses, and a set of IPv4 or/and IPv6 P-CSCF addresses.
- Associating the P-CSCF profile with a DNN profile.

Define the P-CSCF Servers Parameters

This task helps you define the parameters for configuring the P-CSCF server:

Before you begin

Create a P-CSCF profile instance.

Step 1 Specify the P-CSCF server's Fully Qualified Domain Name (FQDN) using the **fqdn** *domain_name* command.

Example:

```
[smf] (config-pcscf-pcscf1)# fqdn cisco.com
```

If the FQDN is configured, SMF selects the P-CSCF addresses from the DNS proxy. If the FQDN is not configured or the DNS proxy is inaccessible, SMF selects the P-CSCF server addresses from the local configuration.

Step 2 Configure the P-CSCF server selection method using the **pcscf-selection round-robin** command.

Example:

```
[smf] (config-pcscf-pcscf1)# pcscf-selection round-robin
```

Step 3 Configure IPv4, IPv6, or IPv4v6 address lists under the configured P-CSCF profile using the **v4-list | v6-list | v4v6-list** commands.

Example:

```
[smf] (config-pcscf-pcscf1)# v4-list | v6-list | v4v6-list
```

Step 4 Configure the precedence for selecting the IP address list using the **precedence** *precedence_value* command. Also specify the primary, secondary, and tertiary P-CSCF IP addresses using the **{ primary** *server_ipv4_address* | *server_ipv6_address* **| secondary** *server_ipv4_address* | *server_ipv6_address* **| tertiary** *server_ipv4_address* | *server_ipv6_address* **}** commands.

Example:

```
[smf] (config-pcscf-pcscf1)# v6-list
                             precedence 1
                             primary fd00:976a:c004:1938::5
                             secondary fd00:976a:b699:4901::5
                             tertiary fd00:976a:b699:4901::7
```

- The value of **precedence** *precedence_value* must be an integer between 1-64.
- **{ primary** *server_ipv4_address* | *server_ipv6_address* **| secondary** *server_ipv4_address* | *server_ipv6_address* | **tertiary** *server_ipv4_address* | *server_ipv6_address* **}** allows configuring primary, secondary, and tertiary IPv4/IPv6 addresses.

Step 5 Exit the current configuration mode and return to the previous configuration mode using the **exit** command.

Example:

```
[smf] smf# config
[smf] (config)# profile pcscf pcscf1
[smf] (config-pcscf-pcscf1)# fqdn cisco.com
[smf] (config-pcscf-pcscf1)# server-cnt-ue 2
[smf] (config-pcscf-pcscf1)# pcscf-selection round-robin
[smf] (config-pcscf-pcscf1)# v6-list
                             precedence 1
                              primary fd00:976a:c004:1938::5
                              secondary fd00:976a:b699:4901::5
                              tertiary fd00:976a:b699:4901::7
[smf] (config-pcscf-pcscf1)# exit
```

What to do next

After configuring the P-CSCF server parameters, associate the P-CSCF profile with the DNN profile.

Define the P-CSCF Profile in DNN Profile Configuration

This task allows you to associate the P-CSCF profile with the DNN profile.

Before you begin

Before associating the P-CSCF profile with the DNN profile, you must:

- Configure the P-CSCF profile.
- Define the P-CSCF server parameters.

Step 1 Configure a DNN profile instance in the Global Configuration mode using the command **profile dnn** *dnn_profile_name*.

Example:

```
[smf] smf#config
[smf] (config)#profile dnn dnntst1
[smf] (config-dnn-dnntst1)#
```

Step 2 Define the P-CSCF profile under the configured DNN profile using the command **pcscf-profile** *pcscf_profile_name*.

Example:

```
[smf] (config-dnn-dnntst1)#pcscf-profile pcscf1
```

Step 3 Exit the DNN configuration mode and return to the Global Configuration mode using the **exit** command.

Example:

```
[smf] (config-dnn-dnntst1)#exit
```

VoNR MO and MT Call Support

Feature Description

The SMF supports Mobile Originated (MO) and Mobile Terminated (MT) VoNR with 5G QoS Identifier (5QI) as Guaranteed Bit Rate (GBR) flow for UE after the IMS PDU Session Creation. The SMF further supports VoNR calls for the following mobility (inter gNB, inter AMF) scenarios:

- MO and MT calls for idle mode UE
- MO and MT calls when the UE is handing over

During the mobility scenario of VoNR MO and MT calls, make sure to consider the following point:

- VoNR GBR flows are supported during UE and network service request procedures, Xn and N2 based handover.

Call Flows

This section describes the call flows associated with this feature.

VoNR MO Call Handling Procedure

This section describes the VoNR MO call handling procedure.

Figure 123: VoNR MO Call Handling Flow

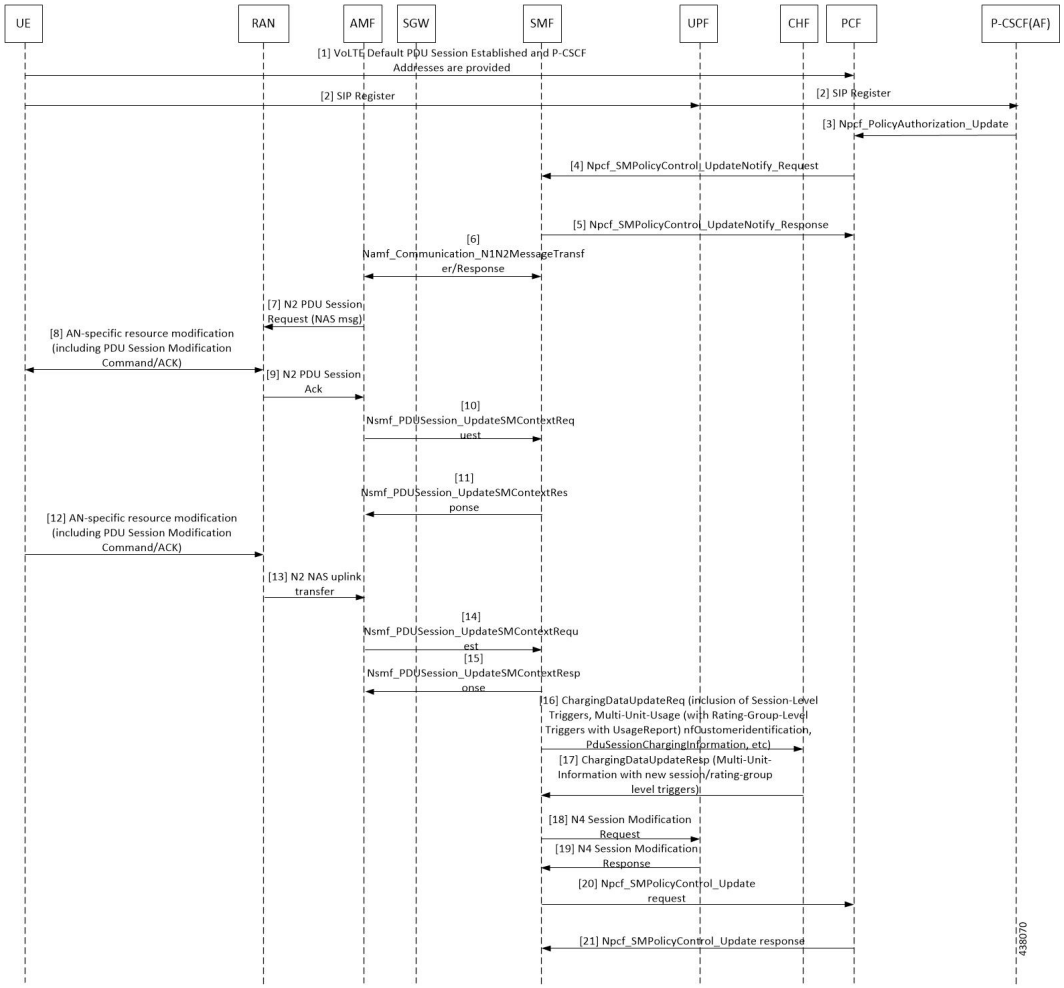


Table 189: VoNR MO Call Handling Flow Description

Step	Description
1	The SMF performs the PDU session establishment procedure as defined in 3GPP TS 23.502.
2	The UE initiates SIP Registration towards the called-party via UPF, P-CSCF through the backed IMS core network.
3	P-CSCF sends “Npcf_PolicyAuthorization_Update” to PCF to enforce policies, modify service information, gate control, modify subscription to SDF notification/deactivation, updating of traffic routing information, and so on (as defined in *3GPP TS 29.514*). This service allows the NF consumer to subscribe and unsubscribe the notification of events (for example, change of Access Type, RAT type, or changes of the PLMN identifier).
4	The PCF sends Npcf_SMPolicyControl_UpdateNotify request to update and/or delete the PCC rule(s) PDU session-related policy context at the SMF and Policy Control Request Trigger information. This enforces PCC rules, policy control request triggers, SDF, and charging related information.

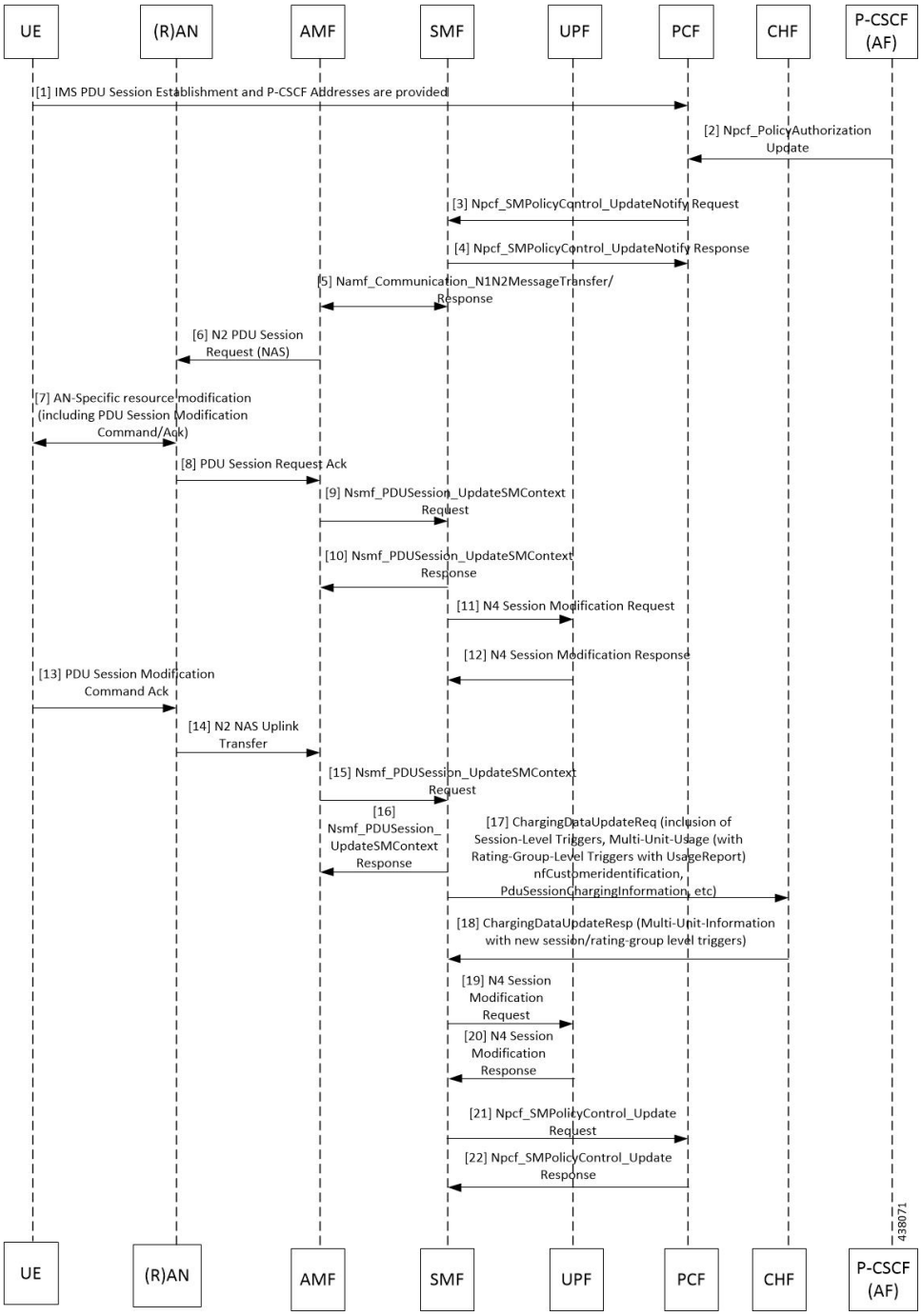
Step	Description
5	The SMF processes the received PCC rules and sends 200 OK message for a successful scenario. When the processing of any content fails, the SMF includes "400 Bad Request" in “Npcf_SMPolicyControl_UpdateNotify request” and sends it along with appropriate cause value as defined in *3GPP TS 29.512*.
6	The SMF sends Namf_Communication_\nN1N2MessageTransfer/Response (PDU Session ID, QFIs, QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the QoS rule(s), QoS rule operation, and QoS Flow level QoS parameters operation, Session-AMBR))). If the UE is in CM-IDLE state or Mobility handover (HO) state, see the procedure in VoNR MO Call Flow for UE in Idle Mode, on page 534.
7	The AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN.
8	The (R)AN issues AN specific signalling exchange with the UE that is related with the information received from SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
9	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session ACK (N2 SM information (List of accepted/rejected QFIs, AN Tunnel Info, PDU Session ID, Secondary RAT usage data), User Location Information) message to the AMF. In case of Dual Connectivity, if one or more QFIs were added to the PDU session, the primary RAN node assigns one or more of these QFIs to an NG-RAN node which was not involved in the PDU session earlier. In this case, the AN Tunnel Info includes a new N3 tunnel endpoint for QFIs assigned to the new NG-RAN node. Correspondingly, if one or more QFIs were removed from the PDU session, a (R)AN node may no longer be involved in the PDU session anymore, and the corresponding tunnel endpoint is removed from the AN Tunnel Info. The NG-RAN rejects QFIs if it cannot fulfill the User Plane Security Enforcement information for a corresponding QoS Profile, for example, due to the UE Integrity Protection Maximum Data Rate being exceeded.
10	The AMF forwards the N2 SM information and the User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. If the (R)AN rejects QFIs, the SMF updates the QoS rules and QoS parameters if needed for the QoS flow(s) associated with the QoS rule(s) in the UE accordingly.
11	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response. N2 SM information includes Secondary RAT Usage Data.
12	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command ACK)) message.
13	The (R)AN forwards the NAS message to the AMF.
14	The AMF forwards the N1 SM container (PDU Session Modification Command ACK) and User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation.

Step	Description
15	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response. If the SMF-initiated modification is to delete QoS Flows (for example, triggered by PCF) which do not include QoS Flow associated with the default QoS rule and the SMF does not receive response from the UE, the SMF marks that the status of those QoS Flows is to be synchronized with the UE.
16	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
17	CHF provides ChargingDataUpdtaeResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides parameter changes for Session-Level and Rating-Group values.
18	The SMF updates N4 session of the UPF(s) that are involved in the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the PCF. For a PDU Session of Ethernet PDU Session Type, the SMF notifies the PCF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s). The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU Session with UL flow classifier (CL) changes, only the UL CL is involved.
19	The PCF sends an N4 session modification response message containing any information that the PCF has to provide to the SMF in response to the control information received.
20	For PCF-initiated policy modification case, the SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in *3GPP TS 23.502, section 4.16.5.1*. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.
21	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.

VoNR MT Call Handling Procedure

This section describes the VoNR MT call handling procedure.

Figure 124: VoNR MT Call Handling Flow

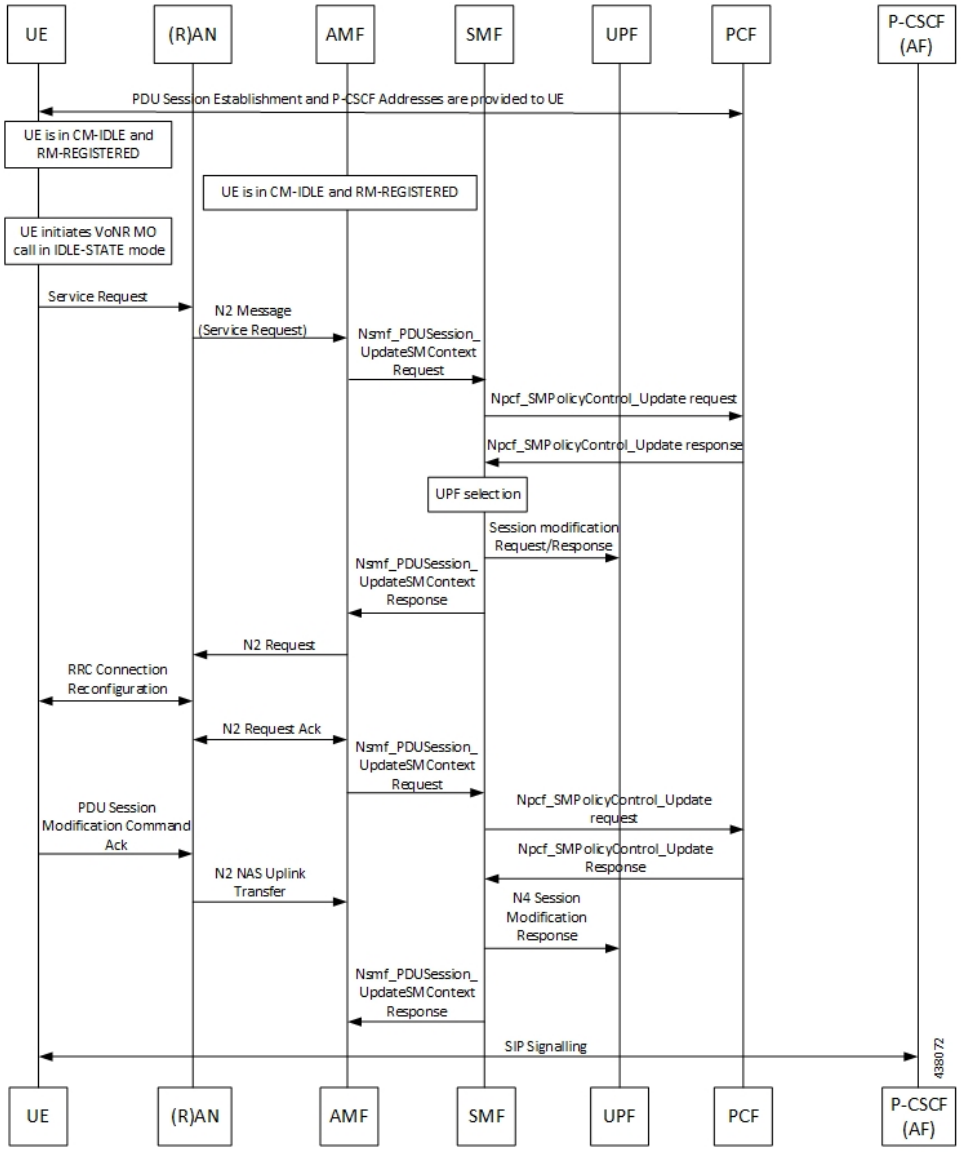


The VoNR MT call handling procedure remains the same as the VoNR MO call handling procedure except for the SIP Registration Request initiated from UE to P-CSCF(AF) through the UPF.

VoNR MO Call Flow for UE in Idle Mode

This section describes the VoNR MO call handling procedure when the UE is in idle mode.

Figure 125: VoNR MO Call Handling Flow for UE in Idle Mode



Step	Description
1	The SMF performs the PDU session establishment procedure as defined in 3GPP TS 23.502 and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with Paging Policy Differentiation (PPD) for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
2	The UE maintains its state in CM-IDLE and RM-REGISTERED.
3	The UPF maintains the UE in CM-IDLE and RM-REGISTERED state.
4	The UE initiates the VoNR call in CM-IDLE state.
5	The UE performs Service-Request procedures as defined in *3GPP TS 23.502*.

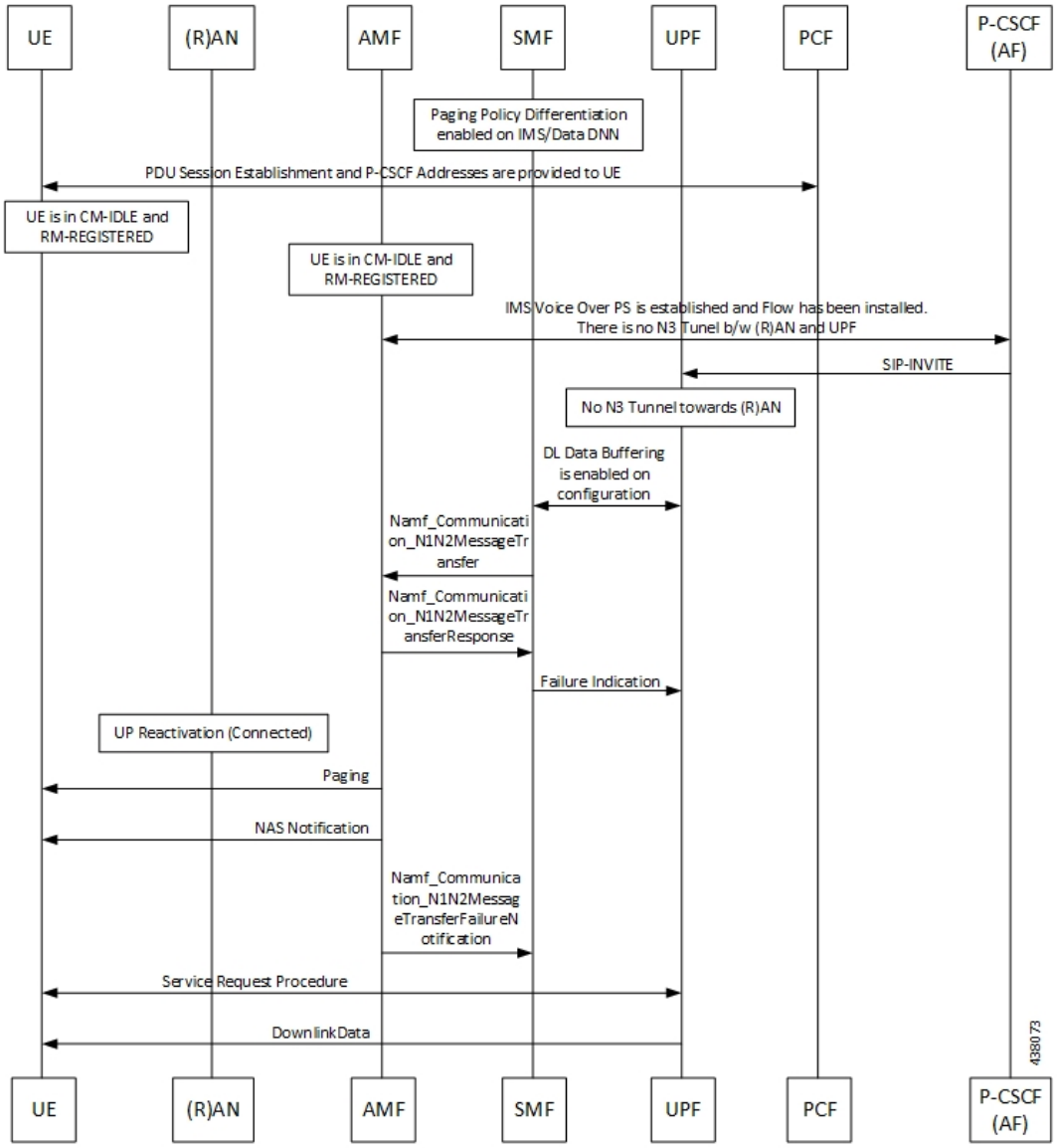
Step	Description
6	The RAN sends N2 message (service request) to the AMF.
7	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID(s), Operation Type, UE Location information, Access Type, RAT Type, UE presence in LADN service area, Indication of Access Type can be changed) to the SMF.
8	If the AMF notifies the SMF that the access type of the PDU session can be changed, and if the PCC is deployed, the SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in *3GPP TS 23.502*, Section 4.16.5.1.
9	The PCF provides the updated PCC Rule(s) to the SMF.
10	The SMF initiates an N4 Session Modification request to the UPF. The SMF provides (R)AN Tunnel Info and the corresponding forwarding rules to the UPF. The UPF provides an N4 Session Modification Response to the SMF.
11	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (N2 SM information (PDU Session ID, QFI(s), QoS profile(s), CN N3 Tunnel Info, S-NSSAI, User Plane Security Enforcement, UE Integrity Protection Maximum Data Rate), N1 SM Container, Cause) to the AMF. The SMF sends N1 SM Container and/or N2 SM Information to the AMF when applicable.
12	The AMF sends N2 Request (N2 SM information received from SMF, security context, Mobility Restriction List, Subscribed UE-AMBR, MM NAS Service Accept, list of recommended cells, TAs, NG-RAN node identifiers, UE Radio Capability, Core Network Assistance Information, Tracing Requirements) to the (R)AN.
13	The NG-RAN performs RRC Connection Reconfiguration with the UE depending on the QoS Information for all the QoS Flows of the PDU sessions whose UP connections are activated, and Data Radio Bearers.
14	The (R)AN sends N2 Request Acknowledgement message (N2 SM information (AN Tunnel Info, List of accepted QoS Flows for the PDU Sessions whose UP connections are activated, List of rejected QoS Flows for the PDU Sessions whose UP connections are activated), PDU Session ID) to the AMF. The N2 Request ACK message includes N2 SM information, for example, AN Tunnel Info. NG-RAN responds N2 SM information with separate N2 message (for example, N2 tunnel setup response) if the AMF sends separate N2 message.
15	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, RAT Type, Access Type) per PDU Session to the SMF. The AMF determines Access Type and RAT Type based on the Global RAN Node ID associated with the N2 interface. If the AMF received N2 SM information (one or multiple), then the AMF forwards the N2 SM information to the relevant SMF per PDU Session ID. If the UE Time Zone has changed compared to the last reported UE Time Zone, then the AMF includes the UE Time Zone IE in this message.
16	The SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in *3GPP TS 23.502*, Section 4.16.5.1. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.

Step	Description
17	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.
18	The SMF updates N4 session of the UPF(s) that are involved in the PDU session modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF. For a PDU session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s). The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU session with UL CL changes, only the UL CL is involved. The UPF sends an N4 session modification response message containing any information that the UPF has to provide to the SMF in response to the control information received.
19	The SMF sends a Nsmf_PDUSession_UpdateSMContext Response. The N2 SM information includes Secondary RAT Usage Data.

VoNR MT Call Flow for UE in Idle Mode

This section describes the VoNR MT call handling procedure when the UE is in idle mode.

Figure 126: VoNR MT Call Flow for UE in Idle Mode



The VoNR MT call flow remains the same as the VoNR MO call flow for service request when the UE is in CM-IDLE state except the following:

- The SIP-INVITE received by P-CSCF
- The PCC rule enforcements triggered from PCF towards SMF.

Note The PCC rules, QoS, PDR, and traffic detection rule enforcements remain the same as the VoNR MT Call Handling procedure as defined in VoNR MT Call Handling Procedure, on page 533 VoNR MT Call Handling Procedure.

When the AMF receives Namf_Communication_N1N2MessageTransfer Request (N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the QoS rule(s), QoS rule operation, and QoS Flow level parameters operation, Session-AMBR))) when the UE is in CM-IDLE state. If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer.

The AMF performs paging operations to the UE, and the UE triggers service request procedure. Once the paging is established, the AMF decides QoS Flows, QoS rules, and Session-AMBR that need to be accepted, which are received in Namf_Communication_N1N2MessageTransfer Request and the AMF performs Nsmf_PDUSession_UpdateSMContext operation with SMF to notify on accepting the QoS Flows, QoS rules, session-AMBR, and so on.

VoNR Paging Policy Differentiation

Feature Description

The SMF supports Paging Policy Differentiation feature by providing a configuration at PLMN, DNN, and 5QI level for data and IMS DNN sessions of the UE. The SMF provides Paging Policy Indicator based on UPF data. The SMF also supports QoS flow (PPI, ARP, and 5QI) towards the AMF over N11 interface.

Call Flows

This section describes the call flows associated with this feature.

VoNR Paging Policy Differentiation Procedure

This section describes the VoNR Paging Policy Differentiation procedure.

Figure 127: VoNR Paging Policy Differentiation Call Flow

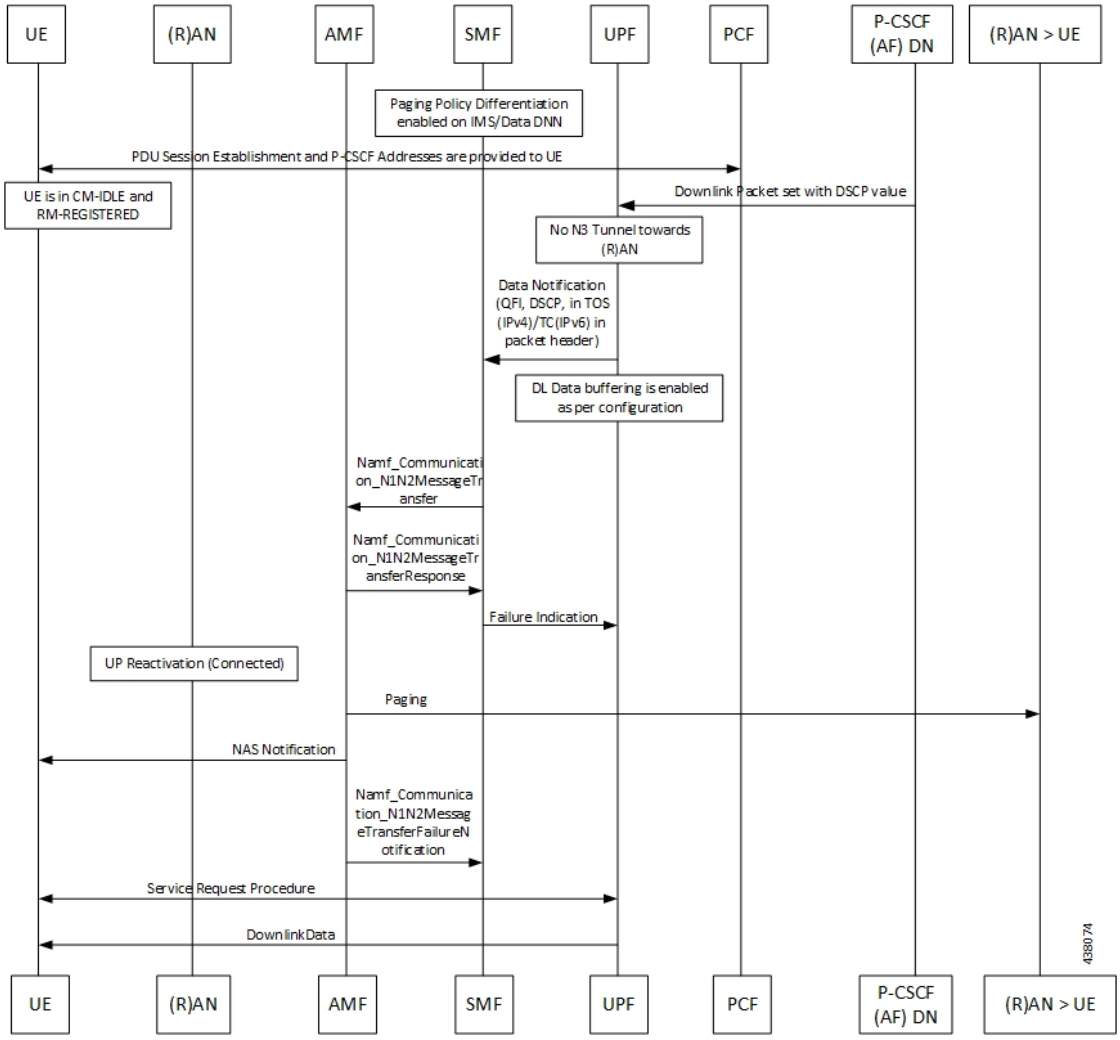


Table 190: VoNR Paging Policy Differentiation Call Flow Description

Step	Description
1	The SMF enables Paging Policy Differentiation (PPD) under DNN profile based on DNN, 5QI, and PLMN.
2	The SMF performs the PDU session establishment procedure as defined in 3GPP TS 23.502 and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with PPD for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
3	The UPF detects if any Downlink (DL) Packet is set with DSCP value (TOS in IPv4 / TC in IPv6) when PPD is enabled for the PDU session.
4	The UPF detects that there is no forwarding path as there is no N3 Tunnel for the DSP marked DL packets.

Step	Description
5	The UPF sends Data-Notification (QFI, DSCP in TOS (IPv4) / TC (IPv6) in packet header).
6	The UPF enables DL Data buffering based on the buffering configuration. The UPF sends Data Notification (N4 Session ID, Information to identify the QoS Flow for the DL data packet, DSCP) message to the SMF. **1.** On arrival of the first DL data packet for any QoS Flow, the UPF sends Data Notification message to the SMF, if the SMF has not previously notified the UPF (in which case the next steps are skipped). **2.** If the UPF receives DL data packets for another QoS Flow in the same PDU session, the UPF sends another Data Notification message to the SMF. **3.** If the Paging Policy Differentiation feature (as specified in *3GPP TS 23.501, section 5.4.3*) is supported by the UPF and if the PDU Session type is IP, the UPF includes the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the DL data packet and the information to identify the QoS Flow for the DL data packet. **4.** The SMF sends the Data Notification Acknowledgement message to the UPF. **5.** The UPF forwards the DL data packets towards the SMF on request. The SMF buffers the data packets.
7	The SMF determines the AMF and invokes the Namf_Communication_N1N2MessageTransfer to the AMF including the PDU Session ID based on N4 Session ID. The SMF, while waiting for the User Plane Connection to be activated, receives additional Data Notification message. The SMF derives a different Paging Policy Indicator according to the additional Data Notification or the DSCP of the data packet. The SMF invokes a new Namf_Communication_N1N2MessageTransfer indicating the higher priority or different Paging Policy Indicator to the AMF. When supporting Paging Policy Differentiation, the SMF determines the Paging Policy Indicator related to the downlink data that has been received from the UPF or triggered the Data Notification message, based on the DSCP as described in *3GPP TS 23.501, section 5.4.3*. The SMF indicates the Paging Policy Indicator in the Namf_Communication_N1N2MessageTransfer.
8	The AMF sends Namf_Communication_N1N2MessageTransfer response to the SMF with a cause “Attempting to reach UE" if the UE is in CM_IDLE State. If the UE is in CM-CONNECTED state, then the AMF sends a Namf_Communication_N1N2MessageTransfer response to the SMF immediately with a cause "N1/N2 transfer success".
9	The SMF sends Failure Indication to the UPF on receiving a negative response from AMF.
10	The AMF initiates paging towards the UE through the (R)AN.
11	The AMF initiates NAS Notification towards the UE.
12	The AMF notifies the SMF by sending Namf_Communications_N1N2MessageTransfer Failure Notification to the Notification Target Address provided by the SMF if the UE does not respond to paging. The AMF is unaware of an ongoing Mobility Management (MM) procedure that prevents the UE from responding. The AMF receives an N14 Context Request message indicating that the UE performs Registration procedure with another AMF.

Step	Description
13	If the UE is in CM-IDLE state, upon receiving a paging request for a PDU session associated to 3GPP access, the UE initiates the UE Triggered Service Request procedure as defined in *3GPP TS 23.502, section 4.2.3.2*.

Configuring the VoNR Paging Profile Differentiation

This section describes how to configure VoNR Paging Profile Differentiation feature.

Configuring VoNR Paging Profile Differentiation feature involves the following steps:

1. Creating PPD Profile
2. Configuring PPD Profile Parameters
3. Enabling PPD in DNN Profile Configuration

Creating PPD Profile

Use the following configuration to create an instance of PPD profile:

```
config
   profile ppd ppd_profile_name
   end
```

NOTES:

- **ppd** *ppd_profile_name*: Specifies the PPD profile. This command creates a PPD profile and provides access to the PPD Profile Configuration mode. For details on the commands supported in this mode, see the *Ultra Cloud Core 5G Session Management Function, CLI Command Reference Guide*. The value of *ppd_profile_name* must be an alphanumeric string.

Configuring PPD Profile Parameters

Use the following configuration to define the PPD profile parameters:

```
config
   profile ppd ppd_profile_name
      5qi 5qi_value
      dscp dscp_value { ppi ppi_value }
      end
```

NOTES:

- **5qi**: Specifies the list of 5QI Priority Level. *5qi_value* must be an integer in the range of 0-127. To list the different priority levels, use comma and hyphen as needed. For example, 5QI 3,10-15,65.
- **dscp** *dscp_value*: Specifies the DSCP value. *dscp_value* must be an integer in the range of 0-63.
- **ppi** *ppi_value:* Specifies the paging policy indicator value. *ppi_value* must be an integer in the range of 0-7.

Enabling PPD in DNN Profile Configuration

Use the following configuration to enable the PPD feature in the existing DNN profile configuration:

```
config
   profile dnn dnn_profile_name
      ppd-profile ppd_profile_name
      end
```

NOTES:

- **ppd-profile** *ppd_profile_name*: This command defines the PPD profile to be associated with the DNN profile. *pdd_profile_name* must be the name of the configured PPD profile.
- This command enables the PPD feature in the DNN profile based on the configured values of DNN, 5QI, and PLMN.

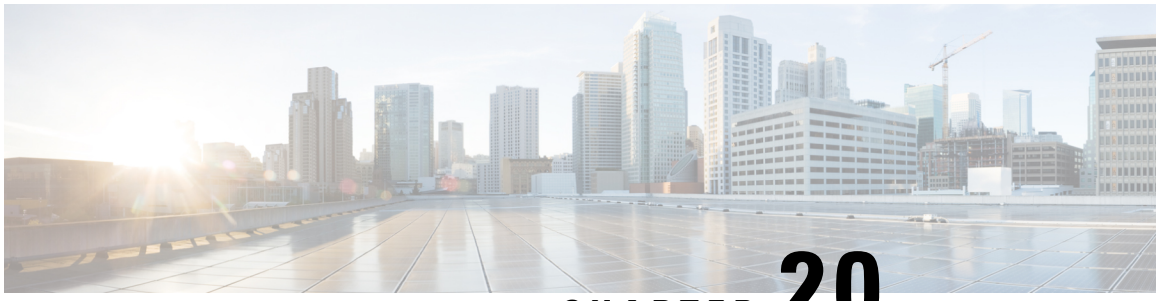
Verifying the Feature Configuration

Use the following show command to verify the feature configuration details.

show running-config

The following is an example of the output of this show command:

```
product smf# show running-config
profile dnn dnntst1
pcscf-profile pcscf1
!
```



CHAPTER 20

Interfaces Support

- Feature Summary and Revision History, on page 545
- Feature Description , on page 548
- 3GPP Specification Compliance for SMF Interfaces, on page 549
- Supported SMF Interfaces, on page 555
- Configuring Interfaces, on page 732
- OAM Support, on page 736

Feature Summary and Revision History

Summary Data

Table 191: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 192: Revision History

Revision Details	Release
Added support for: • Asynchronus and Synchronous Usage Report for Offline Bearer Recalculation • Handling Modify Bearer Request Trigger on the Gz Interface • Gz Change Notification • Default Bearer Modification based on APN-AMBR and Qci change • Handling Periodic Report of Secondary RAT Usage: • EGCDR final record configuration • Zero CDR suppression • Final Unit Indication in subsequent CCR-U • FHT Continue Enhancement • Diameter Credit-Control-Failure-Handling AVP	2023.04.0

Added support for:
• Multiple 3GPP specification compliance for SMF interfaces.
• Gz Interfaces and associated features:
  • PDN Attach and Detach with Gz Interface
  • Gz Usage Reporting
• Indirect communication for NFs through SCP Model D.
• Excluding the optional IE for Locality in the NRF messages.
	2023.03.0

Revision Details	Release

Added support for:
• Gx interfaces and their associated features:
  • Gx initial attach and detach
  • Dynamic and predefined rule
• Gy interfaces and their associated features:
  • Gy usage reporting
  • Gy failure handling
  • Gy MSCC level failure result codes
  • Gy QVT and QHT
  • Gy tarrif time
• IPv6 on data interfaces
	2023.02.0

Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for the SBI interface • 3GPP specification version compliance configuration for CHF server	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3
Added support for: • Cause IE on the N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on the N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for the SBA interface.	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description

Table 193: Feature History

Feature Name	Release Information	Description
Enable IPv6 Connectivity for SMF with Legacy Interfaces	2024.01.1	SMF with legacy interfaces allows IPv6 address configuration to enable communication with the GTP, N4, Gx, and Gy interfaces. With this support, both IPv4 and IPv6 addresses can be used for peer connections. One peer connection can use either IPv4 or IPv6 address. To enable IPv6 connectivity, SMF uses the existing **endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }** and **dual-stack-transport { false | true }** CLI commands. **Default Setting:** Disabled – Configuration Required
Dual Stack Support on N3	2024.01	SMF enables the dual stack transport for the N3 tunnel using the **dual-stack-transport { false | true }** CLI command in the UPF network profile. **Default Setting:** Disabled – Configuration Required

Important The PGW-C term used in this chapter denotes the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

In the 5G System Architecture, the SMF performs the session management functions that the 4G Mobility Management Entity (MME), Serving Gateway Control plane function (SGW-C), and PDN Gateway Control plane function (PGW-C) handle. The SMF is one of the elements of the Service-Based Architecture (SBA). SMF is responsible for communicating with the decoupled data plane, creating, updating, and removing Protocol Data Unit (PDU) sessions. SMF also manages the session context with the User Plane Function (UPF). For the session management-related functions, SMF communicates with various interfaces, such as N1, N4, and N10.

At a given time, the SBI interfaces (N7, N10, N11, and N40) support only an IPv4 or IPv6 address. However, the N3, N4 and GTPC interfaces support either IPv4 or IPv6 address or both. For the IP address support, both

the endpoint and interfaces configuration must include a unique VIP IP and port. For configuration details, see the Configuring Interfaces, on page 732 section.

SMF prioritizes IPv6 over IPv4 addresses while initiating a message on the N4 interface. If the peer GTPC uses both IPv4 and IPv6 addresses, SMF uses the same IP address type on which it has received the last message from the GTPC peer for that particular session, while initiating any new message.

If SMF receives both the IPv4 and IPv6 address as part of a CSR or MBR message, SMF sends an echo using an IPv4 and IPv6 address on the GTPC interface. The peer is considered to be down, only if echo fails on both the interfaces. SMF determines it as path failure and clears the session.

For SBI interfaces, if the discovered NF profile contains both IPv4 and IPv6 addresses, then SMF selects the IP to communicate with the peer NF based on the IP type configuration at SBI endpoint level or interface level for that particular interface.

SMF negotiates between UPF tunnel and RAN by exchanging the IPv6 endpoint identifier information and tunnel information for both.

During HO, SMF creates the tunnel based on the tunnel information received from the target peer and exchanges the tunnel information between UPF and the target peer.

Each interface and endpoint can be independently configured for IPv4 or IPv6 or both based on the current support.

During UPF association setup, the SMF checks if the transport type in the setup request is the same as the configured address. The SMF proceeds with the association request or rejects the request based on the validation result.

Similarly, during NRF discovery, the transport type must match the statically configured transport type either at the endpoint level or interface level. The SMF performs NF selection based on the IP address-matching criteria.

For 4G calls with legacy interfaces, peer SGW IPv4, IPv6, or IPv4v6 data address is supported.

Note DNS, RADIUS, and roaming interfaces currently don’t support the IPv6 address.

3GPP Specification Compliance for SMF Interfaces

Feature Description

The SMF supports configuring any two 3GPP specification compliance versions 15.x (December 2018 and June 2019) for the SMF interfaces N1, N2, N4, N7, N10, N11, N40, and Nnrf. It processes the incoming messages from the peer interfaces in compliance with the profiles configured for the corresponding services.

For more information on a various supported specification versions and the corresponding mapped URI versions for various interfaces, see Standards Compliance section.

For information on the compliance profile configurations, see the Configuring 3GPP Specification Compliance for Interfaces, on page 552 section.

The SMF supports only the IE encoding and decoding functionalities. The existing features work with the June 2019 specification versions. No additional features in the June 2019 version are supported.

Note The SMF continues to support the older versions of 3GPP specifications, and the compliance profile configuration controls the same for the SMF interfaces.

URI Version Selection Logic

When two different 3GPP compliance versions are configured, the Nnrf_NFDiscovery service allows SMF to discover other NF (Network Function) instances with the services they offer, by querying the local NRF (Network Repository Function), i.e CHF, AMF, and PCF.

The Discovery response SearchResult body contains an array of NF Profile objects that satisfy the search filter criteria. The attribute data type **NFServiceVersion** captures the versions supported by various peer NFs.

Based on SMF profile configuration versions and the version received in the Discovery SearchResult, the SMF selects a version for peer NFs for subsequent messages.

The logic based on which the SMF selects the versions for peer NFs, is called the URI Version Selection Logic. It selects the highest version for the peer NFs.

The following table describes how the URI version selection logic selects a suitable version for peers upon receiving the NFServiceVersion as a result of the Discovery response:

Table 194: URI Selection Logic

SMF Compliance Configuration Versions	Discovery Search Result Versions	Selected Version for Peer NFs
V2, V1	V2, V1	V2
V2, V1	V1	V1
V1	V2, V1	V1

Once the version for peer NFs is selected, the subsequent message is sent using the selected version. If during the first message exchange the selected peer NF goes down, the SMF selects another peer with the same or next highest NF version.

After the first message exchange if the selected peer NFs go down, the SMF will not select another peer with the same or different version for the session.

Standards Compliance

The SMF is one of the Control Plane (CP) NFs of the 5G core network. The SMF uses different interfaces to communicate with the other NFs or nodes.

For example, the N4 interface exists between the SMF and User Plane Function (UPF). Each SMF interface complies with a specific version of the 3GPP specification, depending on the supported compliance version.

Use the following table to determine the compliance mapping of each SMF interface and the 3GPP Standards specification versions.

Table 195: SMF Interface and 3GPP Standards Specification Version Map

Interface	Relationship	3GPP Specification	Version
N1/NAS	Between UE and AMF	*24.501*	For December 2018 Compliance Support: *15.2.0* For June 2019 Compliance Support: *15.4.0* Supported Specifications: *15.2.0*, ***15.4.0*** Mapped URI: *V1*
N2/NGAP	Between RAN and AMF	*38.413*	For December 2018 Compliance Support: *15.2.0* For June 2019 Compliance Support:*15.4.0* Supported Specifications: *15.0.0*, *15.2.0*, ***15.4.0*** Mapped URI: *V1*
N4	Between UPF and SMF	*29.244*	For December 2018 Compliance Support: *15.2.0* For June 2019 Compliance Support: *15.4.0*
N7	Between PCF and SMF	*29.512*	For December 2018 Compliance Support: *15.2.0* For June 2019 Compliance Support: *15.4.0* Supported Specifications: *15.0.0*, *15.2.0*, ***15.4.0*** Mapped URI: *V1*
N10	Between UDM and SMF	*29.503*	For December 2018 Compliance Support: *15.2.1* For June 2019 Compliance Support: *15.4.0* Supported Specifications: *15.1.0*,*1 5.2.1*, ***15.4.0*** Mapped URI: • *V1: 15.1.0, 1 5.2.1* • *V2: 15.4.0*
N11	Between AMF and SMF	*29.518* *29.502*	For December 2018 Compliance Support: *15.2.0* For June 2019 Compliance Support: *15.4.0* Supported Specifications: 15.0.0, 15.2.0, **15.4.0** Mapped URI: *V1*

Interface	Relationship	3GPP Specification	Version
N40	Between SMF and CHF	*32.291*	For December 2018 Compliance Support: *15.1.0* For June 2019 Compliance Support: *15.3.0* Supported Specifications: *15.0.0,15.1.0, 15.2.1,* ***15.3.0****, 15.3.0.custom, 15.3.0.std* Mapped URI: • *V1: 15.0.0, 15.1.0* • *V2 15.2.1, 15.3.0, 15.3.0 std, 15.3.0 custom*
Nnrf	Between NRF and SMF	*29.510*	For December 2018 Compliance Support: *15.0.0* For June 2019 Compliance Support: *15.4.0* Supported Specifications: *15.0.0, 15.2.0,* ***15.4.0*** Mapped URI: *V1*

Configuring 3GPP Specification Compliance for Interfaces

To configure the SMF interfaces in compliance with the 3GPP specifications, use the following sample configuration:

```
config
   profile compliance profile_name
       service { n1 | n2 | namf-comm | nchf-convergedcharging | nnrf-disc
 | nnrf-nfm | npcf-smpolicycontrol | nsmf-pdusession | nudm-sdm | nudm-uecm
 | threegpp23502 }
          version { full version_format| spec spec_version| uri uri_version }
          version-list version  version_name { full version_format | mode {
active | offline } | spec  spec_version | uri  uri_version }
          end
       end
   end
```

Important Service selection is based only on the specification version. In future releases, the full API version will be used.

NOTES:

- **service { n1 | n2 | namf-comm | nchf-convergedcharging | nnrf-disc | nnrf-nfm | npcf-smpolicycontrol | nsmf-pdusession | nudm-sdm | nudm-uecm | threegpp23502 }**—Specify the service names as cited in the *3GPP TS 29.510 version 15.2.0, section 6.1.6.3.11*.

Note The compliance profile configuration for the **nchf-convergedcharging** service supports the *3GPP TS 29.510 version 15.4.0* specification. With this configured version, the SMF sends the subscriberIdentifier in the following format to CHF:

"subscriberIdentifier":"imsi-123456789"

- **version**—Specify the compliance version name to be configured. It allows configuring only one version at a time.
- **full** *version_format*—Specify the API full version for each service in the following format:

  <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]

  The format is specified in the *3GPP TS 29.501 version 15.2.0, section 4.3.1.1*.
- **spec** *spec_version*—Specify the 3GPP specification version number, which is one of the following values:
  - 15.0.0
  - 15.1.0
  - 15.2.0
  - 15.2.1
  - 15.3.0
  - 15.3.0.custom
  - 15.3.0.std
  - 15.4.0

  For example, to support 3GPP June 2019 specification compliance for the N7 (PCF) interface, configure the specification version as *15.4.0*.

  The default version number depends on the SMF interface. For example, the default version is *15.2.0* for the N7 interface. Similarly, for the N10 interface, the default version is *15.2.1*.
- **uri** *uri_version*—Specify the API version URI for each service in the following format:

  v—Concatenated with a number, where the value can be both v1 and v2, or either v1 or v2.

  Examples:

  —For the compliance version 15.4.0 in the NRF configuration for the service type nudm-sdm, mandate the configuration of the uri-version in the version to v2. For the compliance version 15.2.1, this configuration is optional.

  —version v1: (- url: '{apiRoot}/nsmf-pdusession/v1').
- **version-list version** *version_name*—Specify the list of compliance versions of the 3GPP specification. If the **version-list version** is configured with only one version, then both **version** and **version-list version** CLIs are considered for version selection logic for peer NFs. Both the CLIs **version** and **version-list version** allow configuring the same set of attributes.

Note **version-list version** is supported for only for N1, N2, N7, N10, N11, N40, and Nnrf interfaces.

- **mode { active | offline }**—Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration under the CLI **version-list version**. The default value of **mode** is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Important Configuring the 3GPP specification version value depends on the SMF interface. Not all the preceding versions are options for the SMF interfaces. Only a combination of the preceding versions exists as an option for the 3GPP version compliance configuration. For details on the compliance version, see the Standards Compliance, on page 550 section.

Important The 15.3.0.custom spec version is customer specific and applicable only to the **nchf-convergedcharging** service. For more details, contact your Cisco account representative.

In this spec version, the MultipleUnitUsage attribute sends the usedUnitContainer field in upper case. For all other spec versions post 15.3.0, the MultipleUnitUsage attribute sends the UsedUnitContainer field in lower case.

Important The release version 2023.03.0 supports both **version** and **version-list version** CLIs. However, the **version** CLI will be discontinued from the future releases.

Configuration Verification

To verify if the 3GPP specification profile compliance is configured, use the following **show full-configuration profile smf** command:

```
[smf] smf(config)# show full-configuration profile smf
profile smf smf1
 locality      LOC1
 instances 1 allowed-nssai [ slice1 ]
 instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123 node-id abcdef
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 242 mnc 01
 exit
 plmn-list mcc 310 mnc 210
 exit
 plmn-list mcc 310 mnc 220
 exit
 plmn-list mcc 310 mnc 260
 exit
 plmn-list mcc 310 mnc 310
 exit
 plmn-list mcc 440 mnc 550
 exit
 service name nsmf-pdu
```

```
  type               pdu-session
  schema             http
  service-id         1
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
```

To verify the configuration, use the **show full** command in the 3GPP specification profile compliance configuration mode:

```
product smf(config-compliance-comp1)# show full
profile compliance comp1
   service nsmf-pdusession
      version uri v1
      version full 1.0.0
      version spec 15.2.0
```

Supported SMF Interfaces

This section describes the different interfaces that SMF uses to facilitate communication with other network functions.

GTP Interface

General Packet Radio Service (GPRS) Tunneling Protocol (GTP) is the primary protocol used in a GPRS core network through 3G, 4G, or 5G networks. The GTP is responsible for signaling and transporting mobile data within the core network.

The GTP uses the N9 interface as the reference point between two core user plane functions (UPFs).

GTP Cause Code Handling

Feature Description

The SMF supports the GTP cause code handling for 4G procedures when it detects any failure with IEs.

Create Session Request

The SMF supports the following causes in the Create Session Request message.

Table 196: Supported Causes in Create Session Request

Cause	SMF Behavior
Missing or unknown APN	If the configured DNN does not match the DNN received in the Create Session Request, then the SMF rejects the message with this cause value in the Create Session Response and sets the appropriate disconnect reason.

Cause	SMF Behavior
User authentication failed	If the SMF receives a failed AAA secondary authentication response from RADIUS, then SMF rejects the message with this cause value in Create Session Response. This cause indicates that the request is rejected due to failure in authentication or security procedure and sets the appropriate disconnect reason.
APN access denied – no subscription	If the SMF receives the subscription fetch failure response from the UDM, then the SMF rejects the message with this cause value in the Create Session Response. This cause indicates that the SMF has denied the user access to an APN because the subscriber does not have the necessary subscription. SMF also sets the appropriate disconnect reason.
New PDN type due to single address bearer only	If the Dual Address Bearer Flag (DAF) indication is not set and the requested PDN-type is IPV4V6 in Create Session Request message, then the SMF rejects the message with this cause value in Create Session Response. SMF also sets the appropriate disconnect reason.
Late Overlapping Request	The Create Session Request message includes the Origination Time Stamp indicating the absolute time at which the request is initiated (as specified in clause 13.2.2, TS29.274). If SMF receives any subsequent CSR from different S-GW and different sequence number with older timestamp in "Origination Time Stamp" than the time stamp stored for the existing session, then SMF rejects the new CSR with this cause value in Create Session Response. This cause indicates the incoming request collides with an existing session that does not have a recent time stamp than the time stamp of the new request. If the timestamp is newer, then SMF aborts the current procedure and handles the new CSR request with the recent time stamp.
Timed Out Request	If the incoming CSR received origination-time-stamp and maximum-wait-time IEs, SMF starts the SLA timer with maximum-wait-time value at the start of the Create procedure and aborts the Create procedure on expiry of the timer. Then SMF rejects with this cause value in CSR Response.
New PDN type due to network preference	If the session type configured under profile dnn is IPv4 or IPv6, and the requested PDN type coming in Create Session Request is IPv4v6, then SMF rejects the message with this cause value in Create Session Response.

Delete Bearer Request

The SMF supports the following causes in the Delete Bearer Request message.

Table 197: Supported Causes in Delete Bearer Request

Cause	Scenario
Reactivation required	SMF sends Delete Bearer Response for default bearer with this cause value in the following cases: • CHF reconciliation • PCF reconciliation • Internal DB conflict • Session Report with SRSR/GTER/SRIR/SPTER/ERIR
PDN connection inactivity timer expires	SMF sends Delete Bearer Response for default bearer with this cause value in the following cases: • CP-IDLE timer expiry • Session Report with UPIR • Absolute Timer Expiry

RAN/NAS Cause IE

SMF receives the RAN/NAS Cause IE from access network in the GTP messages due to QoS flow termination or PDU session termination. SMF provides the received cause in the ranNasRelCauses attribute of the RuleReport to PCF. For more information about this cause, see the 3GPP TS 29.274 version 15.4.0.

The RAN/NAS Cause IE supports the following GTP messages:

- Create Bearer Response
- Update Bearer Response
- Delete Bearer Command
- Delete Session Request

Spec-Derived Cause Code Mapping

The SMF supports specification derived (TS 29.524) cause code mapping for 5G messages for UDM and PCF interfaces.

Table 198: Mapping from HTTP to 5GSM cause values—Request rejected by UDM due to N10 failures

HTTP Status Code on N10	Protocol or Application Error	5GSM Cause to UE
403 Forbidden	ROAMING_NOT_ALLOWED	Cause #29—User authentication or authorization failed
	DNN_NOT_ALLOWED	Cause #27—Missing or unknown DNN
404 Not Found	USER NOT FOUND	Cause #29—User authentication or authorization failed

Table 199: Mapping from HTTP to 5GSM cause values—Request rejected by PCF

HTTP Status Code on N7	Protocol or Application Error	5GSM Cause to UE
400 Bad Request	USER_UNKNOWN	Cause #29—User authentication or authorization failed
	ERROR_INITIAL_PARAMETERS	Cause #31—Request rejected, unspecified
	ERROR_TRIGGER_EVENT	Cause #31—Request rejected, unspecified
403 Forbidden	ERROR_TRAFFIC_MAPPING_INFO_REJECTED	Cause #29—User authentication or authorization failed
	ERROR_CONFLICTING_REQUEST	Cause #67—insufficient resources for specific slice and DNN
	POLICY_CONTEXT_DENIED	Cause #29—User authentication or authorization failed
	VALIDATION_CONDITION_NOT_MET	Cause #29—User authentication or authorization failed

Standards Compliance

The supported GTP cause codes comply with the following standards:

- 3GPP TS 29.274, Version 15.4.0
- 3GPP TS 29.524

Configuring GTP Cause Codes

This section describes how to configure cause-to-class mapping and class-to-cause mapping.

For source interface failures, the **cause-map-class** profile determines which **class-map-cause** profile must be applied on the corresponding target interface, only if the latter is configured under access profile. The respective CLI configurations send the user-defined cause values to the target interface based on the source interface failures and cause values. If the CLI commands are not configured, the target interface sends the spec-driven cause values as default values.

Configuring the GTP cause codes involves the following steps:

- Cause to Class Mapping Configuration, on page 559
  - Configuring Cause-to-Class Map under cause-map-class Profile, on page 559
  - Configuring Cause-to-Class Map under Network-Element Profile, on page 559
- Class to Cause Mapping Configuration, on page 560
  - Configuring Class-to-Cause Map under class-map-cause Profile, on page 560
  - Configuring Class-to-Cause Map under Access Profile, on page 561

Cause to Class Mapping Configuration

This section describes how to configure cause to class mapping in SMF.

Configuring Cause-to-Class Map under cause-map-class Profile

To configure cause-to-class mapping under the cause-map-class profile, use the following sample configuration:

```
config
  profile cause-map-class nf-type [ udm | pcf ] cmc_profile_name
    source { status-code httpv2_code cause cause_value } fail-class
failclass_string
    exit
```

NOTES:

- **profile cause-map-class nf-type [udm | pcf]** *cmc_profile_name*: Specify the NF profile name to configure the cause-map-class profile.
- **source { status-code** *httpv2_code* **cause** *cause_value* **} fail-class** *failclass_string*
  - **status-code** *httpv2_code*: Specify the HTTPv2 status code of the source interface.
  - **cause** *cause_value*: Specify the cause value as a string.
  - **fail-class** *failclass_string*: Specify the failure class as a string.
- The **profile cause-map-class** is associated to the network-element profile.
- The **status-code** and **cause** keywords are optional. If both are configured, then the corresponding **fail-class** is given higher priority followed by **status-code** and **cause**.

Example

The following is an example of the UDM interface configuration:

```
profile cause-map-class nf-type udm UDM-CMC
     source status-code 403 cause DNN_NOT ALLOWED fail-class congestion
```

Configuring Cause-to-Class Map under Network-Element Profile

To configure cause-to-class mapping under the network-element profile, use the following sample configuration:

```
config
  profile network-element [ udm | pcf ] nfprofile_name
    cause-map-class-profile cmcp_name
    exit
```

NOTES:

- **profile network-element [udm | pcf]** *nfprofile_name*: Specify the NF profile name to configure the network-element profile.
- **cause-map-class-profile** *cmcp_name*: Specify the cause-to-class map profile name.

Example

The following is an example of the UDM interface configuration:

```
profile network-element udm nfprf-udm
     cause-map-class UDM-CMC
```

Sample Configuration

```
[smf] smf# show running-config profile cause-map-class
profile cause-map-class nf-type udm CMC-UDM-1
 source status-code 500 cause CAUSE2 fail-class failClass2
 source status-code 500 cause CAUSE3 fail-class failClass3
 source status-code 501 cause CAUSE1 fail-class failClass1
 source status-code 502 cause CAUSE2 fail-class failClass1
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type udm CMC-UDM-2
 source status-code 501 cause CAUSE1 fail-class failClass6
 source status-code 501 cause any fail-class failClass6
 source status-code 502 cause CAUSE1 fail-class failClass6
 source status-code 502 cause CAUSE2 fail-class failClass6
 source status-code 502 cause any fail-class failClass6
 source status-code any cause CAUSE1 fail-class failClass6
 source status-code any cause CAUSE2 fail-class failClass6
exit
profile cause-map-class nf-type udm CMC-UDM-3
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-1
 source status-code 500 cause CAUSE2 fail-class failClass2
 source status-code 500 cause CAUSE3 fail-class failClass3
 source status-code 501 cause CAUSE1 fail-class failClass1
 source status-code 502 cause CAUSE2 fail-class failClass1
 source status-code 504 cause CAUSE4 fail-class failClass4
 source status-code 505 cause CAUSE4 fail-class failClass5
exit
profile cause-map-class nf-type pcf PCF-CMC-2
 source status-code 500 cause any fail-class failClass2
 source status-code 501 cause any fail-class failClass3
 source status-code any cause CAUSE2 fail-class failClass2
 source status-code any cause CAUSE3 fail-class failClass3
exit
[smf] smf#
```

Class to Cause Mapping Configuration

This section describes how to configure class to cause mapping in SMF.

Configuring Class-to-Cause Map under class-map-cause Profile

To configure class-to-cause mapping under the class-map-cause profile, use the following sample configuration:

```
config
  profile class-map-cause cmc_profile_name
    fail-class failclass_string
      target n11 { status-code  httpv2_code cause cause_value } | [ n1 | n2
| gtp ] { cause cause_value }
      exit
```

NOTES:

- **profile class-map-cause** *cmc_profile_name*: Specify the profile name to configure class-map-cause.
- **fail-class** *failclass_string*: Specify the failure class as a string.

- **target n11 { status-code** *httpv2_code* **cause** *cause_value* **} | [n1 | n2 | gtp] { cause** *cause_value* **}**:
  - **target**: Specify the target interface.
  - **status-code** *httpv2_code*: Specify the HTTPv2 status code for the target interface.
  - **cause** *cause_value*: Specify the cause value for the target interface.
- The **profile class-map-cause** is associated to the access profile.
- The **status-code** keyword is not applicable to the GTP, N1, and N2 interfaces.

Example

The following is an example of the CLI configuration:

```
profile class-map-cause cmc1
    fail-class congestion
         target gtp cause 72
```

Configuring Class-to-Cause Map under Access Profile

To configure class-to-cause mapping under the access profile, use the following sample configuration:

```
config
  profile access access_profile_name
    [ gtpc | n1 | n2 | n11 ] class-map-cause-profile cmc_profile_name
    exit
```

NOTES:

- **profile access** *access_profile_name*: Specify the profile name to configure the access profile.
- **class-map-cause-profile** *cmc_profile_name*: Specify the profile name to configure the class-to-cause map profile.

Example

The following is an example of the CLI configuration:

```
profile access access1
       n11 class-map-cause cmc1
```

Sample Configuration

```
[smf] smf# show running-config profile class-map-cause
profile class-map-cause CMC
 fail-class failClass1
  target n11 status-code 403 cause CA1
  target n1 cause CA_N1
  target n2 cause CA_n2
  target gtp cause 75
 exit
 fail-class failClass2
  target n11 status-code 402 cause CAUSE4
  target n1 cause CAUSE3
  target n2 cause CAUSE2
  target gtp cause 95
 exit
```

```
exit
[smf] smf#
```

GTP Cause Code Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The source interface failures support the following disconnect reasons:

- disc_new_pdn_type_due_to_single_addr_bearer_only—The number of Create Session Request failures with cause value "New PDN type due to single address bearer only" in Create Session Response.
- disc_new_pdn_type_due_to_network_preference—The number of Create Session Request failures with cause value "New PDN type due to network preference" in Create Session Response.
- disc_pdnsetup_dnn_missing_or_unknown—The number of Create Session Request failures with cause value "Missing or unknown APN" in Create Session Response.
- disc_request_timeout_at_originating_entry—The number of Create Session Request failures with cause value "Timed Out Request" in Create Session Response.

GTPv2 IE and Cause Codes

Feature Description

This section describes the GPRS Tunneling Protocol, Version 2 (GTPv2) IEs and cause codes for 4G and 5G procedures.

Cause Source Errors

The Cause Source (CS) bit supports the following cause values in Create Session Response, Modify Bearer Response, Modify Bearer Failure Indication (MBFI), or Delete Bearer Failure Indication (DBFI).

Table 200: CS Bit Causes

Cause Value	Scenario
Context Not Found	When the subscriber is not present in SMF and receives Create Session Response with handover indication, the SMF sends this cause.
Missing Or Unknown APN	When Create Session Response receives missing or unknown APN, the SMF sends this cause.
DBFI with Context Not Found	When the subscriber is not present in SMF and receives Delete Bearer Command, the SMF sends this cause.
Delete Session Response with Context Not Found	When the subscriber is not present in SMF and receives a Delete Session Request in old TEID, the SMF sends this cause.

Bearer Context IE Errors

The Bearer Context IE Error (BCE) bit supports the following cause values in Delete Session Response, Modify Bearer Response, Modify Bearer Failure Indication (MBFI), or Delete Bearer Failure Indication (DBFI).

Table 201: BCE Bit Causes

Cause Value	SMF Behavior or Scenario
MBFI with Context Not Found	When SMF receives Modify Bearer Request with a wrong EBI in bearer context, the SMF sends this cause.
DBFI with Context Not Found	When SMF receives Delete Bearer Command with a wrong EBI in bearer context, the SMF sends this cause.

Remote Node Errors

SMF supports the following remote node errors:

- Context not found
- Missing or unknown APN
- PduSessionType
- Mandatory IE missing
- Malformed message errors

Statistics Support

This feature supports the following statistics related to GTPC messages:

smf_gtpc_msg_stats

Description: Stats for GTPC interface messages

Sample Query: `'smf_gtpc_msg_stats{message_type="modify_bearer_request"}'`

Labels:

- Label: `message_type`

  Label Description: GTPC Message Type

  Example: modify_bearer_request, delete_bearer_request, delete_session_request

- Label: `status`

  Label Description: GTPC message status

  Example: attempted, success, failures

- Label: `reason`

  Label Description: The reason associated with the failure

Example: ipc_failed, sgw_failure, EGTP_CAUSE_LOCAL_DETACH,
EGTP_CAUSE_RAT_CHANGED_FROM_3GPP_TO_NON_3GPP,
EGTP_CAUSE_COMPLETE_DETACH, EGTP_CAUSE_ISR_DEACTIVATION,
EGTP_CAUSE_ERROR_IND_RCVD_RNC_ENODE, EGTP_CAUSE_IMSI_DETACH_ONLY,
EGTP_CAUSE_REACTIVATION_REQUESTED,
EGTP_CAUSE_PDN_RECONNECTION_TO_THIS_APN_DISALLOWED,
EGTP_CAUSE_ACCESS_CHANGED_FROM_NON_3GPP_TO_3GPP,
EGTP_CAUSE_PDN_CONN_INACTIVITY_TIMER_EXPIRED,
EGTP_CAUSE_PGW_NOT_RESPONDING, EGTP_CAUSE_NETWORK_FAILURE,
EGTP_CAUSE_QOS_PARAMETER_MISMATCH, EGTP_CAUSE_REQ_ACCEPTED,
EGTP_CAUSE_REQ_ACCEPTED_PARTIALLY,
EGTP_CAUSE_NEW_PDN_TYPE_NETWORK_PREFERENCE,
EGTP_CAUSE_NEW_PDN_TYPE_SINGLE_ADDR_BEARER_ONLY,
EGTP_CAUSE_CONTEXT_NOT_FOUND, EGTP_CAUSE_INVALID_MESSAGE_FORMAT,
EGTP_CAUSE_VERSION_NOT_SUPPORTED_BY_NEXT_PEER,
EGTP_CAUSE_INVALID_LENGTH, EGTP_CAUSE_SERVICE_NOT_SUPPORTED,
EGTP_CAUSE_MANDATORY_IE_INCORRECT, EGTP_CAUSE_MANDATORY_IE_MISSING,
EGTP_CAUSE_SYSTEM_FAILURE, EGTP_CAUSE_NO_RESOURCES_AVAILABLE,
EGTP_CAUSE_SEMANTIC_ERROR_IN_TFT_OPERATION,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_TFT_OPERATION,
EGTP_CAUSE_SEMANTIC_ERROR_IN_PKT_FILTERS,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_PKT_FILTERS,
EGTP_CAUSE_MISSING_OR_UNKNOWN_APN, EGTP_CAUSE_UNEXPECTED_REPEATED_IE,
EGTP_CAUSE_GRE_KEY_NOT_FOUND, EGTP_CAUSE_REALLOCATION_FAILURE,
EGTP_CAUSE_DENIED_IN_RAT, EGTP_CAUSE_PREFERRED_PDN_TYPE_UNSUPPORTED,
EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCPUPIED,
EGTP_CAUSE_UE_CTX_WO_TFT_ALREADY_ACTIVATED,
EGTP_CAUSE_PROTOCOL_TYPE_NOT_SUPPORTED, EGTP_CAUSE_UE_NOT_RESPONDING,
EGTP_CAUSE_UE_REFUSES, EGTP_CAUSE_SERVICE_DENIED,
EGTP_CAUSE_UNABLE_TO_PAGE_UE, EGTP_CAUSE_NO_MEMORY_AVAILABLE,
EGTP_CAUSE_USER_AUTHENTICATION_FAILED,
EGTP_CAUSE_APN_DENIED_NO_SUBSCRIPTION, EGTP_CAUSE_REQUEST_REJECTED,
EGTP_CAUSE_PTMSI_SIGNATURE_MISMATCH, EGTP_CAUSE_IMSI_IMEI_NOT_KNOWN,
EGTP_CAUSE_SEMANTIC_ERROR_IN_TAD_OPERATION,
EGTP_CAUSE_SYNTACTIC_ERROR_IN_TAD_OPERATION,
EGTP_CAUSE_RESERVED_MESSAGE_VALUE_RECEIVED,
EGTP_CAUSE_PEER_NOT_RESPONDING,
EGTP_CAUSE_COLLISION_WITH_NETWORK_INIT_REQUEST,
EGTP_CAUSE_UNABLE_TO_PAGE_UE_DUE_TO_SUSPENSION,
EGTP_CAUSE_CONDITIONAL_IE_MISSING, EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE,
EGTP_CAUSE_INVALID_LENGTH_WITH_PIGGYBACK_MSG,
EGTP_CAUSE_DATA_FORWARDING_NOT_SUPPORTED,
EGTP_CAUSE_INVALID_REPLY_FROM_REMOTE_PEER,
EGTP_CAUSE_FALLBACK_TO_GTPV1, EGTP_CAUSE_INVALID_PEER,
EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS,
EGTP_CAUSE_REQ_REJECTED_FOR_PMIPV6_REASON, EGTP_CAUSE_APN_CONGESTION,
EGTP_CAUSE_BEARER_HANDLING_NOT_SUPPORTED,
EGTP_CAUSE_UE_ALREADY_REATTACHED,
EGTP_CAUSE_MULTI_PDN_CONNECTION_FOR_APN_NOT_ALLOWED,
EGTP_CAUSE_MME_SGSN_REFUSES_DUE_TO_VPLMN_POLICY,
EGTP_CAUSE_GTPC_ENTITY_CONGESTION,

EGTP_CAUSE_TARGET_ACCESS_RESTRICTED_FOR_THE_SUBSCRIBER, EGTP_CAUSE_UE_TEMP_NOT_REACHABLE_DUE_TO_POWER_SAVING, EGTP_CAUSE_RELOC_FAILURE_DUE_TO_NAS_MSG_REDIRECTION, EGTP_CAUSE_MISSING_TIMESTAMP_OPTION, EGTP_CAUSE_MULTIPLE_HNP_NOT_ALLOWED, EGTP_CAUSE_SN_MALFORMED_MSG, EGTP_CAUSE_INT_TIMEOUT

- Label: `qos_5qi`

  Label Description: 5Qi applicable for the QoS flow

  Example: 1, 2, 5

- Label: `rat_type`

  Label Description: Type of the radio access associated with the request

  Example: EUTRA, NR, WLAN, rat_type_unknown

- Label: `smf_current_procedure`

  Label Description: Current Procedure Name for Message Level Stats

  Example: nr_to_untrusted_wifi_handover, eps_fb_ded_brr, PdnDisconnectProcedure, enb_to_untrusted_wifi_handover, pcf_req_ded_brr_create, pcf_req_ded_brr_delete, pcf_req_ded_brr_mod, smf_initiated_pdn_detach, untrusted_wifi_to_enb_handover, upf_sess_report_srir_sess_rel, utn3gpp_to_5g_handover

Gx Interface

The Gx interface is an interface between SMF and Policy and Charging Rules Function (PCRF).

This section describes about the Gx support on the SMF. It includes the details of all the AVPs supported over the Gx interface.

Feature Description

The policy control and charging (PCC) architecture allows operators to perform service-based QoS policy and flow based charging control. The PCC provides access control, resource control, and QoS control.

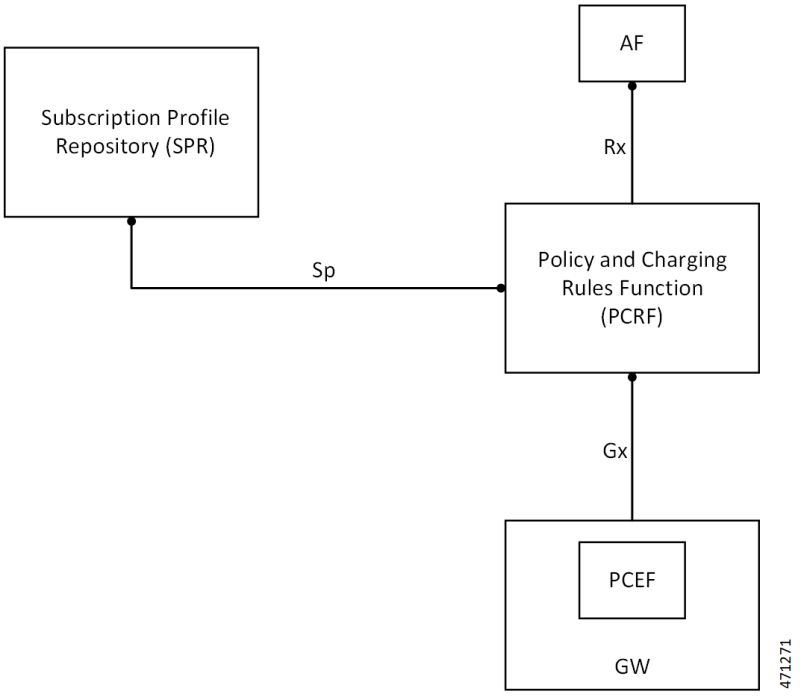
How it Works

The Gx support for SMF uses the following two main elements in the PCC architecture.

- PCEF (Policy enforcement functionality within SMF)
- PCRF (Policy and charging rules function)

Gx reference point lies between the PCRF and the SMF. The Gx reference point allows the provisioning and removal of PCC rules. The following diagram shows the reference points between various elements involved in the policy infrastructure.

Figure 128: Gx Interface



The Gx interface implementation is a part of the diameter connection. The Gx messages commonly involve installing/removing dynamic rules and activating/deactivating predefined rules, and modifying APN-AMBR and Default Bearer QoS.

Associating a rule with a bearer is the task of 'bearer binding'. The PCEF performs this task in SMF. The binding mechanism is the procedure that associates a service data flow. The flow is defined in a PCC rule by the SDF template to the IP-CAN bearer (deemed to transport the service data flow).

- **PCEF bearer binding**: The PCEF binds a rule to a bearer. This rule may require to perform a bearer activation or update. The SMF service performs the task of updating or creating a new Bearer. This update happens by invoking the UBR or CBR request towards SGW/MME.

Note In the current release, PCEF binding only for default bearer is supported.

Gx Initial Attach and Detach Support

Following are the various types of rules associated with the Gx initial attach and detach support for SMF:

- **PCC Rules**: As a part of the initial attach. The PCEF supports:
  - Installation of the dynamic rules using Charging-Rule-Definition AVP
  - Predefined rules using Charging-Rule-Name AVP
  - Bearer binding to the default bearer

Note The CBR procedure and UBR for TFT updates on default bearer is not supported in current release.

- **Rulebase Selection**: PCEF supports the processing of the Charging-Rule-Base-Name AVP. The processing happens as a part of CCA-I and overwrites the ECS rulebase name configuration as part of DNN.
- **APN-AMBR**: The APN-AMBR values as a part of Qos-Information AVP by PCRF during the CCA-I/CCA-U/RAR are processed and applied on the call.
- **Default Bearer QoS**: The values authorized by PCRF using Default-EPS-Bearer-QoS AVP during the CCA-I/CCA-U/RAR are processed and applied on the call.

Following are the AVPs supported over Gx (CCR/CCA/RAR/RAA) interface for SMF:

- Origin-Host
- Origin-Realm
- Destination-Realm
- CC-Request-Type
- CC-Request-Number
- Destination-Host
- Subscription-Id
  - Subscription-Id-Type
  - Subscription-Id-Data
- Supported-Features
  - Vendor-Id
  - Feature-List-ID
  - Feature-List
- Network-Request-Support
- Framed-IP-Address
- Framed-IPv6-Prefix
- IP-CAN-Type
- 3GPP-RAT-Type
- Termination-Cause
- User-Equipment-Info
  - User-Equipment-Info-Type
  - User-Equipment -Info-Value

- QoS-Information
  - APN-Aggregate-Max-Bitrate-UL
  - APN-Aggregate-Max-Bitrate-DL
- Default-EPS-Bearer-QoS
  - QoS-Class-Identifier
  - Allocation-Retention-Priority
    - Priority-Level
    - Pre-Emption-Capability
    - Pre-Emption-Vulnerability
- AN-GW-Address
- 3GPP-SGSN-MCC-MNC
- 3GPP-User-Location-Info
- 3GPP-MS-TimeZone
- Called-Station-Id
- Bearer-Usage
- Online
- Offline
- Charging-Rule-Report
  - Charging-Rule-Name
  - Charging-Rule-Base-Name
  - PCC-Rule-Status
  - Rule-Failure-Code
- Event-Trigger
- Access-Network-Charging-Address
- Access-Network-Charging-Identifier-Gx
  - Access-Network-Charging-Identifier-Value
- Charging-Rule-Install
  - Charging-Rule-Definition
    - Charging-Rule-Name
    - Service-Identifier
    - Rating-Group

- Flow-Information
  - Flow-Description
  - ToS-Traffic-Class
  - Security-Parameter-Index
  - Flow-Label
- Flow-Status
- QoS-Information
- Reporting-Level
- Online
- Offline
- Precedence

- Charging-Rule-Name
- Charging-Rule-Base-Name

- Charging-Rule-Remove
  - Charging-Rule-Name
  - Charging-Rule-Base-Name

SMF advertises the following supported features over Gx interface towards Policy Server (PCRF):

Table 202: Supported Features of Feature-List-ID 1

Feature Bit	Feature
0	Rel8
5	ADC

Table 203: Supported Features of Feature-List-ID 2

Feature Bit	Feature
7	Extended-BW-NR

Origin Host and Origin Realm for Gx

For each subscriber, SMF maintains a record of the Origin-Realm and Origin-Host attribute information sent by PCRF through Diameter messages. If there's any value change to the Origin-Host and Origin-Realm

attributes, SMF updates the latest value and interacts with the corresponding destination host. Later, SMF increments the policy_pcrf_dest_host_change statistics for every change in the attribute value.

Dynamic and Predefined Rule Support

Dynamic Rule

This feature supports the dynamic rule installation for SMF by using the "Charging Rule Definition" AVP. See Gx Initial Attach and Detach Support, on page 566 for the list of AVPs supported as part of Charging-Rule-Definition.

Note The dynamic rule installation support is only available on default bearer in the current release.

Predefined Rule

This feature supports the predefined rule (Charging Rule Name) installation for SMF using the "Charging Rule Name" AVP.

Note The predefined rule installation support is only available on default bearer in the current release.

Charging Rule Base Name (CRBN)

When PCEF receives the "Charging-Rule-Base-Name" AVP from PCRF, it treats the AVP as an ECS rulebase or installation of group of ruledef. This behavior depends on the CLI present in the active charging service configuration.

```
config
  active-charging service  service_name
    policy-control charging-rule-base-name gor
    end
```

Note By default, the "Charging-Rule-Base-Name" AVP is the ECS rulebase for the call.

N4 Support for Initial Attach/Detach

User-Plane and Control-Plane combined together provide the functionality of a node for other elements in the EPC network. SMF supports the N4 interface towards UP.

- **Initial Attach Support (N4 Session Establishment Request)**:

  SMF supports sending the necessary PDR, FAR, QER, URR for the dynamic rule and predefined rules.

  This support is only applicable for the default bearer in the N4 Establishment Request towards the UPF.

  This functionality also supports the sending of rulebase PDR, Default Qos, APN-AMBR values to the UPF.

- **Detach Support (N4 Session Deletion Request)**:

SMF supports sending the N4 session deletion request as part of the detach procedure.

Subscription-ID as Part of CCR towards PCRF

The following CLI controls the Subscription ID value for the CCR messages from SMF to PCRF. The default value is none.

Configuration option is available in the access profile as follows.

```
config
  profile network-element   network_element_name
    subscription-id id_number
    description id_description
      possible completions { e164 | imsi | nai }
      end
```

Online and Offline AVP

The online and offline AVP value that is sent to PCRF in the CCR – Initial Request message is controlled in the following ways:

- **Online AVP to be sent in CCR-I to PCRF**: When the network-profile-element OCS is configured and if any one of the configured rulebase's static rules charging action contains `cca charging-credit` CLI, then the online AVP to PCRF is sent as ENABLE_ONLINE, else it is sent as DISABLE_ONLINE.
- **Offline AVP to be sent in CCR-I to PCRF**: When the network-profile-element OFCS is configured and the configured rulebase has `billing-action egcdr` CLI configured, then the offline AVP to PCRF is sent as ENABLE_OFFLINE, else it is sent as DISABLE_OFFLINE.

Predefined Group-of-Ruledef installation through Charging-Rule-Name AVP

This feature supports the installation of the predefined group-of-ruledef using the charging-rule-name installation from PCRF. This is a default feature and requires no configuration.

Gy Interface

The Gy interface is the Online Charging interface between the SMF Charging Trigger Function (CTF) and the Online Charging System (OCS) Charging-Data-Function (CDF). This interface is based on the 3GPP standards and relies on quota allocation. The OCS is the Diameter Credit Control server, which provides the online Charging data to the SMF. With the Gy interface, customer traffic is gated and billed in an online or prepaid style. SMF supports both the time-based and volume-based charging models.

Gy Usage Reporting

Feature Description

P-GW User Plane sends the usage report for various triggers. For example, volume, time quota, threshold, validity time, quota hold time, Start of Traffic (SoT), and so on. Otherwise, the SMF sends the query usage report after detecting a charging condition event or the removal of a Usage Reporting Rule (URR) as part of PCC Rule removal at SMF.

After receiving the usage report, the Control Plane maps the URRs to the corresponding Charging Multiple-Service Credit Control (MSCC). Then, the Control Plane initiates the Credit Control Update request

for the respective MSCCs. A usage report is either synchronous or asynchronous. SMF receives the synchronous usage report through the N4 Modification Response or the N4 Deletion Response message. SMF receives the asynchronous usage report through the N4 Session Report Request message.

How it Works

The usage report on the Gy interface includes the following usage report procedures:

- Start of Traffic (SoT) when Credit Control Request - Initial (CCR-I) request is not sent during the initial attach or bearer creation.
- SoT when CCR-I is sent without quota request during initial attach or bearer creation.
- SoT for predefined and static rules.
- N4 Modify Response for Query URR.
- N4 Session Report Request.
- N4 Modify Response for removal of URR.
- N4 Delete Session Response.

Call Flows

Usage Report with SoT – CCR-I Message Not Sent During Initial Attach or Bearer Creation

This section provides details about the usage report with SoT when the CCR-I message is not sent during the initial attach or bearer creation.

Figure 129: Usage Report with SoT – CCR-I Message Not Sent During Initial Attach or Bearer Creation

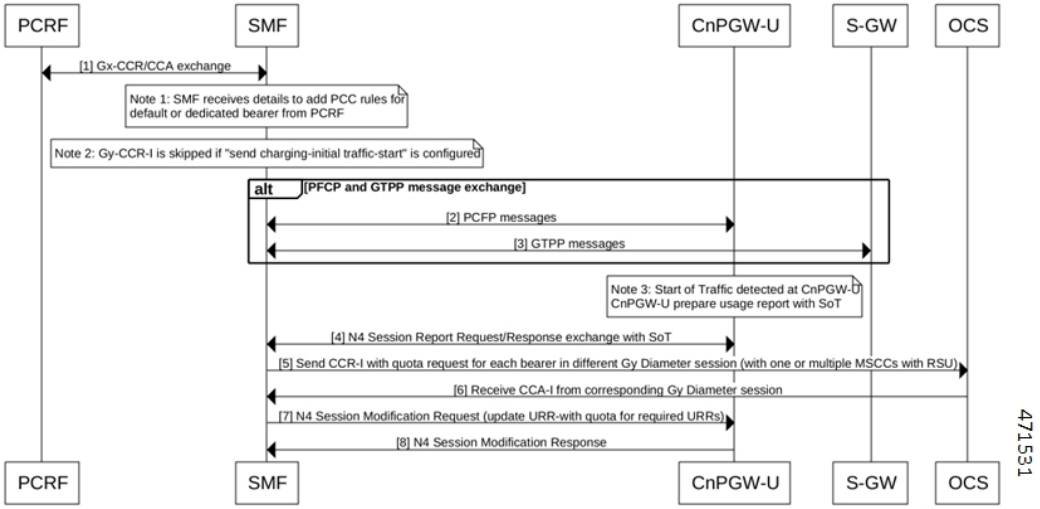


Table 204: Usage Report with SoT – CCR-I Message Not Sent During Initial Attach or Bearer Creation Call Flow Description

Step	Description
1	Both the PCRF and SMF send and receive the Gx Credit Control Request (CCR) and Credit Control Answer (CCA) messages to each other. **Note** • The SMF receives the details to add PCC rules for the default or dedicated bearer from PCRF. • If you have configured the send charging-initial traffic-start value, then the PCRF doesn't send the Gy Credit Control Request-Initial (CCR-I) message to SMF.
2 and 3	The PFCP and GTPP message exchange happens. The SMF sends the PCFP messages to CnPGW-U and GTPP messages to S-GW. **Note** In case of traffic detection at CnPGW-U, the CnPGW-U prepares the usage report with the SoT.
4	The CnPGW-U F sends the N4 Session Report Request to SMF with the SoT details. The SMF sends the N4 Session Report Response to CnPGW-U.
5	The SMF sends the CCR-I message with quota request for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs with Requested-Service-Unit (RSU) AVPs, which is one for each Rating Group and service ID.
6	The OCS sends the CCA-I message from the corresponding Gy Diameter session to SMF. The Diameter session includes details, such as quota and triggers for each Rating Group and Service ID.
7	The SMF sends the N4 Session Modification Request to CnPGW-U. This request includes details on the required URRs with quota.
8	The CnPGW-U sends the N4 Session Modification Response to SMF.

Usage Report with SoT – CCR-I Sent Without Quota Request During Initial Attach or Bearer Creation

This section provides details about the usage report with SoT where the CCR-I message is sent without the quota request during the initial attach or bearer creation.

Figure 130: Usage-Report with SoT – CCR-I Sent Without Quota Request During Initial Attach or Bearer Creation

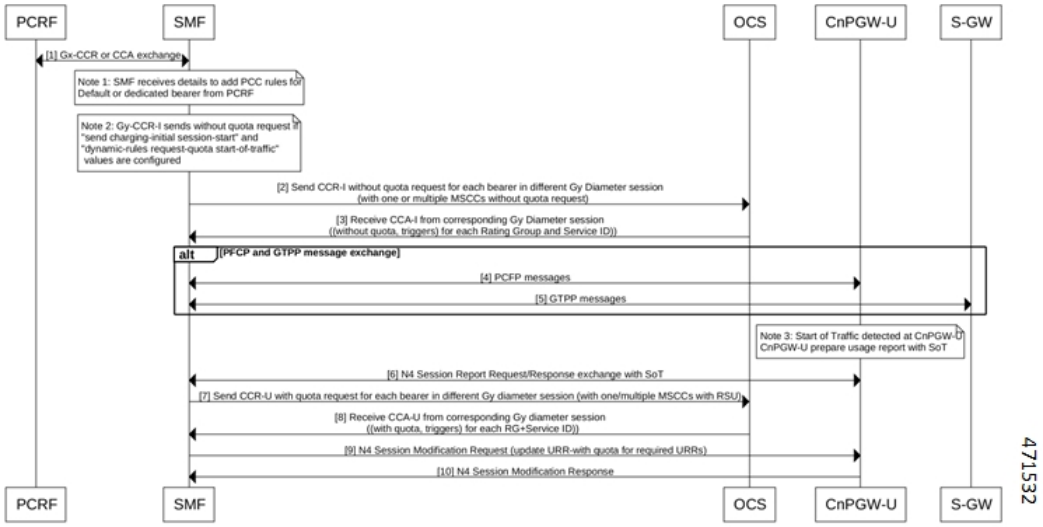


Table 205: Usage-Report with SoT – CCR-I Sent Without Quota Request During Initial Attach or Bearer Creation Call Flow Description

Step	Description
1	Both PCRF and SMF exchange the Gx Credit Control Request (CCR) and Credit Control Answer (CCA) messages from each other. **Note** • The SMF receives the details to add PCC rules for the default or dedicated bearer from PCRF. • If you have configured the **send charging-initial session-start** and **dynamic rules request-quota start-of-traffic** values, then the PCRF sends the Gy CCR-I message without quota request to SMF.
2	SMF sends the CCR-I without quota request for each bearer in various Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs without quota request, which is one for each Rating Group and service ID.
3	OCS sends the CCA-I message from the corresponding Gy Diameter session to SMF. The Diameter session is without quota and triggers.
4 and 5	The PFCP and GTPP message exchange happens. **Note** In case of traffic detection at CnPGW-U, the CnPGW-U prepares the usage report with the SoT.
6	The CnPGW-U sends the N4 Session Report Request to SMF with the SoT details. The SMF sends the N4 Session Report Response to CnPGW-U.
7	SMF sends the CCR-I message with quota request for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs with Requested-Service-Unit (RSU) AVPs.

Step	Description
8	OCS sends the Credit Control Request - Update (CCA-U) message from the corresponding Gy Diameter session to SMF. The Diameter session includes details, such as quota and triggers for each Rating Group and Service ID.
9	SMF sends the N4 Session Modification Request to CnPGW-U. This request includes details on the required URRs with quota.
10	The CnPGW-U sends the N4 Session Modification Response to SMF.

Usage Report with SoT for Predefined and Static Rules

This section provides information on the usage report with SoT for the predefined and the static rules.

Figure 131: Usage Report with SoT for Predefined and Static Rules

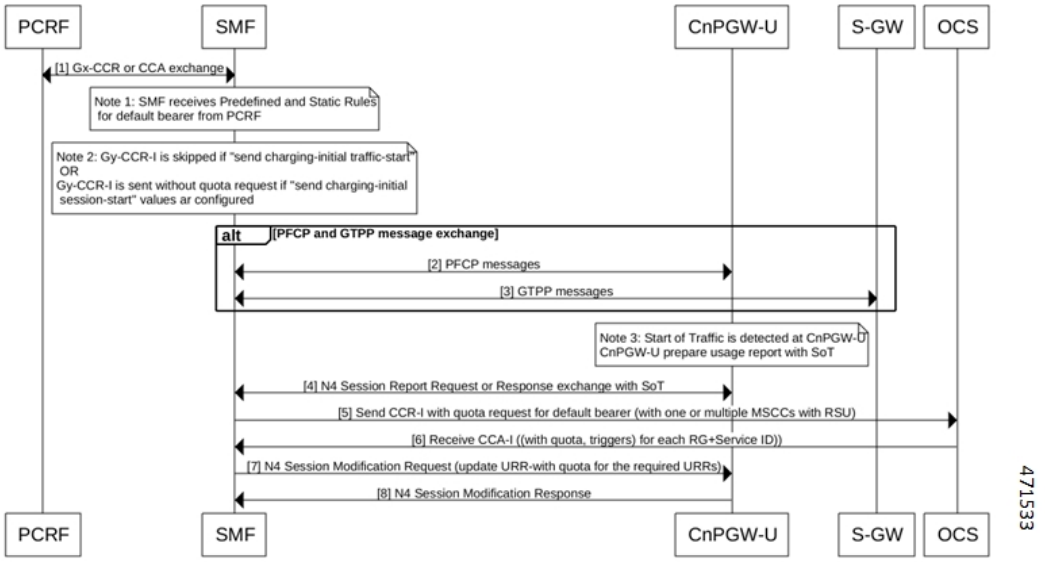


Table 206: Usage Report with SoT for Predefined and Static Rules Call Flow Description

Step	Description
1	Both PCRF and SMF exchange the Gx CCR and CCA messages from each other. **Note** The SMF receives the predefined and static rules for the default bearer from PCRF.
2 and 3	The PFCP and GTPP message exchange happens. The SMF sends the PFCP messages to CnPGW-U and GTPP message to S-GW. **Note** In case of traffic detection at CnPGW-U, the CnPGW-U prepares the usage report with the SoT.
4	The CnPGW-U sends the N4 Session Report Request to SMF with the SoT details. The SMF sends the N4 Session Report Response to CnPGW-U.

Step	Description
5	SMF sends the CCR-I message with quota request for default bearer in Gy Diameter session to OCS. This session can have one or multiple MSCCs with Requested-Service-Unit (RSU) AVP, which is one for each Rating Group and service ID.
6	OCS sends the CCA-I message in the Gy Diameter session to SMF. The Diameter session includes details, such as quota and triggers for each Rating Group and Service ID.
7	SMF sends the N4 Session Modification Request to CnPGW-U. This request includes details on the required URRs with quota.
8	The CnPGW-U sends the N4 Session Modification Response to SMF.

Usage Report in N4 Modify Response (Query URR Scenario)

This section provides details on the usage report in the N4 Modify Response, for the trigger event, in the Query URR scenario.

Figure 132: Usage Report in N4 Modify Response (Query URR Scenario)

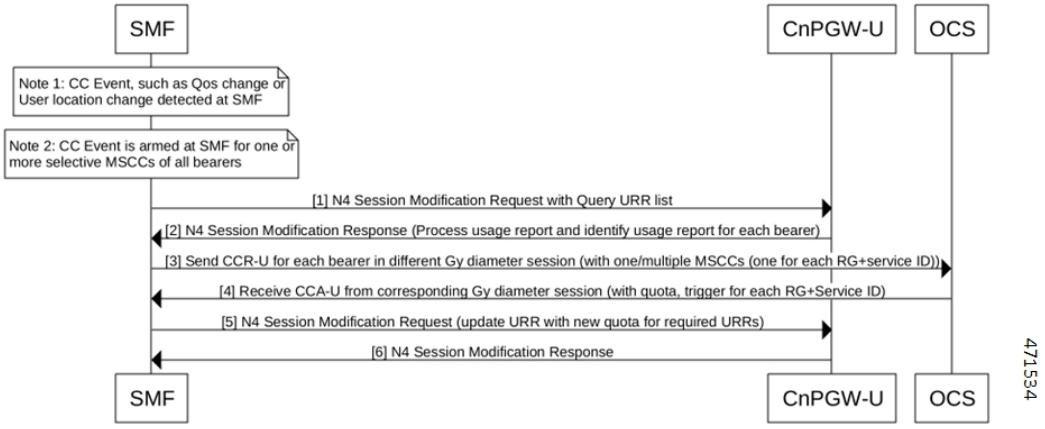


Table 207: Usage Report in N4 Modify Response (Query URR Scenario) Call Flow Description

Step	Description
1	The SMF detects a Charging condition event and is armed for one or more specific MSCCs of all the bearers. Then, SMF creates a list of Query URR for the bearers that are armed. After the creation of this list, the SMF sends the N4 Session Modification Request with the Query URR list to the CnPGW-U.
2	The CnPGW-U sends the N4 Session Modification Response to SMF with the usage report. SMF processes and identifies the usage report for each bearer.
3	The SMF sends the CCR-U message for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs, which is one for each Rating Group and service ID.

Step	Description
4	The OCS sends the CCA-U message from the corresponding Gy Diameter session to SMF. The Diameter session includes details, such as quota and triggers for each Rating Group and Service ID.
5	The SMF sends the N4 Session Modification Request to CnPGW-U. This request includes details on the required URRs with quota.
6	The CnPGW-U sends the N4 Session Modification Response to SMF.

N4 Session Report

This section provides details on the N4 Session Report.

Figure 133: N4 Session Report

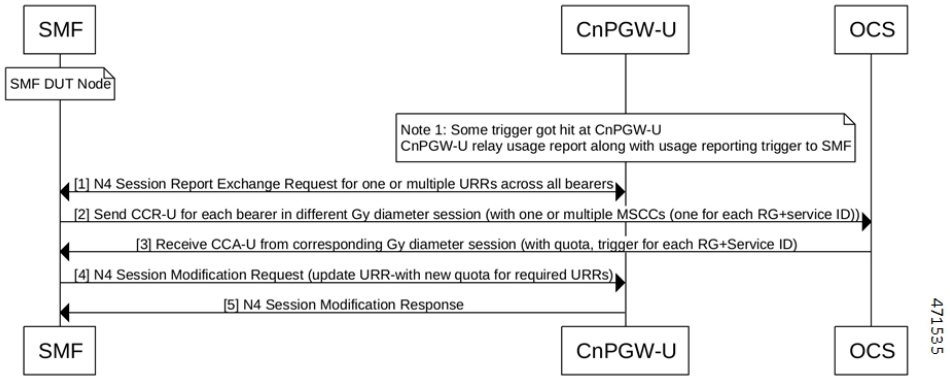


Table 208: N4 Session Report Call Flow Description

Step	Description
1	A Device Under Test (DUT) node exists on SMF. **Note** The CnPGW-U contains various URRs with values, such as threshold, quota, and triggers. Some triggers hit at CnPGW-U for a specific URR. The CnPGW-U sends the usage report along with usage reporting trigger to SMF. CnPGw-U sends the N4 Session Report to SMF for one or multiple URRs across bearers.
2	The SMF sends the CCR-U message for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs, which is one for each Rating Group and service ID.
3	The OCS sends the CCA-U message from the corresponding Gy Diameter session to SMF. The Diameter session includes details, such as quota and triggers for each Rating Group and Service ID.
4	The SMF sends the N4 Session Modification Request to CnPGW-U. This request includes details on the required URRs with new quota.
5	The CnPGW-U sends the N4 Session Modification Response to SMF.

Usage Report in N4 Modify Response (Remove URR Scenario)

This section provides details on the usage report in the N4 Modify Response for the remove URR scenario.

Figure 134: Usage Report in N4 Modify Response (Remove URR Scenario)

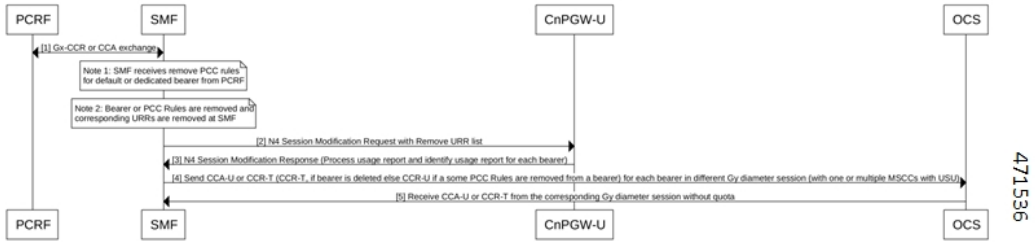


Table 209: Usage Report in N4 Modify Response (Remove URR Scenario) Call Flow Description

Step	Description
1	Both the PCRF and SMF exchange the Gx CCR and CCA messages. **Note** • The SMF receives the N4 Session Modification Request with Remove URR list from PCRF. • The SMF removes the Bearer or PCC Rules and the corresponding URRs.
2	The SMF sends the N4 Session Modification Request with Remove URR list to CnPGW-U.
3	The CnPGW-U sends the N4 Session Modification Response to SMF. SMF processes and identifies the usage report for each bearer.
4	If the SMF removes one or multiple PCC Rules from a bearer, the SMF sends the CCA-U or Credit Control Answer - Terminate (CCR-T) message for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs with Used Service Unit (USU).
5	The OCS sends the CCA-U or CCA-T message from the corresponding Gy Diameter session without quota to SMF.

Usage Report in N4 Delete Session Response

This section provides information on the usage report in N4 Delete Session Response.

Figure 135: Usage Report in N4 Delete Session

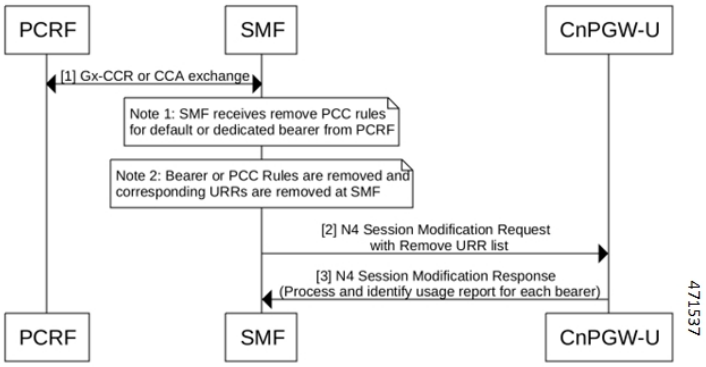


Table 210: Usage Report in N4 Delete Session Call Flow Description

Step	Description
1	**Note** The SMF detects the UE or Network-initiated Delete session. The SMF sends the N4 Delete Session Request to to CnPGW-U to delete the session. The CnPGW-U sends the usage report in the N4 Delete Session Response to SMF.
2	The SMF sends the CCR-T message for each bearer in different Gy Diameter sessions to OCS. These sessions can have one or multiple MSCCs with USU.
3	The OCS sends the CCA-T message from the corresponding Gy Diameter session to SMF.

Gy Failure Handling

Feature Description

A Diameter Failure Handling Template is associated to different Diameter services. A Diameter endpoint pod receives a command-level failure for a Gy message from OCS. Then, the Diameter endpoint pod handles the failure handling configuration.

Supported Actions and Sub-actions

The following table lists the supported failure handling template actions and sub-actions for the Gy interface:

Table 211: Supported Failure Handling Template Actions and Sub-actions

Action	Sub-action
Continue	• FHSubActionEnum_UNKNOWN • FHSubActionEnum_DISCARD_TRAFFIC
Terminate	• FHSubActionEnum_WITH_TERM_REQUEST • FHSubActionEnum_WITHOUT_TERM_REQUEST

Use Cases

Charging Behavior for Failure Handling Template Actions

Following table lists the charging behavior for failure handling template actions:

Table 212: Charging Behavior for Failure Handling Template Actions

Procedure	Failure Handling Template (Actions and Sub-actions)	SMF Behavior
CCR-I (PDN Setup)	Continue + Unknown/None	Disable Charging No URR created. No Gy CCR-T is available during detach procedure. No Gy CCR-U during any trigger or update. Gy Offline charging “Enabled under “Charging-params” (Only for default bearer)
	Continue + Discard	Drop Forwarding Action Rules (FAR) Send URR with drop FAR ID. No Gy CCR-T is available during detach procedure. No Gy CCR-U during any trigger or update. Gy Offline charging “Enabled under “Charging-params” (Only for default bearer)
	Terminate + without term	Terminate the session without Gy CCR-T message
	Terminate + with term	Terminate the session with Gy CCR-T message

Procedure	Failure Handling Template (Actions and Sub-actions)	SMF Behavior
CCR-I (Start of Traffic)	Continue + Unknown/None	**Known URR:** Allocate high quota No Gy CCR-T during detach. No Gy CCR-U during any trigger or update. GyOffline charging “Enabled under “Charging-params” (Only for default bearer) **Unknown URR:** Disable OCS charging No URR created. No Gy CCR-T during detach. No Gy CCR-U during any trigger or update. GyOffline charging “Enabled under “Charging-params” (Only for default bearer)
	Continue + Discard	Drop FAR Send URR with drop FAR ID No Gy CCR-T during detach. No Gy CCR-U during any trigger or update. GyOffline charging “Enabled under “Charging-params” (Only for default bearer)
	Terminate + without term	Terminate the session without Gy CCR-T message
	Terminate + with term	Terminate the session with Gy CCR-T message

Procedure	Failure Handling Template (Actions and Sub-actions)	SMF Behavior
MBR Procedure: **Scenario:** N4 Modification (Query URR) Gy CCR-U (Usage) Gy CCA-U (failure)	Continue + None	Allocate high quota Sent CCR-T in dettach Gy Offline charging "Enabled" in "Charging-params" (Only for default ebarer)
	Continue + Discard	Drop FAR Link created URR to Drop FAR. Sent CCR-T in detach GyOffline charging is "Enabled" in "Charging-params" (Only for default bearer)
	Terminate + without term	If default bearer, then terminate the session without Gy CCR-T.
	Terminate + with term	If default bearer, then terminate the session with Gy CCR-T.
Default Bearer Procedure (UBR): **Scenario:** UBR (QoS change) N4 Modification Gy CCR-U Gy CCA-U fails	Continue + None	Allocate high quota Sent CCR-T in detach GyOffline charging “Enabled under “Charging-params” (Only for default bearer)
	Continue + Discard	Drop FAR Link created URR to drop FAR. Sent CCR-T in detach GyOffline charging “Enabled under “Charging-params” (Only for default bearer)
	Terminate + without term	If default bearer, then terminate the session without Gy CCR-T.
	Terminate + with term	If default bearer, then terminate the session with CCR-T.

Procedure	Failure Handling Template (Actions and Sub-actions)	SMF Behavior
Usage Report for Default bearer: Scenario: Session Report (for default bearer URR) Gy CCR-U Gy CCA-U (Fails)	Continue + None	Allocate high quota Sent CCR-T in detach Gy Offline charging “Enabled under “Charging-params” (Only for default bearer)
	Continue + Discard	Drop FAR Link created URR to drop FAR Sent CCR-T in detach GyOffline charging “Enabled under “Charging-params” (Only for default bearer)
	Terminate + without term	If default bearer, then terminate the session without Gy CCR-T.
	Terminate + with term	If default bearer, then terminate the session with Gy CCR-T.

BGIPC Failure

The Gy interface considers the BGIPC time-out and failure handling template. This behavior applies to the Gx interface too.

Charging Behavior for Non-Gy Failures

Following table lists the charging behavior for non-Gy failures:

Table 213: Charging Behavior for Non-Gy Failures

Step	Procedure	Failure
1	PDN Setup	N4 failure
2	PDN Modify (MBR)	
2.1	**Flow:** • N4 Modification Request (Query URR) N4 Modification Response (Usage): • Gy CCR-U (usage and trigger) • Gy CCA-U (quota) N4 Modification (quota) • Gx CCR-U	First N4 (for query URR) fail

Step	Procedure	Failure
2.2		Second N4 after CCA-U (with q
3	Access Failure	UBR

Diameter Session Failover

Feature Description

This section describes about the SMF behaviour upon handling 4G session failure over Diameter interfaces.

How it Works

The following capabilities are added as part of this feature:

- The SMF processes the CC-Session-Failover AVP received in the CCA-I and CCA-U from OCS.
- The SMF overrides and stores the latest AVP information in the Diameter session on receiving the CC-Session-Failover AVP.
- Based on the configuration and the CC-Session-Failover AVP information, the SMF service sends a session-failover flag indication in the next subsequent request of CCR-U or CCR-T to the Diameter endpoint.
- If the session-failover CLI is enabled and OCS sends the CC-session-failover AVP, SMF retries the request to the secondary server if provisioned under the failure handling template.
- The failover gets overridden by the server in the response message, and it takes precedence over the SMF service indication flag.

Configuring Session Failover

Use the following command to configure Session failover.

```
config
  profile charging charging_profile_name
     [ default | no ] session failover
     exit
```

NOTES:

- **profile charging** *charging_profile_name*: Specify the charging profile name. *charging_profile_name* must be an alphanumeric string.
- **default session failover**: Configures this command with default setting.

Note Default setting depends on the failure-handling configuration.

- **no session failover**: If the primary server isn't reachable, failover isn't triggered and the session is torn down. Failover action isn't taken.
- **session failover**: SMF retries the request to the secondary server if provisioned under the failure handling template.

Configuration Verification

Use the following command to verify if the Session failover handling profile is configured.

```
smf# show running-config profile charging chp
profile charging chp
  session failover
exit
```

Diameter Credit Control Failure Handling

Table 214: Feature History

Feature Name	Release Information	Description
Use of Credit-Control-Failure-Handling AVP for Gy request failure handling	2023.04	The SMF uses the value of Credit-Control-Failure-Handling AVP to derive the Gy request failure handling behavior when the requests are prevented due to a network problem.

Feature Description

As part of charging, the message exchange happens between the SMF service pod and the Diameter endpoint. To define the failure handling behaviour, the Online Charging Server (OCS) sends the Credit-Control-Failure-Handling Attribute Value Pair (AVP) to the Diameter endpoint. The Diameter endpoint forwards the received Gy Credit Control Answer - Initial (CCA-I) or Gy Credit Control Answer - Update (CCA-U) message along with the Credit-Control-Failure-Handling AVP. The SMF service pod stores this AVP from CCA-I or CCA-U OCS response messages and includes the Credit-Control-Failure-Handling AVP in the subsequent Credit Control Response - Update (CCR-U) messages. Then, the Diameter endpoint uses this AVP value to derive the Gy failure handling behavior when no is response received from the OCS or the command level failure result codes are received.

The SMF overrides the existing AVP value and stores the latest value in the charging subscriber data per Diameter session. The SMF service includes the stored value of the Credit-Control-Failure-Handling AVP in the subsequent Credit Control Request Update message. After receiving this message, the Diameter endpoint extracts the value of this AVP and sends it to OCS.

Note The Diameter Credit Control Failure Handling takes precedence over the Diameter session failover and applies the action and subaction based on the received value of the Credit-Control-Failure-Handling AVP.

How it Works

The Diameter endpoint sends the following values of the Credit-Control-Failure-Handling AVP in the CCR-U message to SMF:

- Terminate—Diameter endpoint sends the action as terminate and the subaction as without-termination to the SMF service pod.
- Continue—Diameter endpoint sends the action as continue and the subaction as none to the SMF service pod.

- Retry-AND-Terminate—Diameter endpoint sends the action as retry until it receives a successful message or until the retry count gets exhausted. After the retry count exhaustion, the Diameter endpoint sends the action as terminate and the subaction as without-termination to the SMF service pod.

Note The Retry count value is derived from the failure handling template.

The following table is an example that lists the Credit-Control-Failure-Handling AVP value that OCS sends to the SMF service. The SMF service stores the received value for the subsequent CCR-U message.

Table 215: Credit-Control-Failure-Handling AVP Values from OCS to SMF

	OCS AVP Value in Previous CCA-I or CCA-U Messages	Smf-service Indication to Diameter Endpoint in CCR-U Message
1	CreditControl FailureHandling AVP (Terminate)	CreditControl FailureHandling AVP (Terminate)
2	CreditControl FailureHandling AVP (Continue)	CreditControl FailureHandling AVP (Continue)
3	CreditControl FailureHandling AVP (Retry-AND-Terminate)	CreditControl FailureHandling AVP (Retry-AND -Terminate)

Gy MSCC Level Failure Result Codes

Feature Description

This section describes about the SMF behaviour upon receiving “failure result codes received at MSCC level” for Transient Failures (4xxx) and Permanent Failures (5xxx) result codes.

Table 216: Transient Failures (4xxx)

Result Code	Description
4010	DIAMETER_END_USER_SERVICE_DENIED
4011	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE
4012	DIAMETER_CREDIT_LIMIT_REACHED

Table 217: Permanent Failures (5xxx)

Result Code	Description
5003	DIAMETER_AUTHORIZATION_REJECTED
5012	DIAMETER_UNABLE_TO_COMPLY

Result Code	Description
5030	DIAMETER_USER_UNKNOWN
5031	DIAMETER_RATING_FAILED

How it Works

The following table explains about the various SMF transient and permanent failure result codes:

Failure Codes	Description
SMF receives all the permanent failure result codes and transient failure result codes 4010 and 4012 in CCAI.	SMF sends zero time and volume quota in PFCP_SESSION_ESTABLISHMENT_REQUEST
SMF receives all the permanent failure result codes and transient failure result codes 4010 and 4012 in CCAU	SMF sends zero time and volume quota in PFCP_SESSION_MODIFICATION_REQUEST
SMF receives transient failure result code as 4011 in CCAI	SMF sends high (MAX) time and volume quota in PFCP_SESSION_ESTABLISHMENT_REQUEST
SMF receives transient failure result code as 4011 in CCAU	SMF sends high (MAX) time and volume quota in PFCP_SESSION_ESTABLISHMENT_REQUEST
SMF receives transient failure result code as 4011 in CCAU	SMF high (MAX) time and volume quota in PFCP_SESSION_MODIFICATION_REQUEST
SMF receives usage report with "**termr**" trigger in PFCP_SESSION_DELETION_RESPONSE message then	• SMF sends CCRT message with 3GPP-reporting reason as "FINAL" for the URRs which has received MSCC failure code as 4010 and 4012 • SMF sends CCRT message without MSCC for the URRs which has received MSCC failure code as 4011 • SMF sends CCRT message with USU(time(0) + volume(0)) and 3GPP-reporting reason as "FINAL" for the URRs which has received all the permanent failure result codes

SMF receives all the permanent failure result codes and transient failure result codes 4010 and 4012 in CCAI:

- SMF sends zero time and volume quota in PFCP_SESSION_ESTABLISHMENT_REQUEST: SMF receives all the permanent failure result codes and transient failure result codes 4010 and 4012 in CCAU.
- SMF sends zero time and volume quota in PFCP_SESSION_MODIFICATION_REQUEST: SMF receives transient failure result code as 4011 in CCAI.
- SMF sends high (MAX) time and volume quota in PFCP_SESSION_ESTABLISHMENT_REQUEST: SMF receives transient failure result code as 4011 in CCAU.

Architecture

This section describes about capturing the details related to processing of Multiple-Services-Credit-Control (MSCC) failure result codes at MSCC level in the Credit Control Application (CCA) messages received from Gy interface. This feature enables the SMF to process the Transient Failures (4xxx) and Permanent Failures(5xxx) at MSCC level from Gy interface in **CCAI** and **CCAU** messages.

Result Codes

The following table includes the various result codes and behaviour for Transient Failures (4xxx) and Permanent Failures (5xxx) result codes:

Table 218: Result Codes

Result Code	Behaviour
4010/4012 (CCAI)	1. **CCAI** received with **4010/4012** 2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** with APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0
4010/4012 (CCAU)	1. **CCAU** received with **4010/4012** 2. **PFCP_SESSION_MODIFICATION_REQUEST** goes with **UPDATE FAR** with APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0
4010/4012 (CCRT)	1. **PFCP_SESSION_DELETION_REQUEST received with** usage report with **timqu** trigger 2. **CCRT** should go with3GPP-Reporting reason as “FINAL”

Result Code	Behaviour
4011 (CCAI)	1. **CCAI** received with **4011** 2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10
4011 (CCAU)	1. **CCAU** received with **4011** 2. **PFCP_SESSION_MODIFICATION_REQUEST** should go with **UPDATE FAR** APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10
4011 (CCRT)	1. **PFCP_SESSION_DELETION_REQUEST received with** usage report with **timqu** trigger 2. **CCRT** goes without MSCC
5003/5012/5030/5031 (CCAI)	1. **CCAI** received with **5003/5012/5030/5031** 2. **PFCP_SESSION_ESTABLISHMENT_REQUEST** goes with **CREATE FAR** with APPLY ACTION as DROP:1, **CREATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0

Result Code	Behaviour
5003/5012/5030/5031 (CCAU)	1. **CCAU** received with **5003/5012/5030/5031** 2. **PFCP_SESSION_MODIFICATION_REQUEST** goes with **UPDATE FAR** with APPLY ACTION as DROP:1, **UPDATE URR** with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0
5003/5012/5030/5031 (CCRT)	1. **PFCP_SESSION_DELETION_REQUEST received with** usage report with **timqu** trigger 2. **CCRT** goes with USU(time(0)+volume(0)) and 3GPP-Reporting-Reason as “FINAL”

Note Once SMF receives any supported failure codes for the URRS. No operations are performed on the URRs based on local trigger configuration or triggers received from OCS.

Gy Quota Validity Time (QVT) and Quota Holding Time (QHT)

Feature Description

The following capabilities are added to the SMF as a part of this feature:

- The SMF is capable to receive **Quota Validity time** from Gy interface in **CCAI** and **CCAU** messages. After processing, SMF sends this information towards UPF in the following messages **PFCP_SESSION_ESTABLISHMENT_REQUEST and PFCP_SESSION_MODIFICATION_REQUEST** with trigger as “**timqu**”.

  If PFCP_SESSION_REPORT_REQUEST message receives usage report with “**timqu**” trigger, The SMF sends **CCRU** message with USU with time quota information and adds TGPPReportingReason as “**VALIDITY_TIME**”.

- The SMF is capable to receive **Quota Holding time** from Gy interface in **CCAI** and **CCAU** messages. After processing SMF sends this information towads UPF in the following messages **PFCP_SESSION_ESTABLISHMENT_REQUEST and PFCP_SESSION_MODIFICATION_REQUEST** with trigger as “**quhti**”.

  ```
  PFCP_SESSION_ESTABLISHMENT_REQUEST PFCP_SESSION_MODIFICATION_REQUEST
  ```

  If **PFCP_SESSION_REPORT_REQUEST** message receives usage report with “**quhti**” trigger. The SMF sends **CCRU** message with USU with time quota information and adds TGPPReportingReason as “**QHT**”.

Quota-Validity-Time

This is an optional AVP and may only occur in a CCA command. It is contained in the Multiple-Services-Credit-Control AVP. This field defines the time in order to limit the validity of the granted quota for a given category instance.

The following requirements are supported by SMF:

- "**Validity-Time**" received in Gy CCAI/CCAU messages establishment or modification
- The SMF process received validity time, if it is eligible to send the information towards UPF

  SMF Sends validity time as "**tm_quta**" in PFCP_IE_TIME_QUOTA and set the trigger as **timqu** with in PFCP_IE_REPORTING_TRIGGERS in: `PFCP_SESSION_ESTABLISHMENT_REQUEST and PFCP_SESSION_MODIFICATION_REQUEST`
- SMF can receive PFCP_IE_USAGE_REPORT_REP_REQ with **timqu** as trigger and duration in "**durton_msrt**" in PFCP_SESSION_REPORT_REQUEST message
- SMF process usage report sends received "**durton_msrt**" as "**CC-Time**" inside Used-Service-Unit and **3GPP-Reporting-Reason** added as VALIDITY_TIME with in Multiple-Services-Credit-Control AVP in CCRU.
- If SMF received "**volume_msrmt**" along with "**durton_msrt**", then "**CC-Total-Octets**", "**CC-Input-Octets**", "**CC-Output-Octets**" filled along with "**CC-Time**" inside Used-Service-Unit and **3GPP-Reporting-Reason** added as VALIDITY_TIME with in Multiple-Services-Credit-Control AVP in CCRU.
- If cnPGW not "**Validity-Time**" receives in Gy CCAI/CCAU messages then it read from charging profile configuration and apply it.

Quota-Holding-Time

This is an optional AVP and may only occur in a CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.

The following requirements are supported by the SMF:

- "**3GPP-Quota-Holding-Time**" received in Gy CCAI/CCAU messages establishment or modification
- SMF Sends holding time as "**quta_hldg_tm**" in PFCP_IE_QUOTA_HOLDING_TIME and set the trigger as **quhti** with in PFCP_IE_REPORTING_TRIGGERS in PFCP_SESSION_ESTABLISHMENT_REQUEST and PFCP_SESSION_MODIFICATION_REQUEST
- SMF can receive PFCP_IE_USAGE_REPORT_REP_REQ with **quhti** as trigger
- SMF process usage report **3GPP-Reporting-Reason** added as QHT with in Multiple-Services-Credit-Control AVP in CCRU.

Volume-Quota-Threshold

This is an optional AVP and may only occur in a CCA command. It is contained in the Multiple-Services-Credit-Control AVP. If cnPGW and not the "3GPP-Volume-Quota-Threshold" is received in the Gy CCAI/CCAU messages, then it reads the information from the charging profile configuration and applies it.

How it Works

The SMF sends the quota validity time towards the N4 in “tm_quta” in PFCP_IE_TIME_QUOTA IE. If SMF receives only Quota validity time from CCAI/CCAU or both cc-Time and validity-time are received and validity time is less. If both values are equal then SMF sends cc-Time value in tm_quta. The SMF does not forward the 3GPP-Time-Quota-Threshold to N4, if quota validity time is selected.

If received quota holding time is valid, the SMF sends the quota holding time towards the N4.

Note

- **Zero Validity Time**:

  In SMF validity time or holding time values are forwarded to N4, if validity time or holding time values received from CCRI/CCRU are 0. The SMF relays 0 because honouring 0 is mechanism to disable armed timer at UPF. QVT and QHT implementation is aligned with SMF if validity time or holding time values are received from CCRI/CCRU are 0.

- **QHT trigger received**:

  In SMF, volume_msrmt, duration_msrmt are recived along with quhti trigger, CCRU sends volume_msrmt, duration_msrmt inside USU and updates reporting reason as QHT in MSCC level and also sends “Requested-Service-Unit”. QHT implementation is aligned with SMF if volume_msrmt, duration_msrmt are recived along with quhti trigger.

Logging

Following debug logs are present in various scenarios if validity time is received from the Gy interface:

- Only validity-Time received:

  “**Validity Time present, not time quota**”

- Validity-Time and cc-Time received:

  “**Time Quota is smaller than validity Time**”

  “**Time Quota is Greater than validity Time**”

  “**Time Quota is equal to validity Time**”

Gy Tarrif Time Support

Feature Description

The Tarrif switch time functionality applies when a subscriber switches form one tarrif plan to another. The Tariff-Time-Change AVP is used to determine the tariff switch time, and the Monitoring-Time IE is used to support the Tarrif Time support functionality.

After a tariff timer expiry, the gateway accumulates the usage separately in a charging bucket and continues to consume from the original quota value. At the time of next reporting, (Quota exhausted or another control events) the gateway reports both usages (before and after tarrif time change) for the same charging bucket.

How it Works

The SMF processes the Tariff-Time-Change AVP in Granted-Service-Unit (GSU) level from Gy interface in CCAI and CCAU messages. The SMF includes the Tariff-Change-Usage AVP inside Used-Service-Unit (USU) in CCRU and CCRT messages when the usage report is received from UPF.

Following scenarios are supported:

- Tariff-Time-Change with Quota-Holding-Time Expired Trigger
- Tariff-Time-Change with Validity-Time Expired Trigger
- Tariff-Time-Change with Volume/Time-Quota Exhausted Trigger
- Tariff-Time-Change with Volume/Time-Quota-Threshold Trigger
- Tariff-Time-Change with Immediate Reporting Trigger
- Tariff-Time-Change with Terminate Reporting Trigger

The following capabilities are added to the SMF as part of this feature:

- The OCS provides "Tariff-Time-Change" AVP in CCAI/CCAU messages. After processing, SMF sends this information towards the UPF in PFCP Session Establishment Request and PFCP Session Modification Request using PFCP_IE_MONITORING_TIME IE.
- The SMF receives two usage reports for each URR:
  - one with “Usage Report Trigger” as 'MONIT' and “ PFCP_IE_USAGE_INFORMATION” as ‘bef’ with "PFCP_IE_VOLUME_MEASUREMENT" and "PFCP_IE_DURATION_MEASUREMENT".
  - other usage report with “Usage Report Trigger” as 'TIMQU' and “ PFCP_IE_USAGE_INFORMATION” as ‘aft’ with "PFCP_IE_VOLUME_MEASUREMENT" and "PFCP_IE_DURATION_MEASUREMENT".
- The SMF uses different USU to forward both the usage reports within MSCC towards OCS in CCRU/CCRT messages.

  .
  - first usage report, one with "MONIT" trigger is forwarded in USU1 with "Tariff-Change-Usage: UNIT_BEFORE_TARIFF_CHANGE" and
  - second usage report, one with "TIMQU" tigger is forwarded in USU2 with "Tariff-Change-Usage: UNIT_AFTER_TARIFF_CHANGE ".

Origin Host and Origin Realm for Gy

For each subscriber, SMF maintains a record of the Origin-Realm and Origin-Host attribute information sent by OCS through Diameter messages. If there’s any value change to the Origin-Host and Origin-Realm attributes, SMF updates the latest value and interacts with the corresponding destination host. Later, SMF increments the ocs_dest_host_change_stats statistics for every change in the attribute value.

Pending Traffic Treatment over Diameter Interfaces

The SMF implements the 3GPP recommendations for interworking of Evolved Packet System (EPS) and Diameter Interfaces such as Gy for Online Charging System (OCS) for prepaid subscribers, where it supports pending traffic management during the quota refresh procedure.

Pending Traffic Treatment (PTT) allows pass or drop treatment of traffic that flows at the User Plane Function (UPF) while waiting for Quota Information from P-GW. The traffic is treated based on the following supported configurations under the credit-control group in the Active Charging Service in UPF:

- pending-traffic-treatment noquota pass
- pending-traffic-treatment noquota drop
- pending-traffic-treatment noquota limited-pass volume < in bytes, ranging from 1 to 4294967295>
- pending-traffic-treatment quota-exhausted pass
- pending-traffic-treatment quota-exhausted drop

Note To enable pending traffic treatment over diameter interfaces no configuration is required under the SMF.

For more information, see the *Sample UPF Configuration* chapter in the *UCC 5G UPF Configuration and Administration Guide* and the *Credit Control Configuration Mode Commands* chapter in the *Command Line Interface Reference, Modes C - D*.

Routing Data Support

Feature Description

The Routing Data support functionality allows the SMF to:

- Process routing data received in CCA-I/CCA-U from OCS
- Override and store the routing data information in the ChargingSubData per diameter session. Smf-service includes stored routing data values in the next subsequent CCR-U or CCR-T message. The smf always expects routing data in CCA-I/CCA-U from OCS.

Monitoring and Troubleshooting

This section provides information for troubleshooting any issues that might arise during the feature operation.

The following is an example output of Routing data per Gy diameter session for a subscriber,

```
"gyDiamSession": {
                            "brrId": 1,
                            "sessionID": ":2:69:ocs-prof:64c37b62:1",
                            "originHost": "dummyOriginHost",
                            "originRealm": "dummyOriginRealm.com",
                            "destRealm": "dummyGyDestRealm.com",
                            "destHost": "Gy-server",
                            "RoutingData": {
                                "primaryHost": "10.105.34.14",
                                "primaryRealm": "dummyGyDestRealm.com",
                                "boundPeer": "Gy-server"
```

```
        }
    },
```

Gz Interface

Table 219: Feature History

Feature Name	Release Information	Description
Asynchronous and Synchronous Usage Report for Offline Bearer Recalculation	2023.04	As part of Gz Usage Reporting, SMF receives Asynchronous and Synchronous Usage Reporting for Offline Bearer recalculation.
Handling Modify Bearer Request Triggers	2023.04	SMF receives the Modify Bearer Request from S-GW for the User Location and TimeZone changes, change notifications. SMF supports N4 Query Interface and Recalculate Interface IEs for Rulebase change, Secondary RAT Usage limit, and Record closing triggers. **Default Setting**: Disabled – Configuration required to enable
Gz Default Bearer Modification	2023.04	This feature allows PCRF-initiated modification of a default Bearer through Gx CCR-U and Gx RAR. You can perform the following functions: • Add rules to the Default Bearer • Delete rules from the Default Bearer • Rulebase Modification • Default-bearer QoS change • APN-AMBR change

PDN Attach and Detach with Gz Interface

Feature Description

The SMF with Legacy Interface supports the Packet Data Network (PDN) attach with Gz interface for a default Bearer to enable offline accounting functions.

How It Works

On receiving offline rules from the PCRF through Gx CCA-I, SMF with the Diameter interface creates offline URRs, maps to the corresponding charging buckets (SDFs), and sends N4EstablishmentRequest toward SMF with the Legacy Interface.

On receiving the Usage report for offline SDF/Bearer level URRs, in the N4 Delete Session Response from UPF, it sends the GTPP Data Record Transfer request toward GTPP. For more information about the Gz Usage Report, see the *Subscriber Charging > Gz Usage Report Handling with GTPP* section.

Use the PDN attach and detach with Gz inteface functionality to:

- Attach Procedure with:
  - offline rules only (Gx+Gz)
  - offline and online rules (Gx+Gy+Gz)
- Detach Procedure with:
  - offline rules only (Gx+Gz)
  - offline and online rules (Gx+Gy+Gz)

Information Element and AVP Support

The PDN attach and detach feature supports the following Information Element(IE):

- **Reporting Level IE for offline rules**: ReportingLevel for dynamic rules is received from PCRF in Gx CCA-I. The other conditions are:
  - If ReportingLevel is not present for dynamic offline rule, then SMF considers reporting level based on the RG and service ID received:
    - if only RG received then reporting level is RatingGroupLevel
    - if both RG and ServiceID received then reporting level is ServiceIdentifierLevel
  - If ReportingLevel is present for dynamic offline rule, then the same is considered.

Note The default offlineReportingLevel configuration is not applicable for Gz.

Handling Offline AVP for Dynamic Rules

The following table describes the function of offline AVPs for Dynamic rules.

Table 220: Rule Level and Command Level AVPs

AVP	Description
Offline AVP in Gx CCR-I	The offline AVP present in Gx CCR-I indicates default configuration for offline charging method. If Gz is enabled, then offline AVP is set to enabled in Gx CCR-I. If not, it is set to disabled.

AVP	Description
Offline AVP in Gx CCA -I/ CCA-U/ RAR	If Offline AVP at RULE level is present within charging rule definition, it defines offline charging method for the corresponding dynamic rule. If enabled, offline charging is done for corresponding dynamic rule. If disabled, offline charging is not done for the corresponding dynamic rule.
	If offline AVP at RULE level is absent within charging rule definition, offline AVP at COMMAND level is considered to determine if offline charging method for dynamic rule is enabled or disabled
	If Offline AVP is absent at RULE and COMMAND levels, the default offline charging method is applied for the dynamic rule. If Gz is enabled, the default offline charging method for dynamic rules is enabled. If not, default offline charging method is disabled.

Handling Offline Dynamic Rules when Gz is Disabled

If Gz is disabled in rulebase, no SDF and bearer level URR are created for offline dynamic rule.The table lists possible combination of input values.

Table 221: Combination of Input Values

Gz enabled in Rulebase profile	Dynamic rule has offline enabled	Offline URR created in N4
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

Abnormal GTPP Record Closure

If there are any path failure either from the Control Plane or User Plane, GTPP record closure with abnormal release message is sent for any one of the following reason:

- UPF session report ERIR
- UPF session report SRIR
- GTPU peer path failure
- UPF recovery release
- UPF path peer failure
- Gtpc peer path fail release
- Gtpc peer restart release

PDN Attach with only Offline Rules

The following call flow and procedure describes PDN attach when dynamic rule with offline is enabled through Gx and Gz interfaces.

Figure 136: Call Flow for PDN Attach with Only Offline Rules

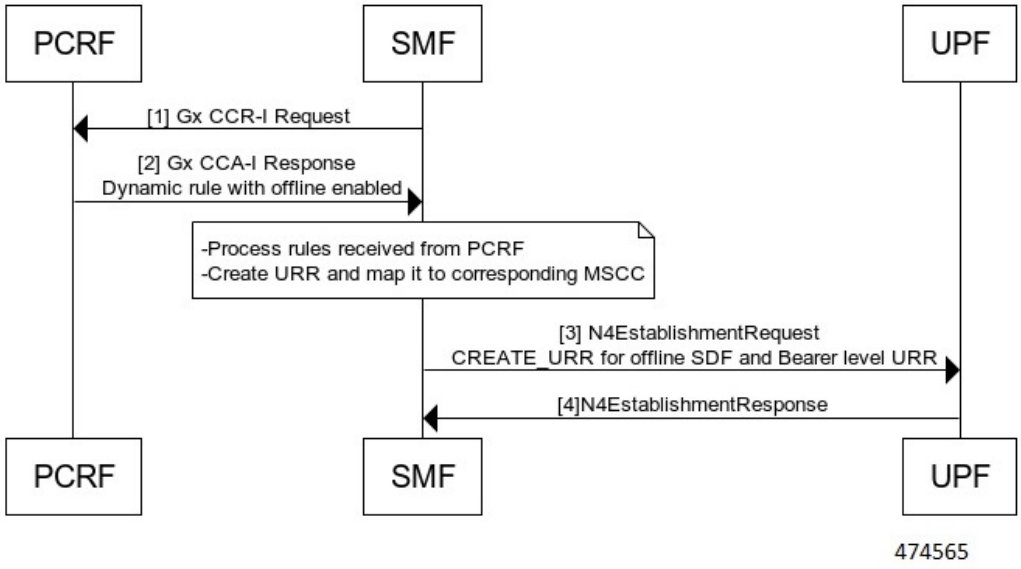


Table 222: Call Flow Description for PDN Attach

Step	Description
1	SMF sends Gx CCR-I towards PCRF.
2	PCRF sends Gx CCA-I towards SMF with default bearer having Dynamic rule with OFFLINE_ENABLED set to True.

Step	Description
3	The N4 Establishment Request is sent towards UPF based on the following conditions: • CREATE_URR for default bearer level URR, if: • PFCP_IE_URR_ID is set to 0x80000002 for default bearer level URR • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD has egcdr threshold values configured in rulebase profile. • PFCP_IE_MEASUREMENT_METHOD has both volume and duration bit set. • CREATE_URR for offline SDF level URR, if: • PFCP_IE_URR_ID has unique offline UrrId • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD has egcdr threshold values configured in the GTPP profile. • PFCP_IE_MEASUREMENT_METHOD has both volume and duration bit set. • All SDF level offline URRs are linked to bearer level URR. That is, PFCP_IE_LINKED_URR_ID has linked URRId set to the BearerLevel URR. • PDR created for dynamic offline rule is mapped to both bearer and SDF level URR.
4	UPF sends N4Establishment response.

PDN Attach with Offline and Online Rules

The following call flow and procedure describes PDN attach when dynamic rule with both online and offline is enabled through Gx, Gy, and Gz interfaces.

Figure 137: Call Flow

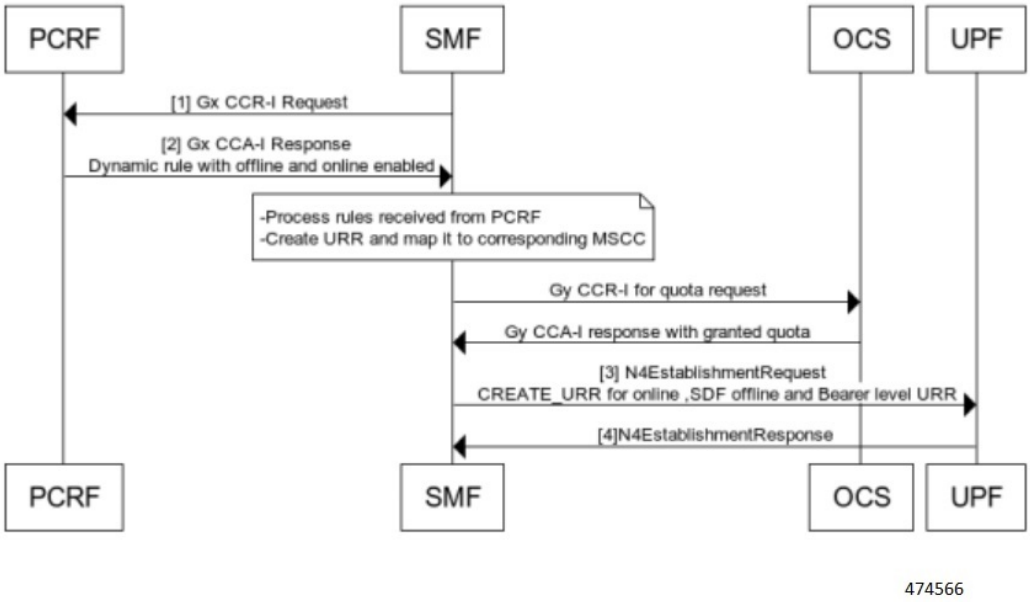


Table 223: Call Flow Description for PDN Attach with Offline and Online Rules

Step	Description
1	SMF sends Gx CCR-I towards PCRF.
2	PCRF sends Gx CCA-I towards SMF with default bearer having Dynamic rule with OFFLINE_ENABLED set to True.

3	The N4 Establishment Request is sent towards UPF based on the following conditions:
	• CREATE_URR for default bearer level URR, if:
	  • PFCP_IE_URR_ID is set to 0x80000002 for default bearer level URR
	• CREATE_URR for offline SDF level URR, if:
	  • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD has egcdr threshold values configured in the GTPP profile.
	• CREATE_URR for Online URR, if:
	  • PFCP_IE_URR_ID has unique online UrrId
	  • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD has threshold values received from OCS
	  • PFCP_IE_MEASUREMENT_METHOD is set based on quota received from OCS.
	• PDR created for dynamic rule (online+offline) is mapped to online, offline SDF and bearer level URR.

Step	Description
4	UPF sends N4Establishment response.

PDN Detach with Offline and Online rules

The following call flow and procedure describes the Usage report in Session Deletion Response.

Figure 138: Call Flow for Usage report as part of N4 Session Delete Response

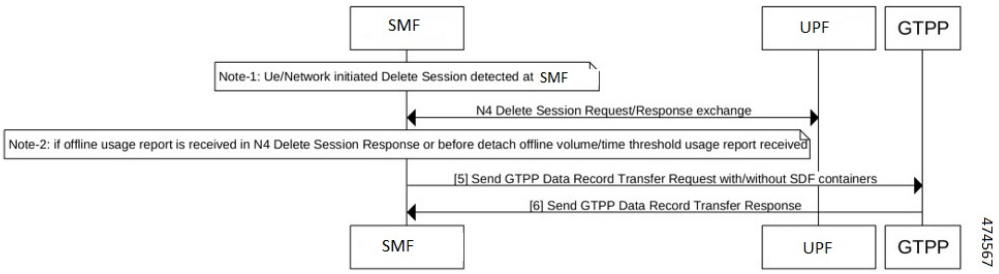


Table 224: Call Flow Description for N4 Session Deletion Response

Step	Description
UE/Network Initiated delete session is detected at SMF.	
1	N4 Delete Session Request or Response is exchanged to delete the session and in turn Usage report is received in the N4 Delete session Response.
3	SMF sends GTPP Data Transfer Request with or without SDF Containers. • If the offline Usage report is received in the N4 Session Deletion Response, then SMF sends the GTPP Data Record Transfer Request for default with SDFs container(with volume usage and serviceConditionChange—one for each RG+service ID. • If the offline Usage report is received without measurement in the N4 Session Deletion Response and no offline Volume/Time threshold usage report received before detach, then the GTPP Data Record Transfer message with GTPP server. • If any offline Volume/Time threshold Usage report is received before detach and no offline Usage report in the N4 Delete Session Response received, then the GTPP Data Record Transfer gets exchanged without SDF Containers for record closure.
4	SMF receives GTPP Data Record Transfer Response from the GTPP server.

Enabling Gz Interface

Use the configuration commands to enable the Gz interface. When the offline AVP is absent at rule and command level, default offline charging method is applied for the dynamic rule. If the Gz interface is enabled, the default offline charging method for dynamic rules is enabled, else the default offline charging is disabled.

```
config
   active-charging service service_name
      rulebase rulebase_name
```

```
        billing-records egcdr value
   profile gtpp-profile  profile_name  gtpp dictionary dictionary_num
   profile network-element ofcs  ofcs_name  gtpp-profile profile_name
   profile dnn intershat network-element-profiles ofcs ofcs_name |
end
```

NOTES:

- **rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.

Note A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow.

- **billing-records egcdr** *value* : Specify to enable eG-CDR billing to True. This associates CnPGW-C with Gz interface in the corresponding rulebase profile. Further, if PCRF sends a different rulebase in Gx CCA-I, Gz interface gets enabled or disabled as per billingRecord EGCDR configuration received in the new rulebase.
- **profile gtpp-profile** *profile_name* **gtpp dictionary** *dictionary_num* : Configure the gtpp profile with dictionary. The correct dictionary is gtpp dictionary *custom24*. *profile_name* specifies list of associated GTPP Profile names that are used in a round robin method for sessions. The maximum number of gtpp profiles allowed is 4.
- **profile network-element ofcs** *ofcs_name* **gtpp-profile** *profile_name* : Configure the network profile ofcs. The OFCS profile config allows option to configure multiple gtpp profiles.

Note Before configuring the **network profile ofcs** ensure to configure the **gtpp-profile.**

Configuring Bearer Level URR Threshold Values

Use the configuration commands to set the Bearer level threshold values.

```
config
   active-charging service service_name
      rulebase rulebase_name
         egcdr threshold volume { downlink | total | uplink }  bytes
end
```

NOTES:

- **rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.
- **egcdr threshold volume { downlink | total | uplink }** *bytes* : Specify the Bearer level URR threshold values. The limit for the number of downlink, total , or uplink octets must be an integer in the range of 100000-4000000000. Example: `egcdr threshold volume downlink 100000 uplink 100000 total 200000`

Configuring SDF Level Offline URR Threshold Values

Use the configuration commands to set the Service Data Fow (SDF) level threshold values.

```
config
   active-charging service service_name
      charging-action charging_action
         egcdr service-data-flow threshold volume { downlink | total |
uplink } bytes
         egcdr service-data-flow threshold interval interval  60
   end
```

NOTES:

- **charging-action** *charging_action_name*: Specify the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- **egcdr service-data-flow threshold volume { downlink | total | uplink }** *bytes* : Specify the SDF level offline URR threshold values. The limit for the number of downlink, total , or uplink octets must be an integer in the range of 100000-4000000000.
- **egcdr service-data-flow threshold interval** *interval* : Configure the threshold for offline charging. Must be an integer in the range of 60–40000000.

Configuring max-losdv Values

Use the configuration commands to create GTPP Data Record with number of Service Data Flow (SDF) container equivalent to the configured maxlosdv value. If the maxlosdv is not configured the default value is 1.

```
config
   active-charging service service_name
      charging-action charging_action
         egcdr losdv-max-containers container_num
   end
```

NOTES:

- **charging-action** *charging_action_name*: Specify the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- **egcdr losdv-max-containers** *container_num* : Specify the maximum List of Service Data containers (LOSDV) for creating a GTPP data record.

Configuring closure-reason

Use the following command to configure closure reason to send in a GTPP Data Record. The closure reason can be for mgmt-intervention or normal release. Default closure reason is mgmt-intervention.

```
config
   active-charging service service_name
      charging-action charging_action
         egcdr closure-reason { admin-disconnect | normal-release |  }

   end
```

NOTES:

- **charging-action** *charging_action_name*: Specify the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- **egcdr closure-reason { admin-disconnect | normal-release | }** : Configure the closure reason.

Gz Usage Reporting

Feature Description

At the time of a converged User Plane function, the P-GW (User Plane) sends the Usage report for triggers such as Volume or Time threshold value for offline charging. During the converged Control Plane function, the P-GW (Control Plane) queries a Usage report when the Charging condition event is detected or URR is removed as part of the Policy Control and Charging (PCC) rule removal at SMF.

After receiving the Usage report, the Control Plane maps URRs to the corresponding offline charging parameter. If the offline charging parameter is not available, then a Service Data Flow (SDF) or Bearer level charging parameter is created for static or predefined rules, and the GTPP Data Record Transfer request is initiated for the respective SDFs. Thus, a Synchronous usage report is received through the N4 Modification Response or N4 Deletion Response message. Asynchronous usage report is received through the N4 Session report request message.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

How it Works

The usage report on the Gz interface includes the following usage report procedures

- Offline Bearer or Offline Bearer along with SDF level, or SDF level URR for Dynamic rules
- Offline Bearer or Offline Bearer along with SDF level, or SDF level URR for Static/Predefined rules
- Online or offline URRs
- N4 Delete Session Response.

Usage Report in N4 Session Report

The following call flows and procedures describe the Usage report in N4 session report with Volume or Time threshold.

Offline Bearer and SDF Level or SDF Level URR for Dynamic Rules

The following call flow and procedure describes the Usage report in N4 session report with Volume/Time threshold for the offline Bearer or SDF level, or SDF level URR for Dynamic rules.

Note Ensure that the URR is present on the UPF with values such as Thresholds and so on. Volume/Time threshold is hit at the UPF for Bearer/SDF or SDF level URRs. UPF relays usage to the SMF along with usage reporting trigger information.

Figure 139: Call Flow for Offline Usage Report in N4 Session Report

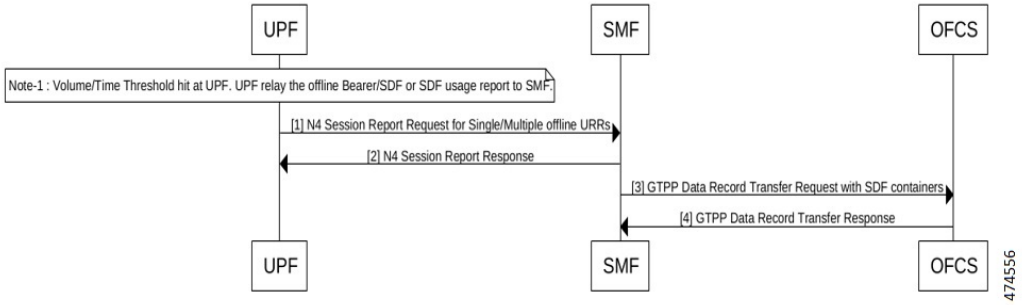


Table 225: Call Flow Description for Offline Usage Report in N4 Session Report

Step	Description
1	UPF sends N4 Session Report Request for either offline Bearer usage along with SDFs or only SDFs usage to the SMF.
2	SMF sends N4 Session Report Response.
3	SMF sends GTPP Data Record Transfer Request with SDF Containers to the Offline Charging System (OFCS). This request is sent with one or multiple SDFs with volume usage and serviceConditionChange—one for each RG+service ID. **Note** The algorithm works based one of the following conditions: • If the Offline Bearer Usage report is received along with the SDF or SDF Usage report that is received and max charging condition hit (**max-losdv** CLI configured value – default value is 1) • If an Offline Usage report received is without measurement for a Bearer level Time threshold in the N4 Session Report Request, then GTPP Data Record Transfer message with recordClosureReason “TimeLimit” without SDF Containers gets exchanged with OFCS. • If an Offline Usage report that is received is without measurement for the SDF level Time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message does not get exchanged with OFCS.
4	OFCS sends GTPP Data Record Transfer Response.

Sample Configuration

The following is sample message output for Dynamic Rule SDF level URR

```
URR ID:
               Type: 81   Length: 4
               Value: 0x000000021.
           USAGE REPORT TRIGGER:
               Type: 63   Length: 2
               Time Threshold
           VOLUME MEASUREMENT:
               Type: 66   Length: 25
```

```
            Total Volume: 450
            Uplink Volume: 250
            Downlink Volume: 200
        DURATION MEASUREMENT:
            Type: 67   Length: 4
            Value: 100

accessPointNameNi                    cisco.com
ratingGroup                          10
chargingRuleBaseName                 cisco
resultCode                           2001
localSequenceNumber                  1
timeOfFirstUsage                     220829173906-0400
timeOfLastUsage                      220829173907-0400
timeUsage                            1
serviceConditionChange               Time Exhaust
 qCI                                  5
 maxRequestedBandwithUL               0
 maxRequestedBandwithDL               0
 guaranteedBitrateUL                  0
 guaranteedBitrateDL                  0
 aRP                                  5
servingNodeAddress                   2002::2:61
datavolumeFBCUplink                  250
datavolumeFBCDownlink                200
timeOfReport                         220829173907-0400
userLocationInformation
 Location Type                    TAI
  MCC                                214
  MNC                                365
  TAC                                0x6789
  Location Type                   ECGI
  MCC                                214
  MNC                                365
  ECI                                0x1234567
```

Offline Static or Predefined Rules

The following call flow and procedure describes the Usage report in N4 session report with Volume/Time threshold for the offline Bearer or SDF level, or SDF level URR for Predefined and Static Rules.

Figure 140: Call Flow for Usage Report in N4 Session Report for Offline Static or Predefined Rules

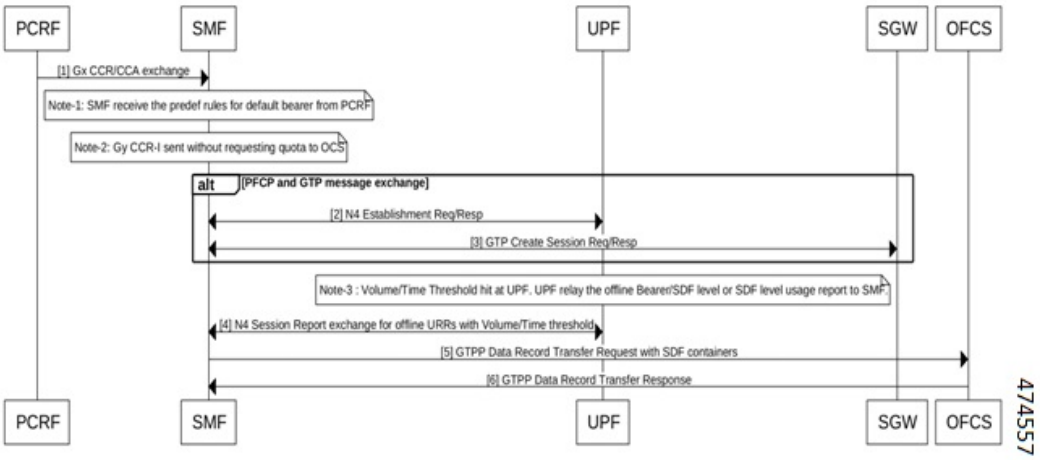


Table 226: Call Flow Description for Offline Static or Predefined Rules

Step	Description
1	PCRF performs Gx-CCR or CCA exchange with SMF. In this exchange, the SMF receives Predefined Rules for default bearer from the PCRF.
2	SMF initiates N4 session establishment request exchange with UPF. In the same request, UPF relays the PFCP message exchange.as response.
3	SMF sends Create session request to the S-GW and GTPP response message is exchanged.
Note	Volume/Time threshold is detected at UPF and UPF prepares Usage report with VOLTH/TIMTH for the offline Bearer/SDF level or SDF level URR.
4	SMF sends N4 Session Report Request/Response exchange with offline Volume/Time threshold. When SMF receives the SDF level or Bearer/SDF level usage report with VOLTH/TIMTH for static/predefined rules, the Bearer/SDF level URR is created at SMF if not there, and the SDF level URR gets linked to the Bearer level URR.
5	SMF sends GTPP Data Record Transfer Request with SDF Containers to the Offline Charging Server (OFCS). This request is sent with one or multiple SDFs with volume usage and serviceConditionChange—one for each RG+service ID. **Note** The algorithm works based one of the following conditions: • If the offline Bearer Usage report is received along with the SDF or SDF Usage report received and a maximum charging condition is hit (**max-losdv** CLI configured value – default value is 1). • If the offline Usage report received is without measurement for the Bearer level Time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message with recordClosureReason “TimeLimit” without SDF Containers gets exchanged with OFCS. • If the offline usage report received is without measurement for the SDF level Time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message does not get exchanged with OFCS.
6	OFCS sends GTPP Data Record transfer response to the SMF.

Sample Configuration

The following is a sample message output for offline SDF level URR Id for static rule Usage report:

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000021.
            USAGE REPORT TRIGGER:
                Type: 63
                Vol Threshold
            VOLUME MEASUREMENT:
                Type: 66
                Total Volume: 400
                Uplink Volume: 200
                Downlink Volume: 200
```

```
accessPointNameNi                   cisco.com
ratingGroup                         101
chargingRuleBaseName                prepaid
resultCode                          2001
localSequenceNumber                 1
timeOfFirstUsage                    220920093554-0400
timeOfLastUsage                     220920093558-0400
timeUsage                           4
serviceConditionChange              Volume Exhaust
 qCI                                 5
 maxRequestedBandwithUL              512000
 maxRequestedBandwithDL              512000
 guaranteedBitrateUL                 0
 guaranteedBitrateDL                 0
 aRP                                 84
servingNodeAddress                  192.60.7.31
datavolumeFBCUplink                 200
datavolumeFBCDownlink               200
timeOfReport                        220920093601-0400
userLocationInformation
 Location Type                    CGI
  MCC                               404
  MNC                               43
  LAC                               0x84C
  CI                                0x4F0A
```

Online and Offline URRs

The following call flow and procedure describes the Usage report in N4 session report for online and offline URRs.

Figure 141: Call Flow for Usage Report in N4 Session Report for Online and Offline

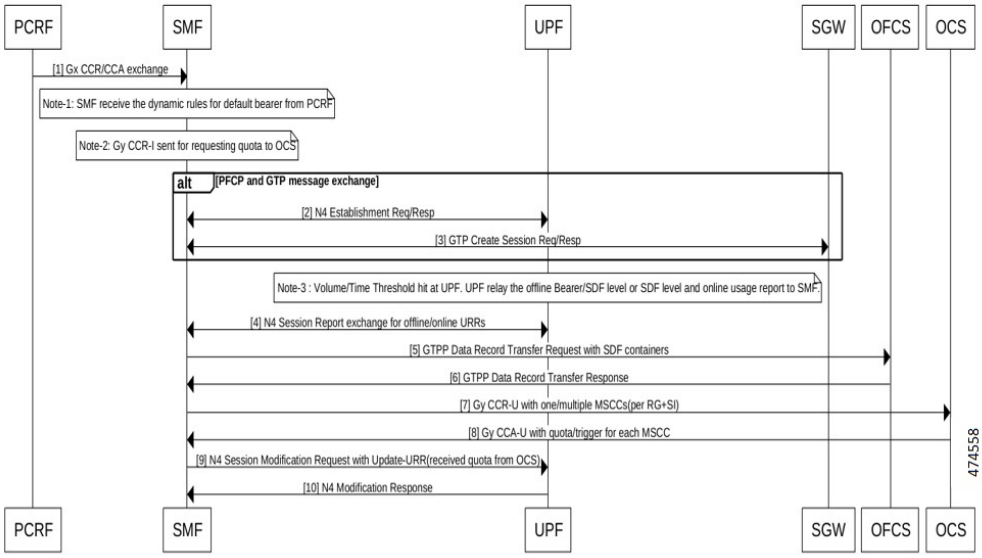


Table 227: Call Flow Description for Online and Offline URRs

Step	Description
1	PCRF performs Gx-CCR or CCA Exchange with SMF. In this Exchange, the SMF receives Dynamic Rules for default bearer from the PCRF.
2	SMF initiates N4 session establishment request Exchange with UPF. In the same request, UPF relays the PFCP message Exchange as response.
3	SMF sends Create session request to the S-GW and the GTPP response message is exchanged.
Note	Volume/Time threshold that is detected at the UPF and UPF prepares a usage report with VOLTH/TIMTH for the online URR and offline Bearer/SDF level or SDF level URR.
4	SMF sends N4 Session Report Request/Response Exchange with online and offline Volume/Time threshold. When SMF receives the SDF level or Bearer/SDF level usage report with VOLTH/TIMTH for online URR and offline bearer/SDF level URR.
5	SMF sends GTPP Data Record Transfer Request with SDF Containers to the Offline Charging Server (OFCS). This request is sent with one or multiple SDFs with volume usage and serviceConditionChange—one for each RG+service ID. **Note** The algorithm works based one of the following conditions: • If the Offline Bearer Usage report is received along with the SDF or SDF Usage report received and a maximum charging condition is hit (**max-losdv** CLI configured value – default value is 1). • If the offline Usage report received is without measurement for the Bearer level Time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message with recordClosureReason “TimeLimit” without SDF Containers gets exchanged with OFCS. • If the offline Usage report received is without measurement for the SDF level Time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message does not get exchanged with OFCS.
6	OFCS sends GTPP Data Record transfer response to the SMF.
7	SMF sends Gy CCR-U with one or multiple MSCCs—for each RG+SID.
8	SMF receives Gy CCA-I with quota, triggers for each RG+Service ID.
9	SMF sends N4 Session Modification Request to the UPF with update-URR. The Quota is received from OCS for the required online URRs.
10	UPF sends N4 Session Modification Response.

Sample Configuration

The following is a sample message output for offline Bearer level URR.

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000002   --- Offline Bearer level URR Id
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Volume Threshold
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 101096
                Uplink Volume: 896
                Downlink Volume: 100200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 16

            URR ID:
                Type: 81   Length: 4
                Value: 0x80000021.
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Linked Usage Reporting
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 101096
                Uplink Volume: 896
                Downlink Volume: 100200
        DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 1


         accessPointNameNi                   cisco.com
         ratingGroup                         10
         chargingRuleBaseName                cisco
         resultCode                          2001
         localSequenceNumber                 1
         timeOfFirstUsage                    220829173906-0400
         timeOfLastUsage                     220829173907-0400
         timeUsage                           1
         serviceConditionChange              Volume Limit
          qCI                                 5
          maxRequestedBandwithUL              0
          maxRequestedBandwithDL              0
          guaranteedBitrateUL                 0
          guaranteedBitrateDL                 0
          aRP                                 5
         servingNodeAddress                  2002::2:61
         datavolumeFBCUplink                 896
         datavolumeFBCDownlink               100200
         timeOfReport                        220829173907-0400
         userLocationInformation
          Location Type                    TAI
           MCC                               214
           MNC                               365
           TAC                               0x6789
           Location Type                   ECGI
           MCC                               214
           MNC                               365
           ECI                               0x1234567
```

Offline Usage Report in N4 Session Deletion Response

The following call flow and procedure describes the Usage report in Session Deletion Response.

Note Ensure that the UE or Network Initiated delete session is detected at the SMF.

Figure 142: Call Flow for Usage Report in N4 Delete Session Response

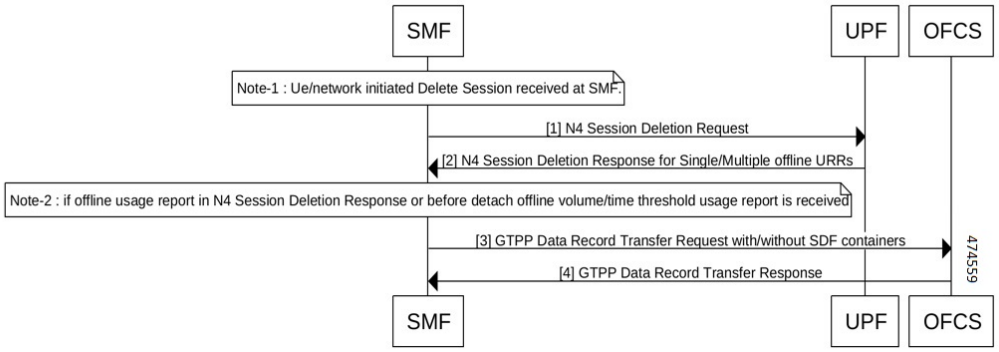


Table 228: Call Flow Description for Session Deletion Response

Step	Description
1	SMF initiates N4 Session Deletion Request to delete the session to the UPF.
2	UPF sends N4 Session Deletion Response with offline Usage report.
3	SMF sends GTPP Data Transfer Request with or without SDF Containers. • If the offline Usage report is received in the N4 Session Deletion Response, then SMF sends the GTPP Data Record Transfer Request for default with SDFs container(with volume usage and serviceConditionChange—one for each RG+service ID. • If the offline Usage report is received without measurement in the N4 Session Deletion Response and no offline Volume/Time threshold usage report received before detach, then the GTPP Data Record Transfer message with recordClosureReason “NormalRelease” without SDF Containers gets exchanged with OFCS. • If any offline Volume/Time threshold Usage report is received before detach and no offline Usage report in the N4 Delete Session Response received, then the GTPP Data Record Transfer gets exchanged without SDF Containers for record closure.
4	SMF receives GTPP Data Record Transfer Response from OFCS.

Offline SDF Usage Report in N4 Session Report

The Offline SDF or Bearer URRs are present on UPF with values like Thresholds and so on. SDF Volume/Time threshold is hit at the UPF for SDF level URRs. UPF relays usage to the SMF along with usage reporting trigger information. The following call flow and procedure describes the Asynchronous Usage report for offline Bearer recalculation.

Figure 143: Call Flow for Asynchronous Usage report for offline Bearer recalculatio

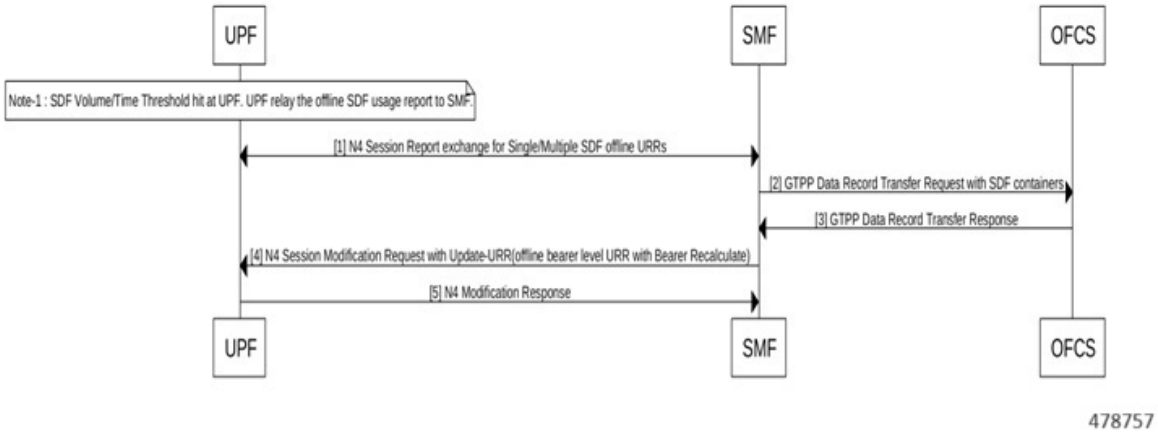


Table 229: Call Flow Description for Async Usage Report Offline Bearer Recalculation

Step	Description
1	UPF initiates N4 Session Report Exchange with SMF.
2	SMF sends GTPP Data Transfer Request with SDF Containers. • If the Offline usage report is received in the N4 Session Report Request, then the SMF sends a GTPP Data Record Transfer Request with SDFs container with volume usage and serviceConditionChange—one for each RG+service ID only if the maximum charging condition is reached. • If the Offline usage report that is received is without measurement for SDF level time threshold in the N4 Session Report Request, then a GTPP Data Record Transfer message does not get exchanged with OFCS.
3	SMF receives GTPP Data Record Transfer Response from OFCS.
4	After receiving the Offline SDF usage, if the SMF sends GTPP Data Record Transfer Request due to maximum charging condition, then N4 Modification Request with Update Bearer level URR (Bearer Recalculate) is sent to the UPF.
5	UPF sends N4 Modification Response.

Offline SDF or Online URRs Usage Report

For the Volume/Time threshold detected at UPF, the UPF prepares the Usage report with VOLTH/TIMTH for online URR or offline SDF level URR. The following call flow and procedure describes the Asynchronous Usage report for online or offline Bearer Recalculation.

Figure 144: Call Flow for Async Usage Report Online or Offline Bearer Recalculate

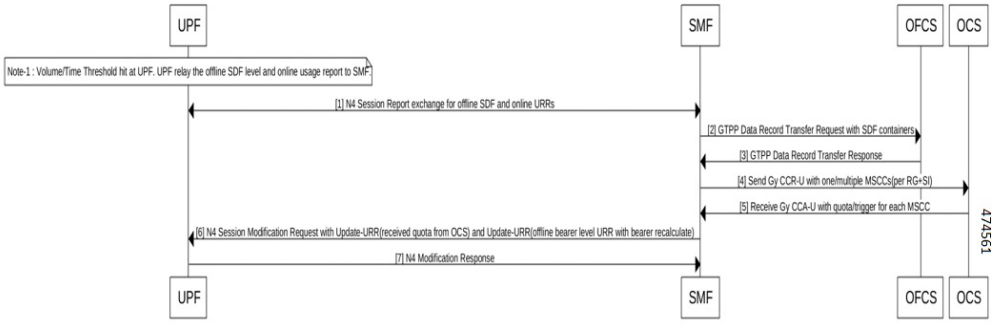


Table 230: Call Flow Description for Async Usage Report Online or Offline Bearer Recalculation

Step	Description
1	UPF initiates N4 Session Report Request/Response exchange with online/offline Volume/Time threshold.
2	SMF sends GTPP Data Transfer Request with SDF Containers. • If the Offline usage report is received in N4 Session Report Request, then SMF sends the GTPP Data Record Transfer Request with SDFs container(with volume usage and serviceConditionChange—one for each RG+service ID only if the maximum charging condition is hit. • If the Offline usage report received is without measurement for the SDF level time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message does not get exchanged with OFCS.
3	SMF receives GTPP Data Record Transfer Response from OFCS.
4	SMF sends Gy CCR-U with one or multiple MSCCs (for each RG+Service ID) to the OCS.
5	SMF receives Gy CCA-I with quota, triggers for each RG+Service ID.
6	SMF sends N4 Session Modification Request to the UPF. **Note** The update URR-with quota for required online URRs and update URR – with bearer recalculate for offline bearer level URR is sent.
7	UPF sends N4 Session Modification Response to the SMF.

Offline Bearer Usage Report

The Offline SDF or Bearer URRs are present on UPF with values like Thresholds and so on. SDF Volume/Time threshold is hit at the UPF for Bearer URRs. UPF relays usage to the SMF along with usage reporting trigger information. The following call flow and procedure describes the Offline Bearer Usage Report in N4 session report with no Bearer Recalculation.

Figure 145: Async Offline Bearer Usage Report

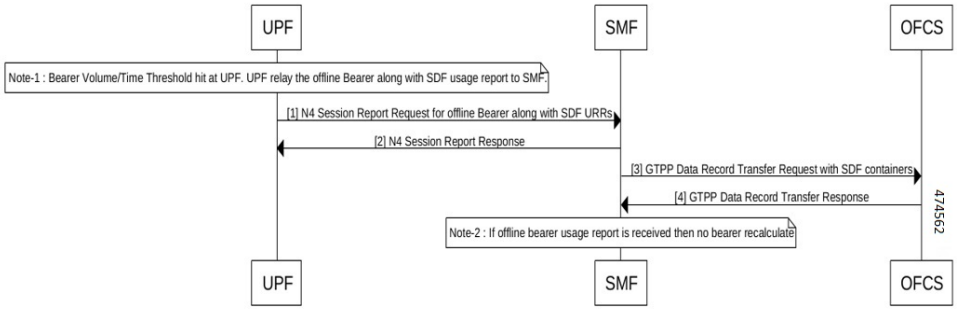


Table 231: Call Flow Description for Async Offline Bearer Usage Report with no Bearer Recalculation

Step	Description
1	UPF sends N4 Session report Request with offline Bearer along with SDF usage to the SMF.
2	SMF sends N4 Session report Response to the UPF.
3	SMF sends GTPP Data Transfer Request with SDF Containers with volume usage and serviceConditionChange—one for each RG+service ID only if the maximum charging condition is hit. If the offline usage report received is without measurement for the Bearer level time threshold in the N4 Session Report Request, then the GTPP Data Record Transfer message is sent without the SDF container with OFCS.
4	SMF receives the GTPP Data Record Transfer Response from OFCS.
Note	When the Bearer usage report is received without volume measurement, the SMF does not send a bearer recalculation to the UPF.

Offline SDF Usage Report

The following call flow and procedure describes the Offline Bearer Usage Report in N4 session report with no Bearer Recalculation.

Figure 146: Call Flow for Async Usage Report Offline with no Bearer Recalculate

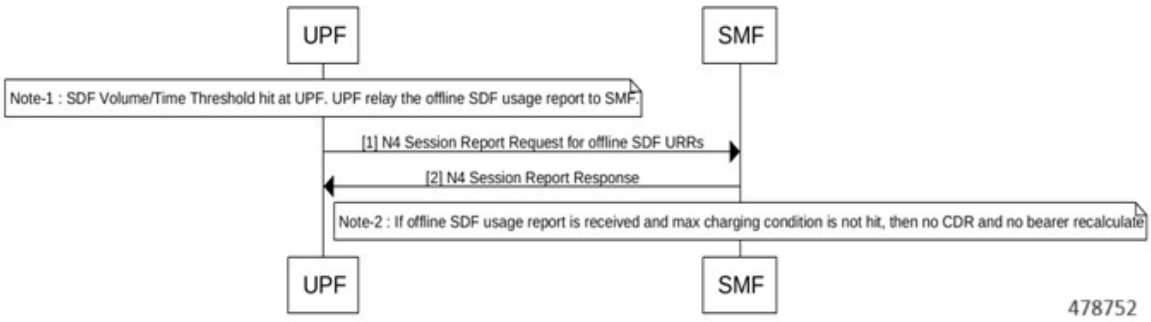


Table 232: Call Flow Description for Async Offline Bearer Usage Report witn no Bearer Recalculation

Step	Description
Note	Offline SDF/Bearer URRs are present on UPF with values such as Thresholds and so on. SDF Volume or Time threshold is hit at UPF for SDF level URRs. UPF need to relay usage to SMF along with Usage reporting trigger information.
1	UPF send N4 Session report Request with offline SDF usage to SMF.
2	SMF sends N4 Session report Response to UPF.
Note	When the SDF usage report is received and maximum charging condition is not hit, SMF does send CDR to OFCS and Bearer recalculate to UPF. The max-losdv CLI value configured as 2 and only one SDF usage report is received. Once the second SDF level usage is received and the maximum charging condition is hit then, CDR is sent to the GTPP and Bearer recalculate to UPF.

Synchronous Online and Offline Usage Report for Offline Bearer Recalculation

The following call flow and procedure explains the Offline SDFs and Online URRs Usage Report in N4 Session Modification Request with immediate trigger.

Figure 147: Call Flow for Sync Usage Report

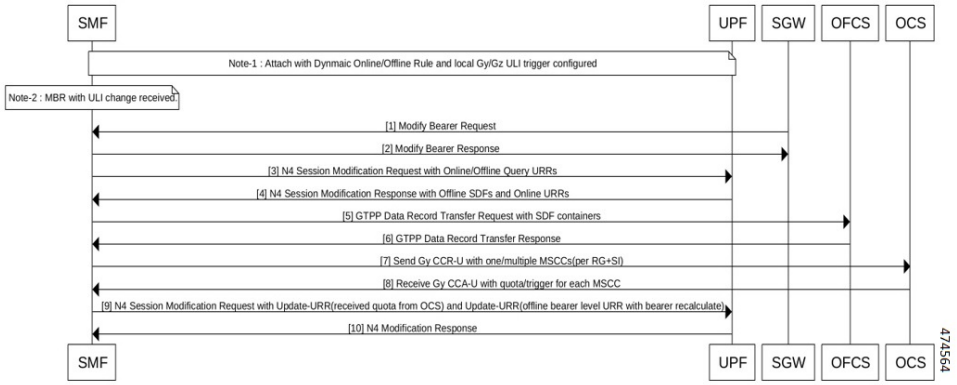


Table 233: Call Flow Description for Synchronous Online and Offline Usage Report for Offline Bearer Recalculation

Step	Description
Note	The Default Bearer is created with one dynamic online and offline rule. The ULI trigger is locally configured under charging profile for OFCS and OCS. Modify Bearer Request with ULI change is received.
1	S-GW sends Modify Bearer Request with new ULI.
2	SMF sends Modify Bearer Response to the S-GW.
3	SMF sends N4 Session Modification request to the UPF with query URR for online and Query Interface for offline URRs. SMF sends N4 Session Modification request to the UPF with query URR for online URRs and Query Interface and Recalculate Interface with offline bit set to 1 for offline URRs.
4	UPF sends N4 Session Modification Response for Offline SDFs and Online URRs with reporting trigger Immediate.
5	SMF sends GTPP Data Transfer Request with SDF Containers. • If the Offline usage report is received in the N4 Session Modification Response, then SMF sends the GTPP Data Record Transfer Request with SDFs container with volume usage and serviceConditionChange—one for each RG+service ID only if the maximum charging condition is hit. • If the Offline usage report received is without measurement for the SDF level time threshold in the N4 Session Modification Response, then the GTPP Data Record Transfer message does not get exchanged with OFCS.
6	SMF receives GTPP Data Record Transfer Response from OFCS.
7	SMF sends Gy CCR-U with one/multiple MSCCs for each RG+SID to the OCS.
8	SMF receives Gy CCA-I with quota, triggers for each RG+Service ID.

Step	Description
9	SMF sends N4 Session Modification Request with update *URR-with received quota* for online URRs and update URR – with bearer recalculate for offline bearer level URR.
10	UPF sends N4 Session Modification Response to the SMF.

Sample Configuration

The following is a sample message output for an Offline Bearer level URR.

```
URR ID:
                Type: 81   Length: 4
                Value: 0x80000002
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Time Threshold
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 450
                Uplink Volume: 250
                Downlink Volume: 200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 100

            URR ID:
                Type: 81   Length: 4
                Value: 0x00000021.
            USAGE REPORT TRIGGER:
                Type: 63   Length: 2
                Linked Usage Reporting
            VOLUME MEASUREMENT:
                Type: 66   Length: 25
                Total Volume: 450
                Uplink Volume: 250
                Downlink Volume: 200
            DURATION MEASUREMENT:
                Type: 67   Length: 4
                Value: 87

        accessPointNameNi                   cisco.com
        ratingGroup                         10
        chargingRuleBaseName                cisco
        resultCode                          2001
        localSequenceNumber                 1
        timeOfFirstUsage                    220822005641-0400
        timeOfLastUsage                     220822005646-0400
        timeUsage                           5
        serviceConditionChange              Time Limit
         qCI                                 5
         maxRequestedBandwithUL              0
         maxRequestedBandwithDL              0
         guaranteedBitrateUL                 0
         guaranteedBitrateDL                 0
         aRP                                 5
        servingNodeAddress                  2002::2:61
        datavolumeFBCUplink                 250
        datavolumeFBCDownlink               200
        timeOfReport                        220822005818-0400
        userLocationInformation
         Location Type                   TAI
```

```
MCC                                 214
MNC                                 365
TAC                                 0x6789
Location Type                     ECGI
MCC                                 214
MNC                                 365
ECI                                 0x1234567
```

OAM Support

This section describes operations, administration, and maintenance information regarding support for interfaces in SMF.

Bulk Statistics Support

The following counters are added for the Gz charging functionality:

- ofcs_cdr_message_stats— The counter is incremeted for every CDR towards CGF. The following labels are added:
  - **gtpp_profile** *gtpp_profile_name*: This metric displays the GTPP profile.
  - **RuleBase** *RuleBase Name*: This metric displays the rule base name.
  - **record_closure_reason***record_closure_reason* : This metric displays any one of the record closure reasons:
    - normalRelease
    - abnormalRelease
    - cAMELInitCallRelease
    - volumeLimit
    - timeLimit
    - servingNodeChange
    - maxChangeCond
    - managementIntervention
    - intraSGSNIntersystemChange
    - rATChange
    - mSTimeZoneChange
    - sGSNPLMNIDChange
    - **dnn** *dnn_name* : This metric displays the DNN name.
    - **TriggerType** *Trigger_name* : This metric displays the following GZ_SECONDARY_RAT_USAGE_LIMIT_REACHED trigger type.
- ofcs_sdf_container_stats—The counter is incremeted for every SDF Containers of CDR towards CGF. The following labels are added.

- **service_condition_change** *service_condition_change_value* : The service_condition_change label value is a comma separated in case of multiple service condition change values for each SDF container. This metric displays any one of the service condition change values:
  - QoSChange
  - PdpContextRelease
  - ConfigurationChange
  - ServiceStop
  - DccaTimeExhausted
  - DccaVolumeExhausted
- ofcs_cdr_drop_stats —The counter is incremeted for every CDR is suppressed due to Zero suppression towards OFCS. The following labels are added:
  - **procedure_type** *procedure_name*: This metric displays SMF procedure name along with trigger name, which met the suppression criterion.
  - **TriggerType** *Trigger_name* : This metric displays any one of the following trigger names:
    - final-cdr
    - external-trigger-cdr
    - intrenal-trigger-cdr
  - **dnn** *dnn_name* : This metric displays the DNN name.

Handling Modify Bearer Request Triggers

Feature Description

SMF receives the Modify Bearer Request from S-GW for the User Location and TimeZone changes. The following functionalities are supported through triggers:

- TimeZone Trigger: Use the CHANGE_IN_UE_TIMEZONE trigger to identify timezone change
- ULI Triggers: Use the CHANGE_IN_LOCATION, CHANGEINLOCATION_TAC and CHANGEINLOCATION_ECGI to identify a location change.

Limitations

Following are the limitations:

- SMF supports QueryInterface and RecalculateInterface for only Gz offline URRs. It is not supported for Gy online URR and RADIUS URR.
- RecalculateInterface value (264) IE type is not in the vendor type range as specified by specification. Update to RecalculateInterface value (264) IE type is required when support is available at UPF.
- Trigger Handling for Dedicated Bearer is not supported.

Timezone Change

Timezone information is sent only at CDR level. The following call flow depicts the Timezone change in the SMF.

Figure 148: Modify Bearer Request with Timezone Change

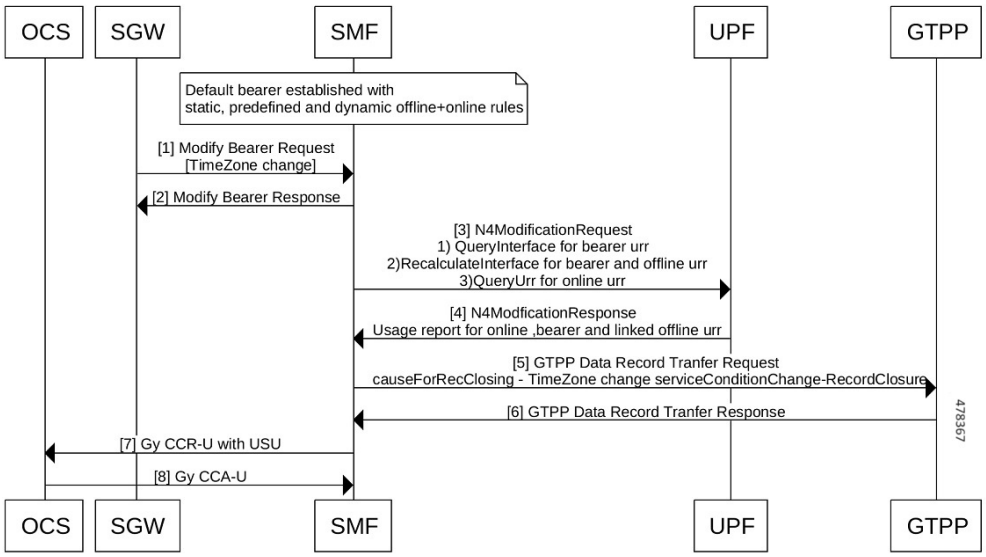


Table 234: Call Flow Description for Timezone Change

Step	Description
A Default Bearer is established successfully and an initial attach happens with dynamic, static, and predefined rules.	
1	SMF receives Modify Bearer request from S-GW with Timezone change.
2	SMF sends the Modify Bearer response.
3	N4 modification request is sent with the following details: • QueryUrr for online URR • Query Interface with **bearer_urr** set for Bearer URR • Recalculate Interface with **offline_urr** and **bearer_urr** for SDF URR. **Note** When the **bearer_urr** is queried in the Query Interface, recalculate is requested for both bearer and offline/SDF URR in the Recalculate Interface.
4	SMF receives an N4 modification response from UPF with the following details: • UsageReport for Bearer URR and linked SDF URRs • UsageReport for online URR

Step	Description
5	SMF sends GTPP Data Record Transfer request to the GTPP with record closure reason Timezone change. **Note** A TimeZone change is a record closure event as per the specification. Hence, the Bearer URR is queried and a CDR is sent in the subsequently.
6	SMF receives the GTPP Data Record Transfer Response.
7	UPF sends a Gy CCR-U message with usage that is received to the OCS.
8	SMF receives Gy CCA-U from OCS.

Sample N4 Modification Request

```
PFCP_SESSION_MODIFICATION_REQUEST (52)
'Retransmit flag'  : 0
'Seid'             : 17293822569102704642
'Length'           : 71
'Sequence Number'  : 3
'Number of IEs'    : 5
    PFCP_IE_SUB_PARAMS (226)
      'sub_params' : {'rat_type': 6, 'sgsn_v4': '10.105.38.134', 'uli_len': 13, 'uli':
{'spare': 0, 'ecgi': 1, 'tai': 1, 'nrtai': 0, 'nrcgi': 0, 'tai-mcc': 123, 'tai-mnc': 456,
'tai-tac': 2347, 'ecgi-mcc': 123, 'ecgi-mnc': 456, 'ecgi-spare': 0, 'ecgi-eci': 1234567},
'ggsn_v4': '10.21.82.217'}

    PFCP_IE_QUERY_URR (77)

            PFCP_IE_URR_ID (81)
                  'urr_id' : 55

    PFCP_IE_PFCPSMREQFLAGS (49)
           'spare' : 0
           'qaurr' : 1
           'sndem' : 0
           'drobu' : 0

    PFCP_IE_QUERY_INTERFACE (253)
    'query_interface' : {'spare_3bit': 0, 'offline_urr': 0, 'online_urr': 0, 'radius_urr':
 0, 'bearer_urr': 1, 'sess_urr': 0}

    PFCP_IE_RECALCULATE_INTERFACE (264)
    'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0,
'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}


        MESSAGE BUFFER:
                2134 0047 F000 0000 0000 0002 0000 0304
                00E2 001C 0100 012A 060A 6926 860D 1821
                6354 092B 2163 5400 12D6 870A 1552 D904
                004D 0008 0051 0004 0000 0037 0031 0001
                0400 FD00 0110 0108 0001 10
```

TimeZone Information sent at CDR level

The following table describes timezone information sent at CDR level.

PreCondition	Scenarios	Expected Behaviour

Maxlosdv 1 CSR with MsTimeZone Bearer threshold 60 seconds **TimeZone** trigger enable	Attach with **TimeZone1** Bearer usage received for Time threshold MBR with **TimeZone2** Bearer usage received for Time threshold MBR with **TimeZone3** Bearer usage received for Time threshold Detach with traffic data	On the N4 interface, Query for TimeZone change happens with **bearer** bit set for offline. After receiving first bearer usage, CDR is sent with **TimeZone1** After receiving bearer usage for the first **MBR**, CDR is sent with **TimeZone1** After receiving second bearer usage, CDR is sent with **TimeZone2** After receiving bearer usage for second **MBR**, CDR is sent with **TimeZone2** After receiving third bearer usage, CDR is sent with **TimeZone3** For terminate usage report during **detach**, CDR is sent with **TimeZone3**
Maxlosdv 1 CSR without **MsTimeZone** Bearer threshold 60 seconds **TimeZone** trigger enable	Attach **without TimeZone** Bearer usage received for Time threshold MBR with **TimeZone1** Bearer usage received for Time threshold MBR with **TimeZone2** Bearer usage received for Time threshold Detach with traffic data	On the N4 interface, Query for TimeZone change happens with **bearer** bit set for offline. After receiving the first Bearer usage, CDR is sent **without TimeZone** After receiving the Bearer usage for first **MBR**, CDR is sent **without TimeZone** After receiving second bearer usage, CDR is sent with **TimeZone1** After receiving Bearer usage for second **MBR**, CDR is sent with **TimeZone1** After receiving third Bearer usage, CDR is sent with **TimeZone2** For terminate usage report during **detach**, CDR is sent with **TimeZone2**
Maxlosdv 1 CSR with **MsTimeZone** Bearer threshold 60 seconds **Suppress zero cdrs** **TimeZone** trigger enable	Attach with **TimeZone1** MBR with **TimeZone2 and zero usage(no traffic, zero volume) received** MBR with **TimeZone3 and zero usage(no traffic, zero volume) received** Zero usage(no traffic, zero volume) received for Time threshold for no traffic Detach with traffic data	On the N4 interface, Query for TimeZone change happens with **bearer** bit set for offline. For terminate usage report during detach, CDR is sent with **TimeZone2**

Maxlosdv 1 CSR with MsTimeZone Bearer threshold 60 seconds **TimeZone** trigger **disable**	Attach with **TimeZone1** Bearer usage received for Time threshold MBR with **TimeZone2** Bearer usage received for Time threshold MBR with **TimeZone3** Bearer usage received for Time threshold Detach	On N4 Query for TimeZone change does not happen for offline. All CDRs are sent with **TimeZone1**
Maxlosdv 1 CSR without MsTimeZone Bearer threshold 60 seconds **TimeZone** trigger **disable**	Attach with **TimeZone1** Bearer usage received for Time threshold MBR with **TimeZone2** Bearer usage received for Time threshold MBR with **TimeZone3** Bearer usage received for Time threshold Detach	On N4 Query for TimeZone change shall not happen for offline. All CDR shall be sent **without TimeZone**.

User Location Information Change

The User Location Information is sent at both CDR and SDFcontainer level. After the attach is performed, one CDR gets opened with the current record opening time and with current ULI. Once a CDR is generated another CDR is opened with the current record opening time and with the last user location information.

The following call flow depicts the User Location Information (ULI) change in the SMF.

Figure 149: Modify Bearer Request with ULI Change

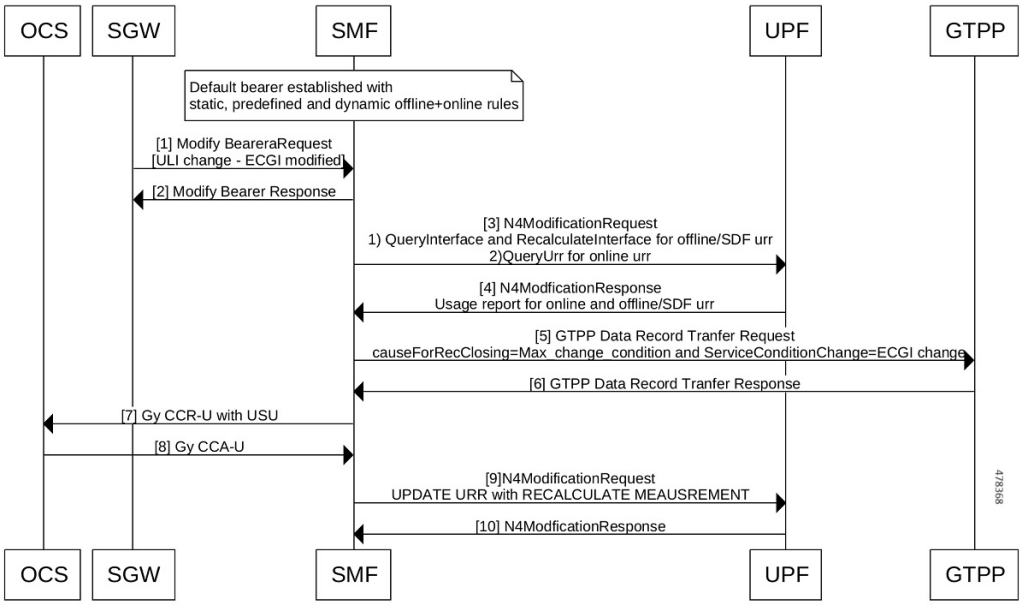


Table 235: Call Flow Description for ULI Change

Step	Description
1	Default Bearer is established successfully and an initial attach happens with dynamic, static, and predefined rules.
2	SMF receives Modify Bearer request from S-GW with ECGI, which is modified in ULI.
3	SMF sends Modify Bearer Response.
4	N4 modification request is sent with the following details: • QueryUrr for online URR. • Query Interface with **offline_urr** set for SDF URR. • Recalculate Interface with **offline_urr** set for SDF URR. **Note** When the **offline_urr** is queried in the Query Interface, recalculation is requested for only offline/SDF URR in the Recalculate Interafce.
5	SMF receives N4 modification response from UPF with the following details: • UsageReport for SDF URRs • UsageReport for online URR

Step	Description
6	SMF sends GTPP Data Record Transfer request with record a closure reason as Max_change_condition and serviceConditionChange as ECGI change. **Note** ULI change is not a closure event record as per the specification. Hence, the SDF URR is queried. On receiving the Usage report for the same, if MaxLosDv is hit, CDR is sent with the corresponding reason.
6	SMF receives the GTPP Data Record Transfer Response.
7	UPF sends a Gy CCR-U message with usage that is received to the OCS.
8	SMF receives Gy CCA-U from OCS.

Sample N4 Modification Request

```
PFCP_SESSION_MODIFICATION_REQUEST (52)
'Retransmit flag'  : 0
'Seid'             : 17293822569102704642
'Length'           : 71
'Sequence Number'  : 3
'Number of IEs'    : 5
    PFCP_IE_SUB_PARAMS (226)
      'sub_params' : {'rat_type': 6, 'sgsn_v4': '10.105.38.134', 'uli_len': 13, 'uli':
{'spare': 0, 'ecgi': 1, 'tai': 1, 'nrtai': 0, 'nrcgi': 0, 'tai-mcc': 123, 'tai-mnc': 456,
'tai-tac': 2347, 'ecgi-mcc': 123, 'ecgi-mnc': 456, 'ecgi-spare': 0, 'ecgi-eci': 1234567},
'ggsn_v4': '10.21.82.217'}

    PFCP_IE_QUERY_URR (77)

            PFCP_IE_URR_ID (81)
                  'urr_id' : 55

    PFCP_IE_PFCPSMREQFLAGS (49)
           'spare' : 0
           'qaurr' : 1
           'sndem' : 0
           'drobu' : 0

    PFCP_IE_QUERY_INTERFACE (253)
    'query_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0, 'radius_urr':
 0, 'bearer_urr': 0, 'sess_urr': 0}

    PFCP_IE_RECALCULATE_INTERFACE (264)
    'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0,
'radius_urr': 0, 'bearer_urr': 0, 'sess_urr': 0}


        MESSAGE BUFFER:
                2134 0047 F000 0000 0000 0002 0000 0304
                00E2 001C 0100 012A 060A 6926 860D 1821
                6354 092B 2163 5400 12D6 870A 1552 D904
                004D 0008 0051 0004 0000 0037 0031 0001
                0400 FD00 0110 0108 0001 10
```

Service Condition Change Reasons

Following are the service condition change reasons for the ULI change.

- If the TAI has changed in ULI, ServiceConditionChange reason in CDR is “TaiChange”
- If ECGI has changed in ULI, ServiceConditionChange reason in CDR is “EcgiChange”
- If both TAI and ECGI changes in ULI, the ServiceConditionChange reason in CDR is a generic “UserLocationChange”

ULI Information sent at CDR and SDF Container Levels

The following table describes scenarios and its behavior for ULI information sent at CDR and SDF container level.

PreCondition	Scenarios	Expected Behaviour
Maxlosdv 1 CSR **with ULI** Bearer threshold 60 seconds **ULI** Trigger **enable**	Attach with **ULI1** Bearer usage received for Time threshold MBR with **ULI2** Bearer usage received for Time threshold MBR with **ULI3** Bearer usage received for Time threshold Detach	On N4 Query for ULI Information change happens with **offline** bit set for offline. After receiving first Bearer usage, CDR and SDF containers are sent with **ULI1**. After receiving SDF usage for **1st MBR**, CDR and SDF containers are sent with **ULI1**. After receiving 2nd bearer usage, CDR with **ULI1** and SDF containers with **ULI2** are sent. After receiving SDF usage for **2nd MBR**, CDR and SDF containers are sent with **ULI2**. After receiving 3rd bearer usage, CDR with **ULI2** and SDF containers with **ULI3** are sent. For terminate usage report during **detach**, CDR and SDF Containers are sent with **ULI3**.

Maxlosdv 1 CSR **without ULI** Bearer threshold 60 seconds **ULI** Trigger **enable**	Attach **without ULI** Bearer usage received for Time threshold MBR with **ULI1** Bearer usage received for Time threshold MBR with **ULI2** Bearer usage received for Time threshold Detach	On N4 Query for ULI Info change happens with **offline** bit set for offline. After receiving 1st Bearer usage, CDR and SDF containers are sent **without ULI**. After receiving SDF usage for **1st MBR**, CDR and SDF containers are sent **without ULI** After receiving second Bearer usage, CDR **without ULI** and SDF containers with **ULI1** are sent. After receiving SDF usage for second **MBR**, CDR and SDF containers are sent with **ULI1**. After receiving third Bearer usage, CDR with **ULI1** and SDF containers with **ULI2** are sent. For terminate usage report during **detach**, CDR and SDF containers are sent with **ULI2**.
Maxlosdv 1 CSR **with ULI** Bearer threshold 60 seconds **Suppress zero cdrs** **ULI** Trigger **enable**	Attach with **ULI1** MBR with **ULI2 and zero usage(no traffic, zero volume) received** MBR with **ULI3 and zero usage(no traffic, zero volume) received** Zero usage(no traffic, zero volume) received for **Time threshold** Detach with **traffic data**	On N4 Query for ULI Information change happens with **offline** bit set for offline. For terminate usage report during **detach**, CDR with **ULI1** and SDF containers with **ULI3** are sent.
Maxlosdv 3 CSR with ULI Bearer threshold 60 seconds **ULI** Trigger **enable**	Attach with **ULI1** MBR with **ULI2** and SDF **usage zero(**no traffic, zero volume) MBR with **ULI3** and SDF **usage zero**(no traffic, zero volume) MBR with **ULI4** and received **2 SDF usages** MBR with **ULI5** and received **3 SDF usages** Detach with 2 SDF usages	On N4 Query for ULI information change happens with **offline** bit set for offline. After receiving **SDF usages for 4th MBR**, one CDR with **ULI1** and 3 SDF containers(**SDF1** with **ULI3**, **SDF2** with **ULI3** and **SDF3** with **ULI4)** are sent After receiving **terminate** usage, **2 CDR**s with SDF containers are sent. **1st CDR** with **ULI4** and 3 SDF containers(**SDF4** with **ULI4**, **SDF5** with **ULI4** and **SDF6** with **ULI5**) **2nd CDR** with **ULI5** and one SDF containers(**SDF7** with **ULI5**).

Maxlosdv 1 CSR **with ULI** Bearer threshold 60 seconds **ULI** Trigger **disable**	Attach with **ULI1** Bearer usage received for Time threshold MBR with **ULI2** Bearer usage received for Time threshold MBR with **ULI3** Bearer usage received for Time threshold Detach	On N4 Query for User Location information change does not happen for offline. All CDR and SDF container are sent with **ULI1**
Maxlosdv 1 CSR **without ULI** Bearer threshold 60 seconds **ULI** Trigger **disable**	Attach **without ULI** Bearer usage received for Time threshold MBR with **ULI1** Bearer usage received for Time threshold MBR with **ULI2** Bearer usage received for Time threshold Detach	On N4 Query for User Location information change does not happen for offline. All CDR and SDF container are sent **without ULI**.

Change Notification

The following call flow and procedure descibes Change Notification in the SMF.

Figure 150: Call Flow for Change Notification

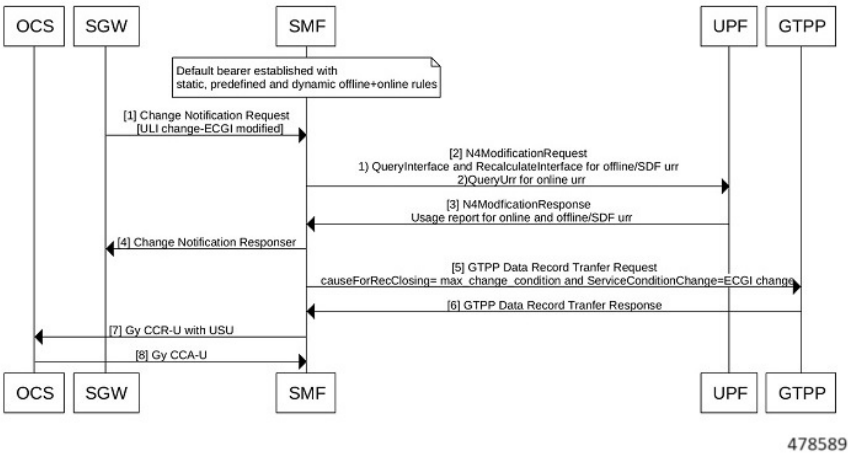


Table 236: Call Flow Description for Change Notification Change

Step	Description
Note	Default Bearer is established successfully and an initial attach happens with dynamic, static,and predefined rules.
1	S-GW sends Change notification request to SMF. For example, the change notification is sent with ULI change-ECGI modified.
3	N4 modification request is sent with the following details: • QueryUrr for online URR • QueryInterface and RecalculateInterface for offline/SDF urr
5	SMF receives N4 modification response from UPF with the following details: • UsageReport for SDF URRs • UsageReport for offline and online URRs
6	SMF sends GTPP Data Record Transfer request to the GTPP with max-change_condition.
6	SMF receives the GTPP Data Record Transfer Response.
7	UPF sends Gy CCR-U message with usage received to the OCS .
8	SMF receives Gy CCA-U from OCS

Query Interface and Recalculate Interface IEs

The following table describes Query Interface and Recalculate Interface IEs.

Trigger	N4 Query Interface	N4 Recalculate Interface	N4 Query URR
Rulebase Change	Query Interface with **-bearer_urr': 1** "offline_urr": 0 “online_urr”:0 “radius_urr”:0 UPF will report Bearer level usage along with SDF level usage.	Recalculate Interface **-"bearer_urr": 1** **"offline_urr": 1** “online_urr”:0 “radius_urr”:0	**NA**

Secondary RAT Usage Limit	Query Interface with **-bearer_urr': 1** "offline_urr": 0 “online_urr”:0 “radius_urr”:0 UPF will report Bearer level usage along with SDF level usage.	Recalculate Interface - **"bearer_urr": 1** **"offline_urr": 1** “online_urr”:0 “radius_urr”:0	
Record Closing trigger- Example: time zone change	Query Interface with **-bearer_urr': 1** "offline_urr": 0 “online_urr”:0 “radius_urr”:0 UPF will report Bearer level usage along with SDF level usage.	Recalculate Interface - "**bearer_urr": 1** **"offline_urr": 1** “online_urr”:0 “radius_urr”:0	online and radius
SDF Level Query - Ex: QOS Change	Query Interface with -bearer_urr': 0 **"offline_urr": 1** “online_urr”:0 “radius_urr”:0 UPF will report all SDF level usage. SMF needs to send recalculate in same N4 to reset thresholds of SDF level URR	Recalculate Interface - "bearer_urr": 0 **"offline_urr": 1** “online_urr”:0 “radius_urr”:0	Online and radius
Recalculate Bearer Level Limits because of Record Closure - Max change condition	**NA**	UPDATE URR: Type: 13 Value: URR ID: Type: 81 Value: 0x80000002 RECALCULATE MEASUREMENT: Type: 216 RCVOL: 1 RCDUR: 1	NA

Individual URR Query - Currently no use case in future will need this.	Query URR : **Value : <XYZ>**	UPDATE URR: Type: 13 Value: URR ID: Type: 81 **Value: XYZ** RECALCULATE MEASUREMENT: Type: 216 RCVOL: 1 RCDUR: 1	NA

Configuring Gz Triggers

To configure Gz triggers, use the following sample configuration.

```
config
   active-charging service service_name
      charging-action charging_action
        egcdr  losdv-max-containers   service-data-flow triggers {
ms-timezone-change [ true | false ] | qos-change [ true | false ] |
uli-change [ true | false ] }
   end
```

NOTES:

- **egcdr losdv-max-containers** : Configure maximum number of LoSDV containers in one EGCDR. The **losdv-max-containers** value must be an integer in the range of 1–255. By default the value is 1.
- **egcdr service-data-flow** : Configure service data flows.
- **egcdr triggers { ms-timezone-change [true | false] | qos-change [true | false] | uli-change [true | false] }**
  - **egcdr triggers**: Configure list of triggers for CDR. By default, the following triggers are enabled:
    - **triggers ms-timezone-change [true | false]**: Enable or disable MS Timezone trigger for CDR default.
    - **triggers qos-change [true | false]**: Enable or disable QoS change trigger for CDR default.
    - **triggers uli-change [true | false]**: Enable or disable User Location change trigger for CDR default.

Gz Default Bearer Modification

Feature Description

SMF supports PCRF-initiated modification of default bearer through Gx CCR-U and Gx RAR. You can perform the following functions:

- Add rules to the Default Bearer

- Delete rules from the Default Bearer
- Rulebase Modification
- Default-bearer QoS change
- APN-AMBR change

How it Works

This section describes the call flows pertaining to the Gz Default Bearer Modification feature in SMF.

Call Flows

Adding Offline Rules to Default Bearer

Bearer level URR ID is created only once for each bearer. The following call flow and procedure describes various dynamic rule addition scenarios.

Figure 151: Call Flow for Adding Offline Rules to Default Bearer

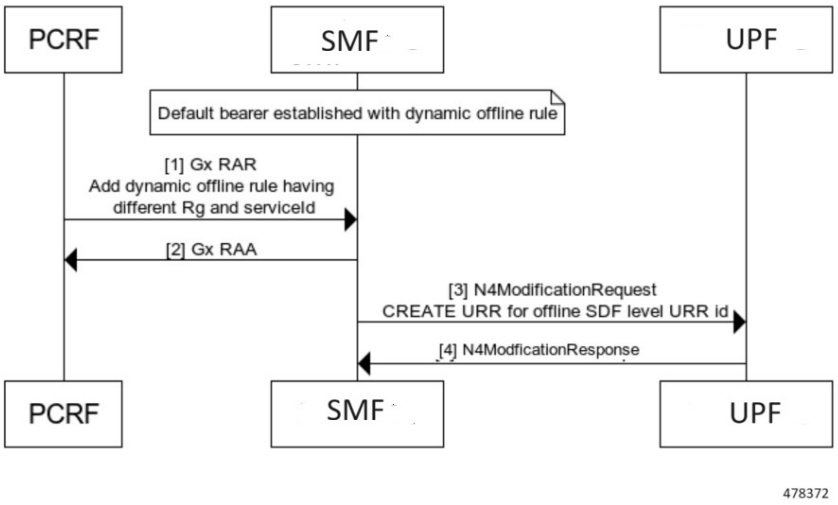


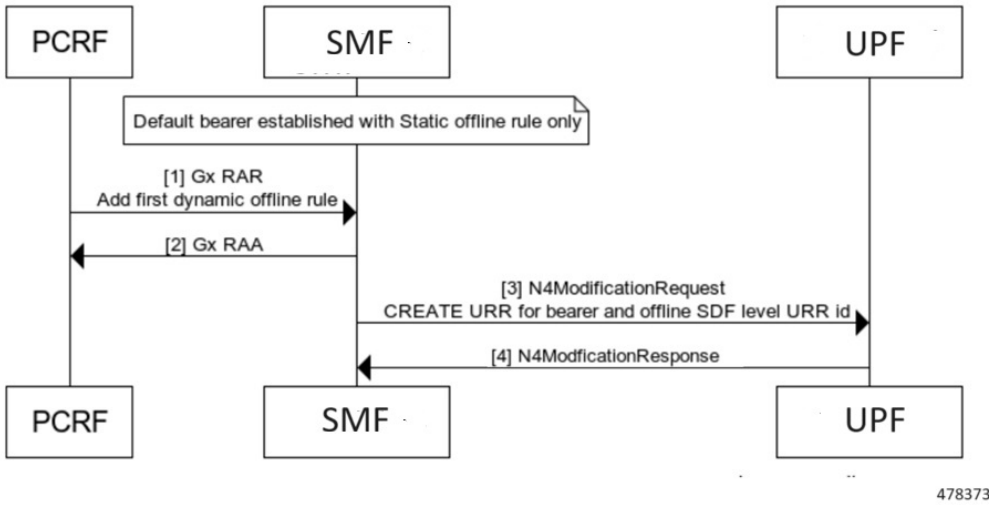
Table 237: Call Flow Description for Adding Offline Rule to Default Bearer

Step	Description
Note	Ensure that the initial attach is successfully done with dynamic offline rule.
1	PCRF adds a new dynamic offline rule with different RG and service ID through Gx RAR.
2	SMF sends Gx RAA to PCRF.

Step	Description
3	SMF sends N4 Modification Request with CREATE_URR for offline SDF URR to UPF. The following conditions must be met: • PFCP_IE_URR_ID should have a unique offline URR ID • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD should have eG-CDR threshold values that are configured in the GTPP profile. • PFCP_IE_MEASUREMENT_METHOD have both volume and duration bit set. • PFCP_IE_REPORTING_TRIGGERS have *lisua* bit set. • Linked to Bearer URR ID.
4	UPF sends N4 Modification response.

Adding First Dynamic Rule

Figure 152: Call Flow for First Dynamic Rule



Addition

Table 238: Call Flow Description for Adding First Dynamic Rule

Step	Description
1	Ensure that the initial attach is successfully done with default bearer having single static offline rule.
2	PCRF adds first dynamic offline rule through Gx RAR.
3	SMF sends Gx RAA to PCRF.

Step	Description
3	SMF sends N4 Modification Request towards UPF: • CREATE_URR for default bearer level URR: • PFCP_IE_URR_ID is set to 0x80000002 for default bearer level URR. • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD have eG-CDR threshold values that are configured in the Rulebase profile. • PFCP_IE_MEASUREMENT_METHOD has both volume and duration bit set. • CREATE_URR for offline SDF level URR: • PFCP_IE_URR_ID has a unique offline URR ID. • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD have eG-CDR threshold values that are configured in the GTPP profile. • PFCP_IE_MEASUREMENT_METHOD has both volume and duration bit set. • PFCP_IE_REPORTING_TRIGGERS have *lisua* bit set. • Linked to Bearer URR ID.
4	UPF sends N4 Modification response.

Adding First Dynamic Rule after Usage Report

Figure 153: Call Flow for Adding First Dynamic Rule after Usage Report

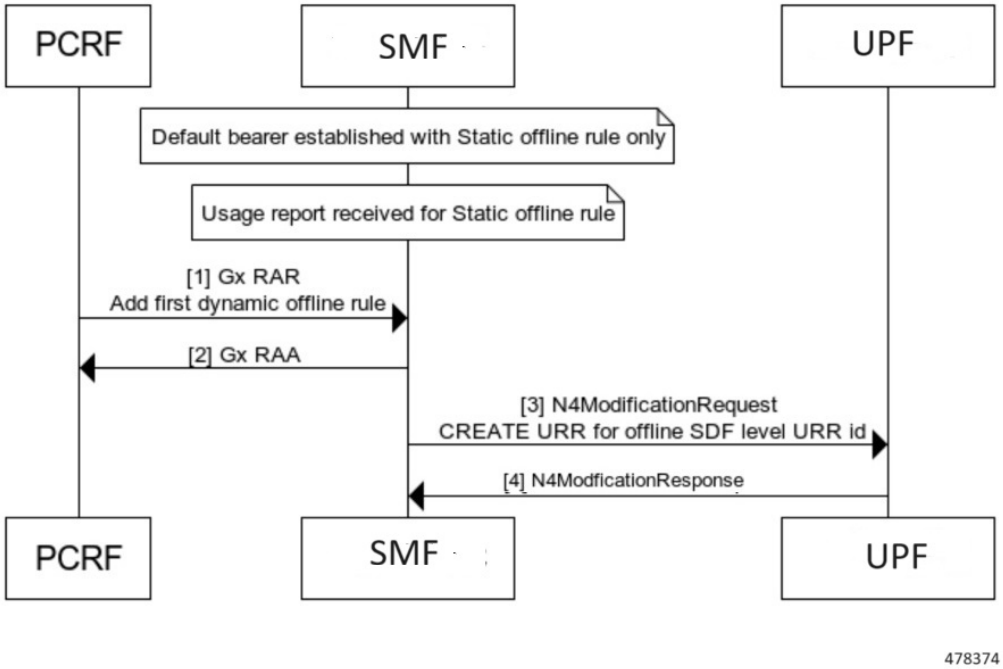


Table 239: Call Flow Description for Adding First Dynamic Rule after Usage Report

Step	Description
Ensure that the initial attach is successfully done with the default bearer having a single static offline rule. Usage report is processed successfully for static offline rule.	
2	PCRF adds the first dynamic offline rule through Gx RAR.
3	SMF sends Gx RAA to PCRF.
3	SMF sends N4 Modification Request toward UPF: • CREATE_URR for offline SDF level URR: • PFCP_IE_URR_ID has a unique offline URR ID. • PFCP_IE_VOLUME_THRESHOLD and PFCP_IE_TIME_THRESHOLD have eG-CDR threshold values that are configured in the GTPP profile. • PFCP_IE_MEASUREMENT_METHOD has both volume and duration bit set. • PFCP_IE_REPORTING_TRIGGERS have *lisua* bit set. • Linked to Bearer URR ID.
4	UPF sends N4 Modification response.

Deleting Rules from Default Bearer

The following call flow and procedure describes Rules deletion from the Default Bearer.

Figure 154: Call Flow for Deleting Rules from Default Bearer

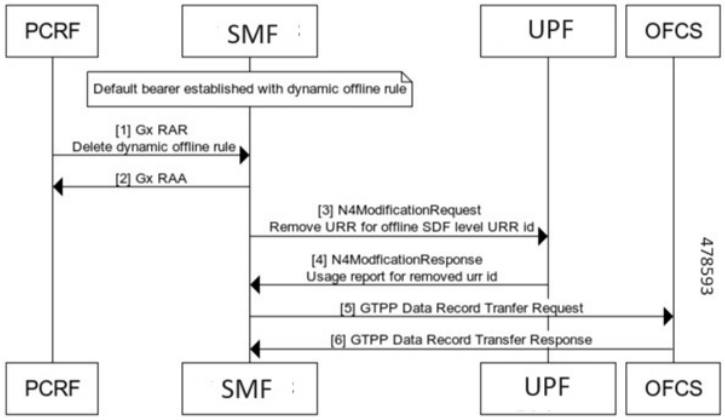


Table 240: Call Flow Description for Deleting Rules from Default Bearer

Step	Description
1	Ensure that the initial attach is successfully done with dynamic offline rule.

Step	Description
2	PCRF removes dynamic offline rule through Gx RAR.
3	CnPGW-C sends Gx RAA to PCRF.
4	N4 Modification Request with REMOVE_URR for offline SDF URR is sent towards CnPGW-U.
5	CnPGW-U sends the following N4 Modification response: • PFCP_IE_USAGE_REPORT_MOD_RES received for removed URR • PFCP_IE_USAGE_REPORT_MOD_RES with 'termr' set

6	OFCS sends GTPP record transfer response. For example,
	`Maxlosdvcontainer: 1.GTPP Data Record Transfer Request is sent with single Service record for the removed URR`
	`causeForRecClosing: Maximum change condition`
	`serviceConditionChange:ServiceStop`

QoS and APN-AMBR Change of Default Bearer

The following section describes QoS and APN-AMBR change for Default Bearers.

Figure 155: Call Flow for QoS/APN-AMBR with only Offline Rules Change

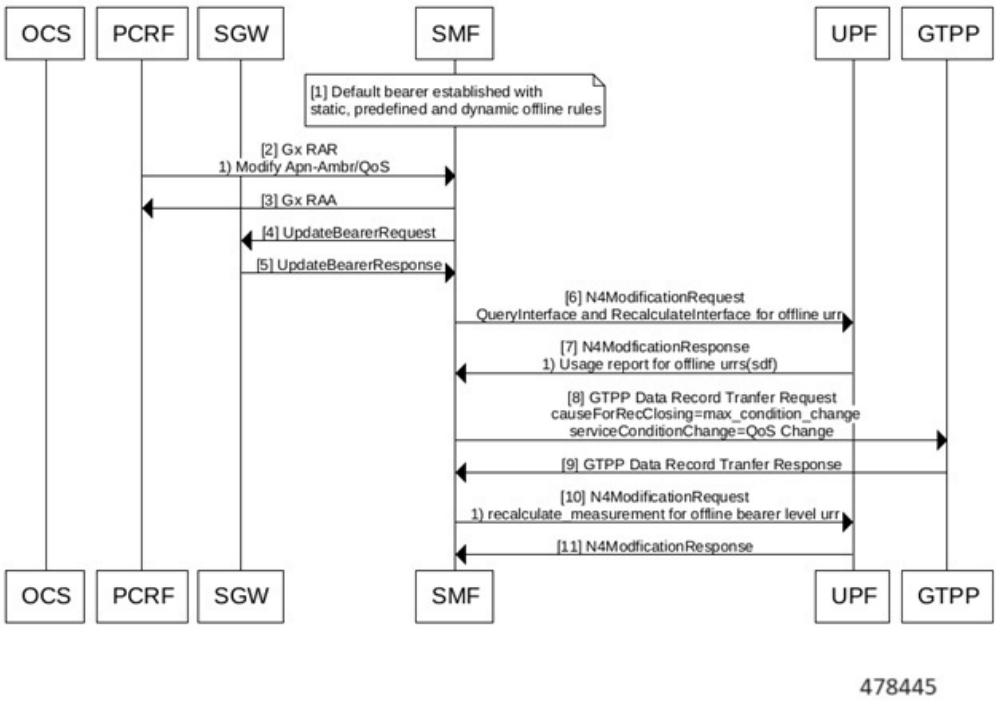


Table 241: Call Flow Description for QoS/APN-AMBR with only Offline Rules Change

Step	Description
1	Establish default dearer attach with dynamic, static, and predefined Offline rules. SMF must have CHANGE_IN_QOS, CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE triggers configuration.
2	PCRF sends GxReAuthRequest with Apn-Ambr or QoS change. For example,change request can be sent for: • Default-Bearer QoS (QCI, ARP) • Apn-Ambr (Uplink or Downlink)
3	SMF sends GxReAuthAnswer to the PCRF.
4	SMF sends Update Bearer Request to the S-GW.
5	S-GW sends Update Bearer Response to the SMF.
6	UPF receives the following N4 Modification Request from SMF: • QueryInterface with offline_urr set for SDF URR • Re-calculate Interface with offline_urr set for SDF URR
7	SMF receives N4Modification response from UPF. For example, SMF receives UsageReport response for SDF URRs.
8	SMF sends GTPP Data Record Transfer request only if there are Maxlosdvcontainer configured limit hits.
9	SMF receives GTPP Data Record Transfer Response.
10	SMF sends N4 Modification Request with Recalculate_measurement for offline Bearer level URR to UPF.
11	UPF sends N4 Modification Response to SMF.

Figure 156: Call Flow for Offline and Online Rules Change

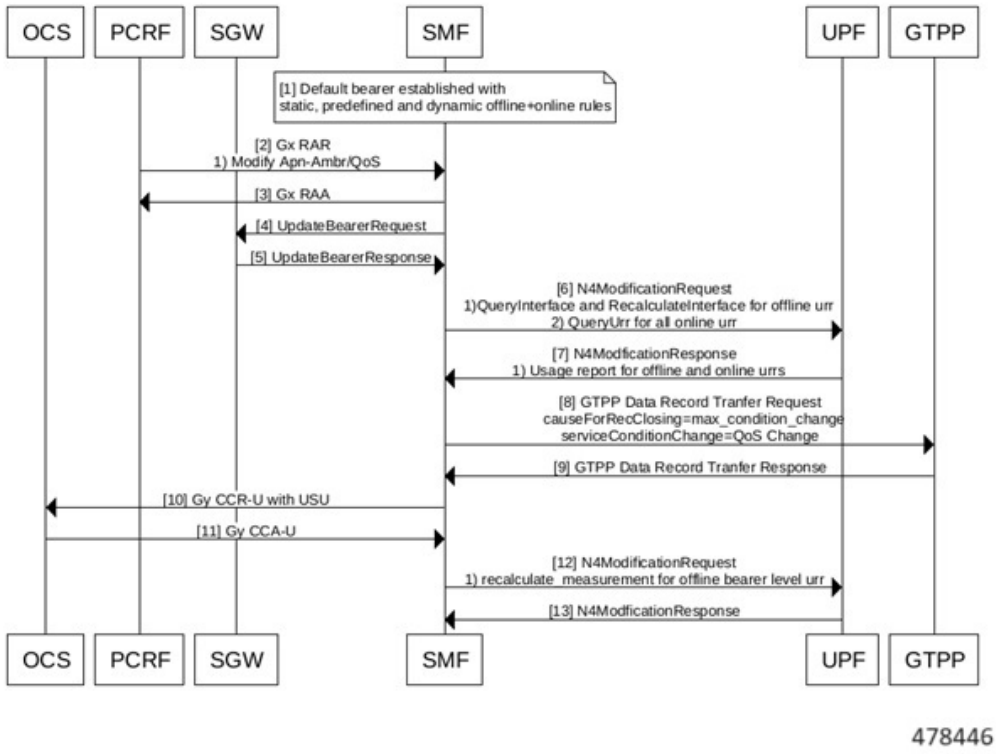


Table 242: Call Flow Description for QoS/APN-AMBR with Offline and Online Rules Change

Step	Description
1	Establish default bearer attach with the following dynamic, static, and predefined offline rules: • OCS arms Gy-triggers such as CHANGE_IN_QOS, CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE for online rule. • SMF must have CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE trigger configuration
2	PCRF sends GxReAuthRequest with APN-AMBR or QoS change. For example, change request can be sent for: • Default-Bearer QoS (QCI, ARP) • Apn-Ambr (Uplink or Downlink)
3	SMF sends GxReAuthAnswer to the PCRF.
4	SMF sends Update Bearer Request to the S-GW.
5	S-GW sends Update Bearer Response to the SMF.

Step	Description
6	UPF receives the following N4 Modification Request from SMF: • QueryInterface with offline_urr set for SDF URR • Re-calculate Interface with offline_urr set for SDF URR
7	SMF receives N4Modification response from UPF. For example, SMF receives UsageReport response for SDF URRs.
8	SMF sends GTPP Data Record Transfer request only if there are Maxlosdvcontainer configured limit hits.
9	SMF receives GTPP Data Record Transfer Response.

10	SMF sends Gy CCR-U to OCS with usage received from UPF in USU. For example,
	`QoS Change => Reporting-Reason with RATING_CONDITION_CHANGE (6), Trigger - CHANGEINQOS_ANY (2).`
	`Apn-Ambr Change => Reporting-Reason with RATING_CONDITION_CHANGE (6), Trigger - CHANGEINQOS_APN_AGGREGATE_MAXIMUM_BIT_RATE (24).`

11	SMF receives Gy CCA-U received from OCS.
12	SMF sends N4 Modification Request with Recalculate_measurement for Offline Bearer level URR to UPF.
13	UPF sends N4 Modification Response to SMF.

QoS Sent in CDR

All the QoS information is sent only at SDF Container level. The APN-AMBR value is sent as **zero** in either maxRequestedBandwithUL or maxRequestedBandwithDL CDR SDF container.

PreCondition	Scenarios	Expected Behavior
Maxlosdv 1 Attach **with Gx** SDF threshold 60 seconds **QoS** trigger **enable**	Attach with Gx (QoS Info - **QoS1**) SDF usage received for Time threshold Gx RAR for QoS change - **QoS2** SDF usage received for Time threshold Gx RAR for QoS change - **QoS3** SDF usage received for Time threshold Detach	On N4 Query for QoS Information change happens with **offline** bit set for offline. After receiving 1st SDF usage, CDR SDF containers is sent with **QoS1** After receiving SDF usage for **1st RAR**, CDR SDF containers is sent with **QoS1** After receiving 2nd SDF usage, CDR SDF containers is sent with **QoS2** After receiving SDF usage for **2nd RAR**, CDR SDF containers is sent with **QoS2** After receiving 3rd SDF usage, CDR SDF containers is sent with **QoS3** For terminate usage report during detach, CDR SDF Containers is sent with **QoS3**

Maxlosdv 1 Attach **without Gx** Bearer threshold 60 seconds **QoS** trigger **enable**	Attach **without Gx (default rule QoS**) SDF usage received for Time threshold Bearer usage received for volume threshold Detach	All CDR SDF container is sent with attach time **default** rule QoS information.
Maxlosdv 1 Attach **with Gx** SDF threshold 60 seconds **QoS** trigger **disable**	Attach with Gx (QoS Info - **QoS1**) Bearer usage received for Time threshold Gx RAR for QoS change - **QoS2** Bearer usage received for Time threshold Gx RAR for QoS change - **QoS3** Bearer usage that is received for Time threshold Detach	On N4 Query for QoS Information change does not happen for offline. All CDR SDF containers are sent with attach time QoS info - **QoS1**
Maxlosdv 1 Attach **without Gx** Bearer threshold 60 seconds **QoS** trigger **disable**	Attach **without Gx (default rule QoS**) SDF usage that is received for Time threshold Bearer usage that is received for volume threshold Detach	All CDR and SDF containers are sent with attach time **default** rule QoS information

Rulebase Modification

The following call flow and procedure describes Rule base modification.

Figure 157: Call Flow for Rulebase Modification

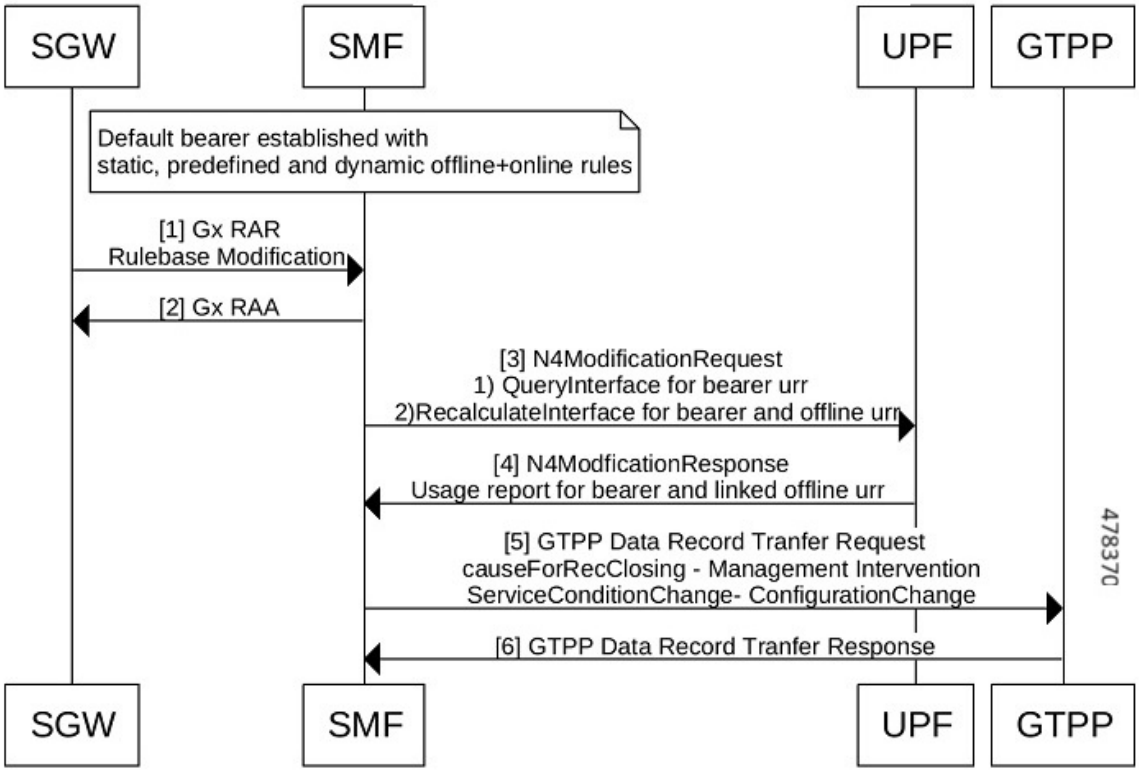


Table 243: Call Flow Description for Rulebase Modification

Step	Description
1	Ensure that the initial attach is successfully done with static, predefined, and dynamic rules.
2	S-GW modifies rulebase through Gx RAR to the SMF.
3	SMF sends Gx RAA to the S-GW.
4	SMF sends following N4 Modification Request towards UPF: • CREATE PDR for new rulebase • REMOVE PDR for old rulebase and predefined rule • QUERY INTERFACE with bearer_urr bit set • RECALCULATE INTERFACE with bearer_urr and offline_urr bit set
5	UPF sends the following N4 Modification response to the SMF: • PFCP_IE_USAGE_REPORT_MOD_RES for bearer level URR with ‘immer’ flag set • PFCP_IE_USAGE_REPORT_MOD_RES for all SDF offline URRs with ‘liusa’ flag set

Step	Description
6	SMF sends the GTPP Data Record Transfer Request to the SMF. `For example, GTPP Data Record Transfer Request is sent with ForRecClosing: Management Intervention serviceConditionChange:Configuration change`
7	GTPP confirms that GTPP Data Record Transfer Response received to the SMF.

Note When billing record is changed through rulebase modification, the Bearer URR is queried if atleast one of the offlline rule (dynamic, static, or activated predefined rule) is currently installed. For example,

- If an attach is done with billing record disabled and no offline rules present. When billing record is modified to enabled through rulebase change, no Bearer URR is queried as no offline rules were present in the system.
- If a new rulebase has EGCDR billing record disabled, exsisting dynamic offline rules are not removed and usage report for the same continues. However, when new offline rule is added, offline URR does not get created for the same and marked as validation failure because of billing record disable.

Handling Periodic Report of Secondary RAT Usage

Table 244: Feature History

Feature Name	Release Information	Description
Periodic Report of Secondary RAT Usage	2023.04	This feature allows SMF to handle periodic Secondary RAT data volume report messages from the MME over the S5 or S8 interface in the Modify Bearer Request, Change Notification Request, Delete Session Request, and Delete Bearer Response **Default Setting**: Disabled – Configuration required to enable

Feature Description

The SMF and UPF track the usage on eNB to differentiate the NR or LTE usage for NSA devices. SMF receives usage data report on S5 interface in various messages, which it reports usage towards OFCS server along with offline usage report.

The SMF handles the periodic Secondary RAT data volume report messages from the MME over the S5 or S8 interface in the Modify Bearer Request, Change Notification Request, Delete Session Request, and Delete Bearer Response based on the Intended Receiver PGW-C (IRPGW) flag. SMF retains the Usage-Report if IRPGW = 1.

The SMF supports multiple instances of Secondary RAT Usage Data Report IEs. It stores reports until they are sent out to OFCS based on the triggers. SMF sends out the stored secondary RAT usage data report through gtpp-ep endpoint when any of the charging triggers are met. You can configure the maximum number of stored secondary RAT usage reports under Charging Profile. SMF sends the stored secondary RAT usage data report along with offline usage report when CDR is closed due to offline usage report.

How it Works

The following figure describes the call flow for Periodic Secondary RAT Usage Report.

Figure 158: Call Flow for Periodic Secondary RAT Usage

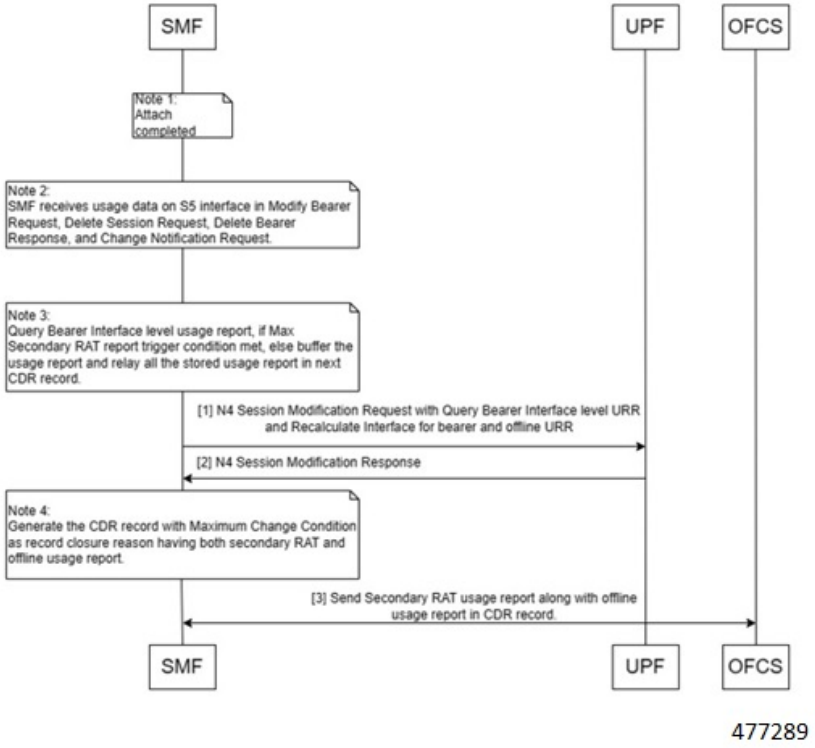


Table 245: Call Flow Description for Periodic Secondary RAT Usage

Step	Description
Note	Ensure that following conditions are met: • Attach procedure is complete. • SMF receives usage data on S5 interface in Modify-Bearer-Request, Delete-Session-Request, Delete-Bearer-Response and Change-Notification-Request. For more information, refer the Sample CDR Output, on page 645. • Handles Query bearer interface level usage report if Max Secondary RAT report trigger condtion is met. Else, buffers the usage report and relays all the stored usage report in next CDR record.

Step	Description

1	SMF sends N4 Session modification request with query Bearer interface level URR and recalculate interface for Bearer and offline URR.
	Following parameters are sent:
	• QueryInterface with **bearer_urr** is set for Bearer URR. For example:
	`PFCP_IE_QUERY_INTERFACE (253)`
	`'query_interface' : {'spare_3bit': 0, 'offline_urr': 0, 'online_urr': 0, 'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}`
	• Recalculate Interface with **offline_urr** and **bearer_urr** is set for SDF URR
	`PFCP_IE_RECALCULATE_INTERFACE (264)`
	`'recalculate_interface' : {'spare_3bit': 0, 'offline_urr': 1, 'online_urr': 0, 'radius_urr': 0, 'bearer_urr': 1, 'sess_urr': 0}`

2	UPF sends the N4 session modification response along with Bearer and linked SDF Usage Report.
3	Generates the CDR record with Maximum Change Condition as CDR Record Closure Reason, on page 644 contains both secondary RAT and offline usage report.
4	SMF sends the CDR record towards OFCS with offline usage report.

CDR Record Closure Reason

Following table describes the CDR Record Closure reason and Service Condition reason in various uses cases of Secondary Rat Usage.

Table 246: CDR Record Closure Reason

Trigger Type	Secondary RAT Limit Hit	Query on N4	SDF Closing Reason	Record Closing Reason	Metric Incremented
SDF Level Query **Example**: ULI Change Trigger	TRUE	Bearer Level query **Example**: ULI Change Trigger Reason	Trigger Reason	Maximum Change Condition	Yes
Bearer Level Query **Example**: Timezone Trigger	TRUE	Bearer Level query	Trigger Reason **Example** : Timezone Trigger Reason	Trigger Reason **Example**: Timezone Trigger Reason	No
No Trigger Hit	TRUE	Bearer Level query	Service Specific Unit Limit	Maximum Change Condition	Yes

Configuring Secondary RAT Usage Limit

Use the following sample configuration to configure secondary RAT usage reports before sending to OFCS.

```
config
  profile charging profile_name
    max-secondary-rat-reports report_range
    exit
```

NOTES:

- **profile charging** *profile_name*: Enter the Charging Profile configuration mode.
- **max-secondary-rat-reports** *report_range*: Configure the maximum number of secondary RAT usage reports to trigger GTPP (Gz) update. *report_range* must be an integer in the range of 0–50. The recommended value for secondary RAT usage limit for **max-secondary-rat-reports** is 25.

Note If the accumulated Secondary RAT usage exceeds the configured limit, the number of Secondary RAT usages exceeding the limit gets combined in a single usage.

Sample CDR Output

The following is the sample output for Secondary RAT Data Usage in the Change Notification Request.

```
CHANGE NOTIFICATION REQUEST" (38)
'Teid'             : 0x4
'Length'           : 86
'Sequence Number'  : 3
'Number of IEs'    : 6
    "GTPV2_IE_IMSI" (1)
          'Length' : 8
            'inst' : 0
            'imsi' : 123456789012345

       IE BUFFER:
                0100 0800 2143 6587 0921 43F5
    "GTPV2_IE_RAT_TYPE" (82)
          'Length' : 1
            'inst' : 0
        'rat_type' : E-Utran (6)
       IE BUFFER:
                5200 0100 06
    "GTPV2_IE_ULI" (86)
          'Length' : 13
            'inst' : 0
             'uli' : {'spare': 0, 'lai': 0, 'ecgi': 1, 'tai': 1, 'rai': 0, 'sai': 0, 'cgi':
 0, 'tai-mcc': 123, 'tai-mnc': 456, 'tai-tac': 2346, 'ecgi-mcc': 123, 'ecgi-mnc': 456,
'ecgi-spare': 0, 'ecgi-eci': 1234567}
       IE BUFFER:
                5600 0D00 1821 6354 092A 2163 5400 12D6
                87
    "GTPV2_IE_PGW_S5/8_GTPC_IP_ADDR" (74)
          'Length' : 4
            'inst' : 0
      'ip_address' : 10.11.12.13
       IE BUFFER:
                4A00 0400 0A0B 0C0D
    "GTPV2_IE_LBI" (73)
          'Length' : 1
```

```
          'inst' : 0
         'spare' : 0
        'eps_id' : 5
      IE BUFFER:
               4900 0100 05
   "GTPV2_IE_SECONDARY_RAT_USAGE_DATA_REPORT" (201)
        'Length' : 27
          'inst' : 0
   'secondary_rat_usage_data_report' : {'irsgw': 0, 'irpgw': 1, 'sec_rat_type': 0, 'ebi':
 5, 'start_timestamp': 3890790208, 'end_timestamp': 3890790218, 'usage_data_dl': 100,
'usage_data_ul': 100}
      IE BUFFER:
               C900 1B00 0100 05E7 E8BF 40E7 E8BF 4A00
               0000 0000 0000 6400 0000 0000 0000 64
       MESSAGE BUFFER:
               4826 0056 0000 0004 0000 0300 0100 0800
               2143 6587 0921 43F5 5200 0100 0656 000D
               0018 2163 5409 2A21 6354 0012 D687 4A00
               0400 0A0B 0C0D 4900 0100 05C9 001B 0001
               0005 E7E8 BF40 E7E8 BF4A 0000 0000 0000
               0064 0000 0000 0000 0064
```

The following is the sample output for GTPP Record with Secondary RAT Usage.

```
CDR ELEMENTS FOLLOW
  recordType                          PGWRECORD
  servedIMSI                          123456789012345
  p_GWAddress                         10.0.2.15
  chargingID                          4
  servingNodeAddress                  10.105.34.80
  accessPointNameNI                   intershat
  pdpPDNType                          IPV4
  servedPDPPDNAddress                 1.1.4.3
  dynamicAddressFlag                  TRUE
  recordOpeningTime                   230608091158+0000
  duration                            2
  causeForRecClosing                  Maximum Change Condition
  recordSequenceNumber                1
  nodeID                              1000acs1
  localSequenceNumber                 7
  apnSelectionMode                    MS Provided Subscription Not Verified
  servedMSISDN                        223310101010101
  chargingCharacteristics             Flat (0x1234)
  chChSelectionMode                   SGSN Supplied
  servingNodePLMNIdentifier           121, 100
  rATType                             eUTRAN
  mSTimeZone                          +04:30 - Daylight savings +2
  userLocationInformation
    Location Type                   TAI
    MCC                               123
    MNC                               456
    TAC                               0x92A
    Location Type                   ECGI
    MCC                               123
    MNC                               456
    ECI                               0x012D687

    ratingGroup                         10
    chargingRuleBaseName                RULE-BASE-1
    localSequenceNumber                 1
    timeUsage                           70
    serviceConditionChange              Service specific Unit Limit
     qCI                                 5
     maxRequestedBandwithUL              0
```

```
    maxRequestedBandwithDL              0
    guaranteedBitrateUL                 0
    guaranteedBitrateDL                 0
    aRP                                 8
   servingNodeAddress                  10.105.34.80
   datavolumeFBCUplink                 1001
   datavolumeFBCDownlink               1001
   timeOfReport                        230608091200+0000
   userLocationInformation
     Location Type                    TAI
     MCC                               123
     MNC                               456
     TAC                               0x92A
     Location Type                    ECGI
     MCC                               123
     MNC                               456
     ECI                               0x012D687

 servingNodeType                      GTPSGW
 subscriptionIDType                   3
subscriptionIDData                  0123456789012345@nai.epc.mnc456.mcc123.3gppnetwork.org

 p_GWPLMNIdentifier                   123, 456
 startTime                            230608091158+0000
 pDNConnectionID                      4

listOfRANSecondaryRATUsageReports

  RANSecondaryRATUsageReport
   dataVolumeUplink                   100
   dataVolumeDownlink                 100
   rANStartTime                       230418070328+0000
   rANEndTime                         230418070338+0000
   secondaryRATType                   New Radio 5G

  RANSecondaryRATUsageReport
   dataVolumeUplink                   400
   dataVolumeDownlink                 500
   rANStartTime                       230418070455+0000
   rANEndTime                         230418070615+0000
   secondaryRATType                   New Radio 5G
```

Configuring DCNR

To enable SMF to support the DCNR capability for the sessions handled using the DNN profile, use the following sample configuration:

```
config
   profile dnn profile_name  intershat dcnr
      dcnr { false | true }
      exit
```

NOTES:

- **profile dnn** *profile_name*: Specify the DNN profile name. *profile_name* must be an alphanumeric string.
- **intershat dcnr** : Enables support for dual connectivity with new radio.

Note The Secondary RAT usage report processing is done if the DCNR configuration is enabled, and UE has “UP plane Indication IE” in the Create Session Request.

- **dcnr { false | true }**:
  - **false**: Configure the DNN profile to have DCNR flag set to false. The DCNR configuration is disabled by default.
  - **true**: Configure the DNN profile to have DCNR flag set to true.

    This configuration enables the SMF to support DCNR capability. When the DCNR capability is enabled, the UE sends the DCNR flag to indicate that it supports dual connectivity.

Support for EGCDR Final Record Closing Cause

Table 247: Feature History

Feature Name	Release Information	Description
EGCDR Final Record Closing Cause	2023.04	This feature allows you to send unique record closure reason for final CDR through CLI configuration.

Feature Description

By default, if multiple CDRs are generated for the end of a subscriber session, all the CDRs have the same cause for record closure.

The SMF through a CLI option closing-cause controls the cause for record closing in the final CDR. In case multiple CDRs are generated for the end of the subscriber session then final CDR record closure reason is set to NormalRelease and all other CDRs record closure reason is set to MaxChangeCondition.

Configuring Final Record Closure

Use the following command to configure final-record closing-cause.

```
config
   active-charging service service_name
      charging-action charging_action
         egcdr-final-record
            closing-cause [ same-in-all-partials | unique ]
  end
```

NOTES:

- **egcdr-final-record** : Configures the final CDR.
- **closing-cause** : Closing cause in case of the final CDR:
  - **same-in-all-partials** : Specifies that the same closing cause is to be included for multiple final CDRs.
  - **unique**: Specifies that the closing cause for final CDR is to be unique.

Suppress CDR with Zero Volume

Table 248: Feature History

Feature Name	Release Information	Description
Zero CDR Suppression Support on the Gz Interface	2023.04	This feature allows you to suppress CDR records based on the **egcdr suppress-cdrs zero-volume** CLI.

Feature Description

You can suppress CDR records in the following scenarios:

- If there is no volume usage based on the CLI configuration
- If the CDR is having zero volume and if it matches the configured trigger.
- If the CDR is having zero volume and it does not match the configured trigger. If the egcdr suppress-cdrs zero-volume CLI is not configured, a CDR without any SDF containers is sent.

Note If a session usage report from UPF contains a SDF level usage with zero volume, the SDF container is suppressed by default.

The egcdr suppress-cdrs zero-volume CLI is applicable only for call terminanation usage report or bearer level usage cases. For example, when a call gets terminated with zero volume report or if there is a bearer level Sync or Async usage report with zero volume, the CDR to be sent out or not is determined based on the CLI configuration.

Configuring Zero Suppression CDR

Using the following CLI configuration, to suppress the CDR records in case the CDR does not report any volume usage.

```
config
   active-charging service service_name
      charging-action charging_action
        egcdr suppress-cdrs zero-volume   triggers [ internal-trigger-cdr
 |  final-cdr | external-trigger-cdr ]
  end
```

NOTES:

- **egcdr suppress-cdrs zero-volume** : Suppress CDRs.
- **triggers** : Configures one of the list of triggers that can be used to suppress CDR with zero volume:
  - **egcdr suppress-cdrs zero-volume trigger internal-trigger-cdr** : Specifies that an Async volume usage reporting is from UPF through PFCP session usage report.
  - **egcdr suppress-cdrs zero-volume trigger final-cdr** : Specifies that a call is getting terminated.
  - **egcdr suppress-cdrs zero-volume trigger external-trigger-cdr** : Specifies that a Sync volume usage reporting is from UPF through Query URR.

N1/NAS Interface

The N1 interface is the reference point between the User Equipment (UE) and the Access and Mobility Management Function (AMF). This interface is used to transfer UE information, which is related to connection, mobility and sessions, to the AMF.

For session management, PDU sessions are established upon UE request, modified upon UE and 5GC request, and released upon UE and 5GC request through the NAS SM signalling. This signalling is exchanged over N1 interface between the UE and the SMF.

NAS Messages Compliance with Invalid Protocol Data Handling

Feature Description

The SMF is NAS messages compliant with invalid protocol data handling as defined in 3GPP TS 24.501 with this release.

How it Works

The NAS messages compliance with invalid protocol data handling feature works as follows:

- SMF ignores a NAS message that is too short to contain a complete message type information element (IE).
- SMF ignores a NAS message that is longer than the maximum limit as defined in the 3GPP specification.
- SMF ignores the IEs that are unknown in a NAS message.
- SMF ignores the IEs with incorrect sequence in a NAS message.
- If an information element with the T, TV, TLV, or TLV-E format repeats in a message with the unspecified repetition of the IE, then the SMF handles only the contents of the information element that appears first. In addition, SMF ignores the subsequent repetitions of the information element.
- SMF considers any optional IE with incorrect syntax in a message as an unavailable message.
- The network ignores any of the following messages and returns a status message with cause #100 “conditional IE error”:
  - When SMF receives a NAS message with a missing conditional IE error
  - When SMF receives an unexpected conditional IE error
  - When SMF receives a message with at least one syntactically incorrect conditional IE

NAS Messages Compliance and Invalid Protocol Data Handling

SMF complies with the following sections of the 3GPP specifications for the NAS messages compliance with invalid protocol data handling feature:

Message Too Short

SMF discards a NAS message whose size doesn't meet the minimum limit.

Following table lists the minimum limit for NAS messages that SMF receives from UE:

Table 249: Minimum Limit for NAS Messages

Number	NAS Message	Minimum Limit
1	PDU Session Establishment Request	6 octets
2	PDU Session Authentication Complete	4 octets
3	PDU Session Modification Request	4 octets
4	PDU Session Modification Complete	4 octets
5	PDU Session Modification Command Reject	5 octets
6	PDU Session Release Request	4 octets
7	PDU Session Release Complete	4 octets

Message Too Long

SMF discards a NAS message whose size doesn't meet the maximum limit.

The maximum size of a NAS message for NR that is connected to 5G Core Network is 9000 bytes.

Unknown IEs

SMF ignores unknown IEs in a NAS message.

Note SMF handles only the IEs relevant to a specific NAS message type. SMF ignores other IEs that are unknown to the message type.

Out of Sequence IEs

SMF ignores IEs that have incorrect sequence of mandatory IEs in a NAS message.

Repeated IEs

Sometimes SMF can receive an IE multiple times in a NAS message with no information on the repetition of IE. In such a case, SMF considers only the first occurrence of the repeated IE and ignores all the subsequent occurrences of the IE.

Syntactically Incorrect IEs

SMF ignores syntactically incorrect optional IEs in a NAS message.

Missing or Unexpected Conditional IEs

SMF ignores the received NAS message with the following conditional IE errors:

- Missing expected conditional IE
- Unexpected conditional IE
- Syntactically incorrect conditional IE

Standards Compliance

The NAS messages compliance with invalid protocol data handling feature complies with the following standards:

- *3GPP TS 24.501 – 5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3*
- *3GPP TS 38.323 – 5G; NR; Packet Data Convergence Protocol (PDCP)*

5GSM Cause Code Handling

Feature Description

The SMF or vSMF supports 5G Session Management (5GSM) cause handling for the UE-initiated and network-initiated procedures.

The supported procedures are:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

PDU Session Establishment Reject Cause Values

If the connectivity with the requested data network (DN) is rejected by the network, SMF sets the 5GSM cause IE of the PDU Session Establishment Reject message to indicate the reason for rejecting the PDU Session Establishment procedure.

The following table describes the supported 5GSM causes in the PDU Session Establishment Reject message.

Table 250: 5GSM Causes—PDU Session Establishment Reject

5GSM Reject Cause	SMF Behavior
Cause #26 – Insufficient Resources	The SMF includes this cause when it receives N2SmInfoType with "PDU_RES_SETUP_FAIL" along with any of the following N2 causes: • RadioNetwork/Radio_resources_not_available • RadioNetwork/Failure_in_the_radio_interface_procedure • Misc/Not_enough_user_plane_processing_resources
Cause #27 – Missing or unknown DNN	The SMF includes this cause when the DNN is not available in SmContextCreateData because the DNN is required and not configured in SMF.

5GSM Reject Cause	SMF Behavior
Cause #28 – Unknown PDU session type	The SMF includes this cause when the PDU Session Establishment Request message includes a PDU session type that is not supported by SMF.
Cause #29 – User authentication or authorization failed	The SMF includes this cause when the DNN authentication of the UE was unsuccessful (RADIUS Authentication Timeout).
Cause #32 – Service option not supported	The SMF includes this cause when the validation of received S-NSSAI fails against the allowed list of S-NSSAI.
Cause #33 – Requested service option not subscribed	The SMF includes this cause when the UE requests a service option for which it has no subscription.
Cause #38 – Network failure	The SMF includes this cause when the requested service was rejected due to an error in the network. This includes any internal failures or no response from any external NF during the PDN-setup procedure.
Cause #54 – PDU session does not exist	The SMF includes this cause when it does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.
Cause #70 – Missing or unknown DNN in a slice	The SMF includes this cause when the slice configuration is present but the requested DNN is not configured under the slice in the SMF.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.

PDU Session Modification Reject

If the SMF does not accept the request to modify the PDU session, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification procedure.

The following table describes the supported 5GSM causes in the PDU Session Modification Reject message.

Table 251: 5GSM Causes—PDU Session Modification Reject

5GSM Reject Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF sends this cause when SMF does not have the session.
Protocol errors	

5GSM Reject Cause	SMF Behavior
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.

PDU Session Release Reject

If the SMF does not accept the request to release the PDU session, SMF sets the 5GSM Cause IE of the PDU Session Release Reject message to indicate the reason for rejecting the PDU session release.

The SMF supports the following causes in the PDU Session Release Reject message.

Table 252: 5GSM Causes—PDU Session Release Reject

5GSM Reject Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF supports this cause when SMF does not have the PDU session.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content. **Important** The SMF also sends this cause for mandatory parameters with non-semantical errors such as PDU Session Identity and Procedure Transaction Identity.

PDU Session Release Request

To initiate the UE-requested PDU Session Release procedure, UE sends the PDU Session Release Request message with the 5GSM Cause IE to indicate the reason for releasing the PDU session.

The SMF supports the following causes in the PDU Session Release Request message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #36 – regular deactivation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #41 – Semantic error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #42 – Syntactical error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #44 – Semantic errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #45 – Syntactical errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.

PDU Session Modification Command Reject

If the UE rejects the PDU-Session-Modification-Command, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification.

The SMF supports the following 5GSM causes.

Table 253: Supported PDU Session Modification Reject messages

5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF retains the statistics based on the cause.
Cause #43 – Invalid PDU session identity	The SMF retains the statistics based on the cause and releases the existing PDU session.
Cause #44 – Semantic error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #45 – Syntactical error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #83 – Semantic error in the QoS operation	The SMF retains the statistics based on the cause.
Cause #85 – Syntactical error in the QoS operation	The SMF retains the statistics based on the cause.

How it Works

The SMF supports 5GSM cause handling for the PDU Session Establishment, PDU Session Modification, and PDU Session Release procedures. An appropriate SM cause will be sent through the N1 message to the UE.

The vSMF sends an indication toward hSMF to release the PDU session and associated resources for all session cleanups in the preceding scenarios.

Standards Compliance

The 5GSM Cause Handling feature complies with *3GPP TS 24.501 Release 15—Non-Access-Stratum (NAS) protocol for 5G System (5GS), Stage 3*.

5GSM Cause Handling OAM

This section describes operations, administration, and maintenance information for this feature.

Statistics

The 5GSM Cause Handling feature supports the following statistics to track the number of failures based on the 5GSM cause.

SMF N1 Message Stats

PDU-Session-Establishment-Reject:

- NETWORK_FAILURE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "NETWORK_FAILURE".
- UNKNOWN_PDU_SESSION_TYPE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "UNKNOWN_PDU_SESSION_TYPE".
- USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED".
- REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED".
- MISSING_OR_UNKNOWN_DNN: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN".
- SERVICE_OPTION_NOT_SUPPORTED: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "SERVICE_OPTION_NOT_SUPPORTED".
- INSUFFICIENT_RESOURCES: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- MISSING_OR_UNKNOWN_DNN_IN_A_SLICE: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING_OR_UNKNOWN_DNN_IN_A_SLICE".
- PDU_SESSION_DOES_NOT_EXIST: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "PDU_SESSION_DOES_NOT_EXIST".

PDU-Session-Modification-Reject:

- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Modification-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

PDU-Session-Release-Reject:

- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Release-Reject messages sent from SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".

PDU-Session-Release-Request:

- REGULAR_DEACTIVATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "REGULAR_DEACTIVATION".
- SEMANTIC_ERRORS_IN_PACKET_FILTER: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- SYNTACTICAL_ERROR_IN_PACKET_FILTER: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- SEMANTIC_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_TFT_OPERATION".
- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".

PDU-Session-Modification-Command-Reject:

- INSUFFICIENT_RESOURCES: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INSUFFICIENT_RESOURCES".
- INVALID_PDU_SESSION_IDENTITY: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INVALID_PDU_SESSION_IDENTITY".
- SEMANTIC_ERRORS_IN_PACKET_FILTER: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERRORS_IN_PACKET_FILTER".
- SYNTACTICAL_ERROR_IN_PACKET_FILTER: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_PACKET_FILTER".
- SEMANTIC_ERROR_IN_THE_QOS_OPERATION: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC_ERROR_IN_THE_QOS_OPERATION".
- SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL_ERROR_IN_THE_TFT_OPERATION".

N2/NGAP Interface

The N2 interface is the reference point between the RAN and the AMF. This interface connects the gNodeB to the AMF and is required due to Control and User Plane Separation (CUPS).

The N2 interface is needed because before accessing a service, the UE must be connected to the network. SMF handles the session control and the AMF handles the UE context. So, before initiating traffic or session, information, such as UE context, is required.

The N2 interface handles control-plane signalling. So, SMF uses N2 to generate and validate user traffic.

N2 Cause and Diagnostic IE Support

Feature Description

SMF supports the handling of N2 Cause and Criticality Diagnostics IE received over N2 message to and from NG Radio Access Network (NG-RAN).

How it Works

For this feature, SMF supports the following IE and cause values:

- Decode "Criticality Diagnostics" IE, which SMF receives as part of the following N2 messages:
  - PDU Session Resource Setup Unsuccessful Transfer
  - PDU Session Resource Modify Unsuccessful Transfer
- Handle the following N2 cause values in PDU Session Resource Setup Unsuccessful Transfer:
  - Radio Network Layer cause values:
    - Unspecified

- Multiple PDU Session ID instances
- NG intra-system handover triggered
- NG inter-system handover triggered
- Xn handover triggered
- UP integrity protection not possible
- UP confidentiality protection not possible
- UE maximum integrity protected data rate reason

- Protocol cause values:
  - Transfer syntax error
  - Abstract syntax error (reject)
  - Abstract syntax error (ignore and notify)
  - Message not compatible with receiver state
  - Semantic error
  - Abstract syntax error (falsely constructed message)
  - Unspecified

- Miscellaneous cause values:
  - Not enough user plane processing resources

- Handle the following N2 cause values in PDU Session Resource Modify Unsuccessful Transfer:
  - Radio Network Layer cause values:
    - Unspecified
    - Unknown PDU Session ID
    - Multiple PDU Session ID instances
    - IMS voice EPS fallback or RAT fallback triggered
    - NG intra-system handover triggered
    - NG inter-system handover triggered
    - Xn handover triggered

  - Protocol cause values:
    - Transfer syntax error
    - Abstract syntax error (reject)
    - Abstract syntax error (ignore and notify)
    - Message not compatible with receiver state

        - Semantic error
        - Abstract syntax error (falsely constructed message)
        - Unspecified
    - Miscellaneous cause values:
        - Hardware failure
        - Unknown PLMN

- Send the following N2 cause values in PDU Session Resource Release Command Transfer:
    - Radio Network Layer cause values:
        - Unspecified
        - Release due to 5GC generated reason
    - NAS cause values:
        - Normal release
        - Authentication failure
        - Deregister
        - Unspecified

- Handle the following N2 Cause values in Path Switch Request Setup Failed Transfer
    - Radio Network Layer cause values:
        - Unspecified
        - No radio resources available in target cell
        - Radio resources not available
        - Slices not supported
        - Resources not available for the slices
        - UP integrity protection not possible
        - UP confidentiality protection not possible
        - Not supported 5QI value
        - Encryption and/or integrity protection algorithms not supported
        - No radio resources available in target cell

- Generate an error-level log after SMF receives the N2 cause for a failure cause and debug-level log for a successful cause.

- Maintain statistics based on N2 cause that SMF receives for PDU Session Resource Setup Unsuccessful Transfer, PDU Session Resource Modify Unsuccessful Transfer, and Path Switch Request Setup Failed Transfer messages.
- Maintain statistics based on the N2 cause sent in PDU Session Resource Release Command Transfer message.

N2 Cause Handling

SMF handles the N2 Causes with the following IEs:

- PDU Session Resource Setup Unsuccessful Transfer IE
- PDU Session Resource Modify Unsuccessful Transfer IE
- PDU Session Resource Release Command Transfer IE
- Path Switch Request Setup Failed Transfer IE

PDU Session Resource Setup Unsuccessful Transfer IE

For each PDU session resource with the failed configuration, the NG-RAN includes PDU Session Resource Setup Unsuccessful Transfer IE of the PDU Session Resource Setup Request message. This message includes the cause value, with the details on cause for the unsuccessful establishment, for SMF.

In case the serving NG-RAN doesn't accept the partial QoS Flow failures of a PDU Session, the SMF initiates the PDU Session Modification procedure. This procedure removes the non-accepted QoS flows from the PDU Session after PDU Setup procedure is completed.

Note SMF supports the decoding of "Criticality Diagnostics" IE that it receives as part of the N2 message only. For example, PDU Session Resource Setup Unsuccessful Transfer message and PDU Session Resource Modify Unsuccessful Transfer message. SMF doesn't fully support the "Criticality Diagnostics" IE for other messages.

The PDU Session Resource Setup Unsuccessful Transfer IE includes the following causes and their cause values:

Table 254: PDU Session Resource Setup Unsuccessful Transfer IE Causes and Cause Values

Cause	Cause Value	Description
Radio Network Layer	Multiple PDU Session ID instances	NG-RAN includes this cause value after receiving the PDU Session Resource Setup Request message. This message includes various PDU Session ID IEs in the PDU Session Resource Setup Request List IE, which is configured to the same value.
	User Plane Security Enforcement	NG-RAN includes the following cause values in case the User Plane Security Enforcement information is unfulfilled. These cause values have either the Required or Preferred value: • UP integrity protection not possible • UP confidentiality protection not possible • UE maximum integrity protected data rate reason
	Collision with Handovers	NG-RAN includes the following cause value after receiving the Handover request and continues with the Handover Preparation procedure: • NG intra-system handover triggered • NG inter-system handover triggered • Xn handover triggered **Note** The Handover request is necessary during PDU Session Resource Setup procedure.
	Note For the preceding cause values, in case of failure detection, if the NG-RAN doesn't forward N1 message to UE and continues with the session release, the SMF sends the PDU Session Establishment Reject message toward UE through N1 message. NG-RAN maintains the N2 cause-based statistics in the N2 message type.	
	Unspecified	In case the NG-RAN failure is unspecified, SMF triggers the release of this PDU Session. NG-RAN maintains a N2 cause-based statistics in the N2 message type.

Cause	Cause Value	Description
Protocol Group	Erroneous errors in Protocol data	NG-RAN includes the following cause values when it couldn't decode the received message: • Transfer syntax error • Abstract syntax error (reject) • Abstract syntax error (falsely constructed message) • Semantic error **Note** If the NG-RAN doesn't forward N1 message to UE and continues with the session release, the SMF sends the PDU Session Establishment Reject message toward UE through N1 message. NG-RAN maintains the N2 cause-based statistics in the N2 message type.
	Unforeseen or Unknown information in Protocol data	NG-RAN includes the following cause value when it is unable to decode the received message: • Message not compatible with receiver state • Unspecified • Abstract syntax error (ignore and notify) When the NG-RAN is unable to decode the message, SMF triggers the release of the PDU Session. NG-RAN maintains an N2 cause-based statistics in the N2 message type.
Transport Group	Inaccessible transport resources	NG-RAN includes the following cause values when required transport resources are unavailable: • Resource Unavailable • Unspecified When the NG-RAN is unable to access the transport resources, SMF triggers the release of the PDU Session. NG-RAN maintains an N2 cause-based statistics in the N2 message type.

Cause	Cause Value	Description
Miscellaneous	Not enough user plane processing resources	NG-RAN includes this cause value when insufficient resources are available for the User Plane processing. When the NG-RAN is unable to access the User Plane processing resources, SMF triggers the release of the PDU Session. NG-RAN maintains an N2 cause-based statistics in the N2 message type.

PDU Session Resource Modify Unsuccessful Transfer IE

For each PDU session resource with the failed modification, NG-RAN includes PDU Session Resource Modify Unsuccessful Transfer IE of the PDU Session Resource Modify Request message. This message includes the cause value, with the details on cause for the unsuccessful modification, for SMF.

The PDU Session Resource Modify Unsuccessful Transfer IE includes the following causes and their cause values:

Table 255: PDU Session Resource Modify Unsuccessful Transfer IE Causes and Cause Values

Cause	Cause Value	Details
Radio Network Layer	Multiple PDU Session ID instances	NG-RAN includes this cause value after receiving the PDU Session Resource Modify Request message. This message includes various PDU Session ID IEs in the PDU Session Resource Modify Request List IE, with the same configured value.
	Collision with Handovers	NG-RAN includes the following cause values after receiving the Handover request and continues with the Handover Preparation procedure: • NG intra-system handover triggered • NG inter-system handover triggered • Xn handover triggered **Note** The Handover request is necessary during the PDU Session Resource Modify procedure.
	Unspecified	
	Note For the preceding cause values, SMF stops the PDU Session Modification procedure and continues to use the same value for all the fields as existed in the earlier modification procedure. SMF maintains an N2 cause-based statistics under N2 message type.	
	Unknown PDU Session ID	NG-RAN includes this cause value after receiving the PDU Session Resource Modify Request message. This message includes PDU Session ID IEs, from the PDU Session Resource Modify Request List IE, which NG-RAN couldn't identify. These sessions are invalid PDU sessions. SMF releases the PDU Session of the PDU Session IDs that NG-RAN marks as invalid or unknown. NG-RAN maintains a N2 cause-based statistics in the N2 message type.

Cause	Cause Value	Details
Transport group		NG-RAN includes the transport cause value when the required transport resources are unavailable. SMF stops the PDU Session Modification procedure and continues to use the same value for all the fields as existed in the earlier modification procedure. SMF maintains an N2 cause-based statistics in the N2 message type.
NAS		SMF stops the PDU Session Modification procedure and continues to use the same value for all the fields as existed in the earlier modification procedure. SMF maintains an N2 cause-based statistics in the N2 message type.
Protocol group		
Miscellaneous		SMF triggers the release of the PDU Session after receiving the PDU Session Resource Modify Request message. This message includes the following Miscellaneous causes in N2 SM information. SMF maintains a N2 cause-based statistics in the N2 message type. • Hardware failure • Unknown PLMN Except for the cause value of the preceding causes, SMF stops the PDU Session Modification procedure and continues to use the same value for all the fields as existed in the earlier modification procedure. SMF maintains an N2 cause-based statistics in the N2 message type.

PDU Session Resource Release Command Transfer IE

For each PDU session resource to be released, SMF includes PDU Session Resource Release Command Transfer IE with a cause value. This value includes details on cause for the release to NG-RAN.

The PDU Session Resource Release Command Transfer IE includes the following causes and their cause values:

Table 256: PDU Session Resource Release Command Transfer IE Causes and Cause Values

Cause	Cause Value	Details
NAS	Normal Release	SMF includes this cause for the UE-initiated PDU Session release.
	Deregister	SMF includes this cause for the UDM-initiated PDU Session release.

Cause	Cause Value	Details
Radio Network Layer	Release due to 5GC generated reason	SMF includes this cause for both the network-initiated PDU Session release and the internal failure cases.
	Note For all the preceding cause values, SMF maintains an N2 cause-based statistics in the N2 message type.	

Path Switch Request Setup Failed Transfer IE

For each PDU session resource with failed switching, NG-RAN includes Path Switch Request Setup Failed Transfer IE of the Path Switch Request message. This message includes the cause value, with the details on cause for the unsuccessful switching to Target NG-RAN.

Note SMF supports only the decoding of N2 Cause IE.

The Path Switch Request Setup Failed Transfer IE includes the following causes and their cause values:

Table 257: Path Switch Request Setup Failed Transfer IE Causes and Cause Values

Cause	Cause Value	Description
Radio Network Layer	User Plane Security Enforcement	NG-RAN includes the following cause values in case the User Plane Security Enforcement information is unfulfilled. These cause values have either the Required or Preferred value: • UP integrity protection not possible • UP confidentiality protection not possible • UE maximum integrity protected data rate reason • Encryption and/or integrity protection algorithms not supported
	Not Supported 5QI Value	NG-RAN includes this cause value when the Target NG-RAN accepts none of the QoS Flows of a PDU Session.
	Slice not supported	NG-RAN includes the following cause values when the corresponding network slice isn't supported in the Target NG-RAN. • Slices not supported • Resources not available for the slices
	Resource Unavailability	NG-RAN includes the following cause values when insufficient resources are available to switch in the Target NG-RAN. • No radio resources available in target cell • Radio resources not available
	Unspecified	
	Note For all the preceding cause values, SMF deactivates the UPF N3 tunnel for the QoS flows with the failed switching for Target RAN. SMF maintains an N2 cause-based statistics under N2 message type.	

Standards Compliance

The N2 Cause and Diagnostic IE Support feature complies with the following standards:

- *3GPP TS 38.413 version 15.4.0 Release 15—5G; NG-RAN; NG Application Protocol (NGAP)*
- *3GPP TS 23.502 version 15.6.0 Release 15—5G; 5G System; Session Management Services; Stage 3*

N4 Interface

The SMF sends messages to the User Plane Function (UPF) over the N4 interface by using the Packet Forwarding Control Protocol (PFCP). SMF performs various session management procedures using the N4 interface. An example of a management procedure is when UPF identifies and transports user plane traffic information and flow based on session management data that it receives from the SMF.

N4 Over IPSec

SMF supports Internet Protocol Security (IPSec) on N4 interface for secure network traffic.

The N4/Sx Over IPSec feature requires some basic configurations to be enabled on SMF, UPF and SMI. For complete information on this feature, see the *UCC 5G UPF Configuration and Administration Guide* applicable for the release.

SMI strongSwan Configuration

To spawn the SMI strongSwan pod, use the following sample configuration:

```
SMI:
addons strongswan enabled
strongswan connections N4_IPSec_RCM3
  auto add
  keyexchange ikev2
  type tunnel
  left 192.12.31.202
  right 50.50.29.5
  leftsubnet 192.12.31.202/24
  rightsubnet 50.50.29.4/32
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
==-----END CERTIFICATE-----"
  server-priv-key "$8$gFVXFkFlJplgshiCqWs222+/vkNL5suwjGgqQVwhm1HEIvNp5ViKE8Stz7NK
jubZL1uXIDuy\nTbZmSPp8gIyWFTAJadMNjSoJswWhFYHX+aYoliCIdWQEUFSnJTz2Gofjgex3kM7g8iFkw
BNb\nB6qnSOV2WwMHown1ZfIGEZQAZ6B6iNnQbIHVrOgsyAY6akkyoNzIuc1gFdijQ2W56wW6tQR1\n5EpV
5zweW/Nr0RoOma+ZjpKY8L2VDW30SZ+VwbeTWexrVVfTbYifYYURekyIr6SbK4wFwt+3\nLhBUIr/6zvOlV
```

```
QBh4GVEheB5IJid0vHSI3N91sxX+VRaBodSKyw22HpC5BgWanarhkd1KfCT\nmoLzQ7+Nw0X0UfbKTLM5G8
IhXGxqccjl8Jb8nZf490MGx+XrYMkNcFNJ7ua7bxNhl1goTyUs\n4Wbw9hcviv9ZD4leTwnSlqnv5Yfr0ED
GJVrkW2zFv808fKdkJ2rO9T843u9DOrKrFo6XMPT2\n3JU9RL6zlI6bUMTHRqy2xLDfTtDBrD5jg3joJdD7
nkQfCW6cS79cXTBSLTc79p8otX8Jy56n\nkg1uDmQvdY+PgmbByvjQLrPkFr1BQ0C/g5F1uTPSiy2bNGr9l
QF8LfV8kakQMsi+FT0BJbil\nXHxw9pMu2p9srsZRmiBUw4PMq5nQ69jqDJweoNwzjqcJKBvIV1mvKIzHll
Ha0jOqA/FqASn0\nXzmKuZwG49c8qJaE5JBTLTjxeD7tG6A5XuewKynAYWnynT/0xP0mMDMcwEPdOt4e/L4
WJUOJ\nUn4EVo9EMOeG/eRzqILwAbeo2faQtY3HR7c5qMGgnBk903zIVsxl7SP4ujR0HuRw3zq7co5y\n6O
GSmu5Q79EeHezgxn+uiCsPSBwD3gkjvCerdBi8lKPptp//J+XyFA6MdgTbjzb+MxsDXszt\nyXaojBhn9t1
RxwVepAyVesm511JdH/IeDGIYY21Q2DT/k3RT490yKQSu2U2J3n49PCsEtHTQ\nbJo0WmoBVzkysE5kkL2R
MMD6PN+oV8eSqXJHkc1lAFhTpB+TqXcUI+QM0DsLdC1KOr7I5a6P\nl7jdyFFKlbPW8bOe2BB+bKA+5lOQ0
ygb9hlM76WdKmr8hhaimIuH6covaqISrFJJ0IvXcaWS\nhiatKxAq/KhkdczeM0WS6Z8PFlUwRoqgL8X8tn
v1C6tvJbUNLOPgTbHYjkflOyEeFHgXVlXi\nnzE4iAADsRTaMT/3G5YuPjk7+0lmtiZRKHXUPy7LyRwJHNZ
vkaEY+LALhA0ukMpH4DcdDibh\n16kPVUPvWZNZ2Mw3kILH5raqICdGYDDuW1SwCLBeV2pqMuaTzFiSPpLt
5AFXKtF5u9vA+VIC\nJcWP77XVbPTkbsnSBtxFy32RlZY5rx6hLEf/XsMnPAOJvprZvWuc7F+KzrexMmYAY
bJbKE3S\n8POaPet9r8+mPkQf+F5NQD7r3iz0iZ7Hj4IVzm5cvlo9yfatvm03cDplBhVAvsa5dTRuJCq+\
n0UMpf6PbcZI3vhVjIGm7iR+SVSVrq27+lGW76MpnpGwffm/gnyVvg97wl21LmPuool6vKljs\nc9DBybr
dOIwf6gkHkfwDPITGZEbc0SiH3AnIc8Z6HPiCqm1jLJ+2PfC6xnJdLRgkB8sJA1UC\n1VikR2YOvSR26Z6
PI5x7Nhq73jlRMr2N7cvrbBgfjmQyluHa0H/fnOYh4/D6Va8ROWCM4Ca3\nGOPeGn/oJAY1qogLSad33OI
DLsExvyh52x8KvrhdBCRRY5EabXa97XG0TtRTgt6NDd9NwZZ0\n2xxE06VUMS307UBAmyQn7vuezVqcHtv
3H9NnDFPRVLsnyreNo04VjZN6PHtqqOei/sLfL1GK\nVzvleeNGfSAvh1kmFh13f9p1jXgnTwt4iFErpaR
1lvk5K1RoF/+Sjo0HYhETvJFxA/yd/2I0\nZQe3ob/W4hBqI069yQjHbk+9L6kGWzQl3Tl8Lw1/YU/2AXS
zW8V9wCV0OhNLwQezt7a8EBm4\nX3CsPNVhhixhdvC/rSrXFPJnXy0mrcuCXhqLitWRA5VO6883Yry7ldP
uHzcVTyLCxYm0PWaT\nif4TQ6BxvT/gz7Ic6F3dO/QwMKoyeA7RoRR3XpnFcN1QMNTrF17jg17hDFjJwBO
dsq1gfau5\nUDeG6HihvcggYwnbkTprwaHflK/tsTCReNi+j/+ei+4DIe0f2vFgqaGjHdaa6qGkpSXks4L
R\nhyVd9/y+"
  nodes master-3
  exit
 exit
strongswan connections N4_IPSec_V6
  auto add
  keyexchange ikev2
  type tunnel
  left 2001:4888:192:1231::202
  right 2001:4888:50:50::22
  leftsubnet 2001:4888:192:1231::202/64
  rightsubnet 2001:4888:50:50::21/128
  leftauth psk
  rightauth psk
  leftsendcert never
  psk starent
  esp aes128-sha1,aes128-sha256-prfsha256
  ike aes128-sha1-modp1024,aes128-sha256-modp1536
  reauth no
  dpdaction clear
  dpddelay 300
  dpdtimeout 60
  closeaction none
  server-cert "-----BEGIN CERTIFICATE-----MIIDjTCCAnWgAwIBAgIUF6njegbcarj2oq
/x9c2+utqPThUwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3R
hdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA5MDcwOTQ0MDdaFw0zM
jA5MDQwOTQ0MDdaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBh
JbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkKA
vGj94OWcFV8j7Enpr5HHqQxakb7hD0fETPByMIb9lPA73AM/3g7YjyIuAFhhs/fx4ZbFQJKDUVjiK/
PE7Mq/Opw5vIsUAgyhors2goa3YvBEPCmTk4fPz21hkWLHZgTARKq3XkgdCAO7kB7UsJpxVBSGg0A
52bIy3bB5C8YNa4rTrafVqzzFdYrQfAama2lpLrfxI7TzoZ6qK1LUDe8U7K/Ln/LJOeqxXClGSEzz
GRBqG41FeU18u3mpJ1pDINUJj7E7r+UN58aTwMoW3/ThCL/2ou+vjTVN7TDzva6XdJPNBCMA5dKEh
0EF10rMo8nmtLzo4UW9NBKMbiv7KPAgMBAAGjdTBzMB8GA1UdIwQYMBaAFC/Lvz0LAowgIkydSpKNUwy/
wHzJMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMDgGA1UdEQQxMC+CFWNuZHAtbmFybWFkYS1tYXN0ZXIt
M4cEwAwfyocQIAFIiAGSEjEAAAAAAAACAjANBgkqhkiG9w0BAQsFAAOCAQEAB6WUQI4qgEHQ8E5sYwzP
zw5KC/zGP2WZIkBfcs8ReiGmLJlC8n8uceWH12ZbFwY75j3EBFfqkmnNXftQGmuU8oGyZsuPDpmEySo+
nE28xnQDZDGzABLZWLSZqqeR6obnYUKvDho14kd40o1hnVlaONw1mrwc/QyFvn3tOwoYnXgaktGM01Fu
cQY1Kc33DvJx3n7fOsdoOLRm9jEENYT3Dv8b6/Ezr2mMHRhAwuoaFpvOSc/eLJy0QO7RpQLpHcRmnh9n
XO+gccB+e0YzvuBS5PONt8wjNSCKl46ZW4F9jpvehR8P/rvH/3VbwDaa8c6xARHNxzNcfq5S4tK/f58RSA
==-----END CERTIFICATE-----"
```

```
  server-priv-key "$8$jW1TFB0/rJW4V6NrVjk4+1KE7Dw6ynkP3Bqtiwp2k+GQDrI4bX2n+a6Yvyeq
zzKdQ+EQLuy6\ncj9xOrxtNflmzaptNF9Ku786m934ID9hzmC8ISya6/4f2Xu+WdG6uIJl2jDhB/3B2PIc
b6VQ\nV7c4GmwPRNBlIZTVMvTS/2xiUx9bdXIQTVzl2Sc3bZqwLJ6ho/qr4r++T7blVZ16j5sYxUI6\nat
ZKNMMk8+0aoH4UaOd5vtoSkhXCLXkfyrGYagx4KceKxPxSciSEptAzM36py7hDqazW5epU\nFaAnw3PMhq
Ut1r790CaG3VZR5WpcJVkHbdpf0iMCt6pJjNeNlL7BTvns+vo16Mcgt0pyi6Rj\nBAo5lSzog9max0EiRk
spb4a91DFX8mV4tzTy0RCzbgkuzdZ3ecbB9OOvrkWOv7dLiWsZe66Q\nrQA4SLH7eOkgRQvDzqmx3DpqXP
7rebptkLAGXAxZV5uvUuyivdal0EPiB6fu3OwP+gJweZIg\nLjIVbJsREgN7YdukihOmk/xbSMK25Eu3X3
yI1Y55vvQfsY08WEfKBO+Alzjrvz4ABydVJcEE\nqywkSUK/j0VksGvN4lzgely07tpz22VjMTrxJvoWB+
5j9j183T/C1Wgf53miFz2z8ak0NYYe\n2AEP9NNs4tFkB9bY9JQsFv6zY3J+2hQ8iyCiYIROd5ItRyLenO
Bt1fKGp5FHg7dlPuOz0VoI\nUm7GlEexMIycNEr9rzOqzBbMiH5c53htY4iQWFvOARHhw2f5GWPZOIe8Z8
uTq4k5iUjWmaLa\nfhNMXIGX2QNgoduZwXiX6yv3gCpK8WDgF4dlvPjFB+f+iA+QyBlc5AYZuE/2yjYRCr
aaPkzx\ndrWm+Uh18d1YdmQq4ss/rUY4Q0DxDblv94Xx64NIq8dbnY7Zehjs9LXXHk2X6daSTC/FYIY+\n
J/Sks+tmnZ489Tojo/F5dS9iVVstP68MdKOl4OC53lDkqcNl0xhniu2nneS6HTlzUrKFSi4I\n3eRW0FwK
ONKrePxKdObZFB+FvV+xOa2UKnXBbpIh/ENFE0XnADP7Ljox3YsZZpvnXTcz7OcE\nq1b8ggtLt6KyWDb0
tdZljLAb4posj1NioJQzyxHT0gsdfkZxtWiqgt65gqXS/iDo9XXdFEj1\n1Gr07SoE+HwoJIPzAG/8fNhm
27CCYaUW1uWJAOUt9I5UCbER+2kFaVC+odEY2W5/Hfc/gWAy\nSRd6/46kvjN/SzabIdb1yqr68G4LIrHg
1kEBoAf9hXSkD7WY2SMSjl950Co4Cq6zVbk6PAcX\n2ET02FhFewiq+TamVNr0/ruyPohyr1Cpgjqzvx6s
+s7EMWOPJh+XEh8PPBKY+DcDEr2RBIcZ\n4O9uAzwiYTm1x4u8dw5kKRd+H8HFobgaQ18i3IfCdZ4DXyrq
mMrxOw52fGIuAd3Ln2j/AitZ\nQP61dlQlwWPHX7ykvXqCP6oZnfbMUVW3iIdFauZLiCDZkX98UXY3IZUi
Eq13GL6KZtKwFAbu\nqHYEtb5OJRiHRZnqmoOf7BQjC3cdDTBpmPd/s9JCSejqSahlSaSl4Qghbba35HIG
o9PVyks3\nGny6P6twYnDCHLdXbmfE+HE71MnRRPd63CNp+SeX/pP5nBhu6RU/K61ovPrSqcsmo8GiytZB
\ndtVH7nYk3ZUWan04us/bd5zNZfrQ1mCF4rS4KGprQ0N7xWSCilMI49aIxSCNM9WkYl8HAEWA\n1IceEZ
RxHxeltl3JMNTxwFlkP4i4IEalf//Tidrd13jka0NnnjOsboUgn7lay3LvsC6zsIGN\nkP0sTGI1hHj9OL
1iKkw6IhTS1Py5Bjof+XPE844QwOY6Qj6GTd5F/GQJOOD3rL2J/S651TvJ\nsnKM5roovBVb1dUANC/Eay
frpC/2w8wjqPQ/O02SzVNSbZOIPn8P8BV3Ql+NC8rEWL1FZMkI\nkM1AsZTx8BQ0Z1Haf4uhtV5+/29ula
EqEiTH1x2QDV9idWPekqr7eC3009YoGESWHuIH/JE/\n76Rr2zi4wK0JVecxbCGDOynIRFE3I3gRdxgtTi
GrOMe2WdqsUDvDkcijCVpHo0JS3jFVONR8\nxbEo7RpxdrQJ5Zr/u/vx1jnQV/bXTzwlkqoy1g9C3V1m4m
NrqYz62taNTF7+NEVyWC/cp5CU\n5SDuAs3JmFyLaRvyU5SsmDbzlyj+z3DUaByHWlWtC5+klwXYoZOKIy
8zNj+1Kzxosk1wiVX1\nqT4CoAKX"
  nodes master-3
  exit
 exit
```

For the latest strongSwan configurations, see the *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*.

SMI strongSwan Validation

To determine the spawned pods on a specific node, use the following command:

kubectl get pods -o wide -n smi-strongswan

```
NAME              READY   STATUS    RESTARTS   AGE     IP          NODE    NOMINATED NODE
READINESS GATES
strongswan-d7zzp   1/1    Running     0       4h57m   10.1.27.7  master-3    <none>
 <none>
```

The following is a sample SMI strongSwan configuration to validate the IPSec tunnel CLI on SMF protocol pod:

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan --
 ipsec statusall
Status of IKE charon daemon (strongSwan 5.9.3, Linux 5.4.0-122-generic, x86_64):
uptime: 14 days, since Sep 19 16:36:02 2022
malloc: sbrk 6221824, mmap 0, used 3867536, free 2354288
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 15
loaded plugins: charon aesni aes des rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation
constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl af-alg fips-prf
gmp curve25519 xcbc cmac hmac ccm gcm drbg curl files attr kernel-netlink resolve
socket-default stroke vici updown eap-identity eap-dynamic eap-tls xauth-generic counters
Listening IP addresses:
10.105.90.166
2001:420:5504:2004::90:18
```

```
71.71.71.15
71.71.71.70
71.71.71.72
71.71.71.73
192.12.31.21
2001:4888:192:1231:42a6:b7ff:fe3b:7161
2001:4888:192:1231::21
192.12.31.203
192.12.31.206
192.12.31.207
192.12.31.208
192.12.31.209
192.12.31.210
192.12.31.211
192.12.31.213
192.12.31.214
192.12.31.215
2001:4888:192:1231::203
2001:4888:192:1231::206
2001:4888:192:1231::207
2001:4888:192:1231::208
2001:4888:192:1231::209
2001:4888:192:1231::210
2001:4888:192:1231::211
2001:4888:192:1231::213
2001:4888:192:1231::214
2001:4888:192:1231::215
2001:4888:192:1231::121
192.12.31.121
192.12.31.205
192.12.31.212
2001:4888:192:1231::205
2001:4888:192:1231::212
192.12.31.202
192.12.31.221
192.12.31.222
2001:4888:192:1231::202
2001:4888:192:1231::221
2001:4888:192:1231::222
192.50.0.1
fd00::1
192.115.3.37
Connections:
N4_IPSec_RCM1: 192.12.31.202...50.50.27.5 IKEv2, dpddelay=300s
N4_IPSec_RCM1: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM1: remote: [50.50.27.5] uses pre-shared key authentication
N4_IPSec_RCM1: child: 192.12.31.0/24 === 50.50.27.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM2: 192.12.31.202...50.50.28.5 IKEv2, dpddelay=300s
N4_IPSec_RCM2: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM2: remote: [50.50.28.5] uses pre-shared key authentication
N4_IPSec_RCM2: child: 192.12.31.0/24 === 50.50.28.4/32 TUNNEL, dpdaction=clear
N4_IPSec_RCM3: 192.12.31.202...50.50.29.5 IKEv2, dpddelay=300s
N4_IPSec_RCM3: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec_RCM3: remote: [50.50.29.5] uses pre-shared key authentication
N4_IPSec_RCM3: child: 192.12.31.0/24 === 50.50.29.4/32 TUNNEL, dpdaction=clear
N4_IPSec_V6: 2001:4888:192:1231::202...2001:4888:50:50::22 IKEv2, dpddelay=300s
N4_IPSec_V6: local: [2001:4888:192:1231::202] uses pre-shared key authentication
N4_IPSec_V6: remote: [2001:4888:50:50::22] uses pre-shared key authentication
N4_IPSec_V6: child: 2001:4888:192:1231::/64 === 2001:4888:50:50::21/128 TUNNEL,
dpdaction=clear
N4_IPSec: 192.12.31.202...50.50.21.5 IKEv2, dpddelay=300s
N4_IPSec: local: [192.12.31.202] uses pre-shared key authentication
N4_IPSec: remote: [50.50.21.5] uses pre-shared key authentication
N4_IPSec: child: 192.12.31.0/24 === 50.50.21.4/32 TUNNEL, dpdaction=clear
```

```
Security Associations (5 up, 0 connecting):
N4_IPSec_RCM1[1345]: ESTABLISHED 96 minutes ago,
192.12.31.202[192.12.31.202]...50.50.27.5[50.50.27.5]
N4_IPSec_RCM1[1345]: IKEv2 SPIs: bc79a16793c7d7eb_i 087bb5cd20fd2f34_r*, rekeying in 72
minutes
N4_IPSec_RCM1[1345]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM1{2501}: INSTALLED, TUNNEL, reqid 2, ESP SPIs: cd664851_i 13009213_o
N4_IPSec_RCM1{2501}: AES_CBC_128/HMAC_SHA2_256_128, 900 bytes_i (17 pkts, 16s ago), 829
bytes_o (17 pkts, 16s ago), rekeying in 36 minutes
N4_IPSec_RCM1{2501}: 192.12.31.202/32 === 50.50.27.4/32
N4_IPSec_RCM3[1343]: ESTABLISHED 97 minutes ago,
192.12.31.202[192.12.31.202]...50.50.29.5[50.50.29.5]
N4_IPSec_RCM3[1343]: IKEv2 SPIs: 1a50e1d11dfeacb7_i 7be50275473937a3_r*, rekeying in 65
minutes
N4_IPSec_RCM3[1343]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM3{2499}: INSTALLED, TUNNEL, reqid 5, ESP SPIs: cd6f47ec_i 13009213_o
N4_IPSec_RCM3{2499}: AES_CBC_128/HMAC_SHA2_256_128, 1328 bytes_i (25 pkts, 26s ago), 1217
bytes_o (25 pkts, 26s ago), rekeying in 30 minutes
N4_IPSec_RCM3{2499}: 192.12.31.202/32 === 50.50.29.4/32
N4_IPSec_RCM2[1341]: ESTABLISHED 103 minutes ago,
192.12.31.202[192.12.31.202]...50.50.28.5[50.50.28.5]
N4_IPSec_RCM2[1341]: IKEv2 SPIs: 26fd8455c09927ab_i 78c5379f6559be4b_r*, rekeying in 60
minutes
N4_IPSec_RCM2[1341]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_RCM2{2500}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6f5243c_i 13009213_o
N4_IPSec_RCM2{2500}: AES_CBC_128/HMAC_SHA2_256_128, 1026 bytes_i (19 pkts, 0s ago), 917
bytes_o (19 pkts, 0s ago), rekeying in 34 minutes
N4_IPSec_RCM2{2500}: 192.12.31.202/32 === 50.50.28.4/32
N4_IPSec_V6[1339]: ESTABLISHED 2 hours ago,
2001:4888:192:1231::202[2001:4888:192:1231::202]...2001:4888:50:50::22[2001:4888:50:50::22]
N4_IPSec_V6[1339]: IKEv2 SPIs: 64e5d5e102e885e7_i 9062914577d9eb95_r*, rekeying in 36 minutes
N4_IPSec_V6[1339]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec_V6{2498}: INSTALLED, TUNNEL, reqid 3, ESP SPIs: c25a2531_i 0f009d13_o
N4_IPSec_V6{2498}: AES_CBC_128/HMAC_SHA2_256_128, 6817 bytes_i (89 pkts, 17s ago), 6326
bytes_o (89 pkts, 17s ago), rekeying in 17 minutes
N4_IPSec_V6{2498}: 2001:4888:192:1231::202/128 === 2001:4888:50:50::21/128
N4_IPSec[1337]: ESTABLISHED 2 hours ago, 192.12.31.202[192.12.31.202]...50.50.21.5[50.50.21.5]
N4_IPSec[1337]: IKEv2 SPIs: 9af4e1f24dcc0edb_i 6fcea88758803d37_r*, rekeying in 26 minutes
N4_IPSec[1337]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536
N4_IPSec{2497}: INSTALLED, TUNNEL, reqid 4, ESP SPIs: cc7c3bf1_i 0f009c13_o
N4_IPSec{2497}: AES_CBC_128/HMAC_SHA2_256_128, 6844 bytes_i (121 pkts, 19s ago), 5693 bytes_o
 (121 pkts, 19s ago), rekeying in 4 minutes
N4_IPSec{2497}: 192.12.31.202/32 === 50.50.21.4/32
cloud-user@cndp-narmada-master-1:~$
```

The following is a sample SMI strongSwan configuration to validate the *ipsec.yaml* file on SMF:

```
cloud-user@cndp-narmada-master-1:~$ kubectl exec -ti strongswan-d7zzp -n smi-strongswan --
 cat /etc/ipsec.conf
conn N4_IPSec_RCM1
leftcert=/etc/ipsec.d/certs/N4_IPSec_RCM1.cert.pem
auto=add
closeaction=none
compress=no
dpdaction=clear
dpddelay=300
dpdtimeout=60
esp=aes128-sha1,aes128-sha256-prfsha256
ike=aes128-sha1-modp1024,aes128-sha256-modp1536
ikedscp=000000
ikelifetime=3h
keyexchange=ikev2
left=192.12.31.202
leftallowany=no
leftauth=psk
```

```
leftsendcert=never
leftsubnet=192.12.31.202/24
lifetime=1h
mobike=yes
reauth=no
rekey=yes
right=50.50.27.5
rightallowany=no
rightauth=psk
rightsubnet=50.50.27.4/32
sha256_96=no
type=tunnel
```

User Plane Integrity Protection

Feature Description

SMF supports integrity protection of user data packets exchanged between UE and gNB. Though the 3GPP specification mandates the Integrity Protection feature on both the UE and the gNB, this feature remains optional to use due to the overhead of the packet size.

SMF learns the integrity protection status from UDM and decides whether to enforce the User Plane Integrity Protection at gNB. In the absence of status information from UDM, the SMF uses its local configuration data.

SMF decides the maximum integrity data rate by comparing the data rate values that were requested by UE and configured locally on SMF. If there is no local configuration for data rates, then the UE requested data rates are applied.

For example, if the UE indicates 64 kbps as its maximum data rate for integrity protected traffic, then the network only turns on integrity protection for UP connections where the data rates are not expected to exceed the 64 kbps.

How it Works

This section describes how the user data packets between UE and gNB are integrity protected.

SMF retrieves UP security subscription per DNN from UDM during 5G session creation and gives priority to the UPIP status (UP integrity values) received from UDM over local configuration.

SMF decides UPIP enforcement status and UPIP enforcement data rate based on UP security subscription, local configuration, and the UPIP data rate values received from UE. Then, the SMF sends the appropriate UPIP enforcement status and data rate to gNB through PDU Session Resource Setup Request message during PDU establishment procedure.

SMF includes the following information in Security Indication in the N2 setup request message.

- Integrity Protection Indication IE with UPIP enforcement status
- Maximum Integrity Protection Data Rate Uplink or Downlink IE with UPIP enforcement data rate
- Confidentiality Protection Indication IE with “not-needed” as the value

If gNB cannot meet the UPIP enforcement data rates and if the Integrity Protection Indication IE is set as “required”, it rejects PDU session resource setup request with cause “up-integrity-protection-not-possible”. Then, the SMF clears the call and sends N1 release to the UE.

If gNB cannot meet the enforcement data rates and if the Integrity Protection Indication IE is set as “preferred”, it includes Security Result with integrity protection result set to “not performed” in PDU Session Resource Setup Response message.

If gNB is able to enforce UPIP data rates and if the Integrity Protection Indication IE is set as “preferred”, it includes Security Result with integrity protection result set to “performed” in PDU Session Resource Setup Response message.

SMF populates the UPIP enforcement values in N2 messages based on the algorithms specified in the following tables.

Table 258: Negotiated UPIP Status based on UDM Subscription and Local Configuration

UPIP Subscription	Local Configuration	UPIP Status
Required	Not Applicable	Required
Preferred	Not Applicable	Preferred
Not needed	Not Applicable	Not needed
Not received	Required	Required
Not received	Preferred	Preferred
Not received	Not needed	Not needed
Not received	Not configured	None

Table 259: Negotiated UPIP Data Rate based on UE Supported Values and Local Configuration

UE Requested Data Rate	Local Configuration	UPIP Data Rate
64 kbps	Not configured	64 kbps
Null	Not configured	Null
Null	Configured	Null
Full rate	Not configured	Full rate
64 kbps	64 kbps	64 kbps
Full rate	64 kbps	64 kbps
64 kbps	Null	Null
Full rate	Null	Null
64 kbps	Full rate	Null
Full rate	Full rate	Full rate

Table 260: N2 UPIP based on UPIP Status and UPIP Data Rate Output

UPIP Status	UPIP Data Rate	N2 UPIP Indication	N2 Security Data Rate	N2 Security Result	Comment
Required	64 kbps	Required	64 kbps	Not Applicable	Call is cleared if N2 failure received due to one of the following reasons: • Encryption and integrity protection algorithms not supported • UP integrity protection not possible.
Required	Null	Not Applicable	Not Applicable	Not Applicable	Call is cleared with N1 cause= #82 "maximum data rate per UE for user plane integrity protection is too low". N11 SmContextCreate error is sent with cause INTEGRITY_ PROTECTION_ MDR_NOT _ACCEPTABLE (forbidden).
Required	Full rate	Required	Full rate	Not Applicable	Call is cleared if N2 failure received due to one of the following reasons: • Encryption and integrity protection algorithms not supported • UP integrity protection not possible.
Preferred	64 kbps	Preferred	64 kbps	Performed or Not performed	
Preferred	Null	IE not included	IE not included	Not Applicable	

UPIP Status	UPIP Data Rate	N2 UPIP Indication	N2 Security Data Rate	N2 Security Result	Comment
Preferred	Full rate	Preferred	Full rate	Performed or Not performed	
Not required or none	Not Applicable	IE not included	IE not included	Not Applicable	
Not required or none	Not Applicable	IE not included	IE not included	Not Applicable	
Not required or none	Not Applicable	IE not included	IE not included	Not Applicable	

If the data rate configured locally on SMF is less than the UE requested value, SMF sends the UE requested value to gNB unless the locally configured value is null.

SMF receives the maximum data rate per UE for user plane integrity protection in N1 PDU session establishment request. If the UP security subscription indicates that UPIP is required, then the SMF compares the UE requested data rate with the configured data rate. If the UE requested data rate is low, SMF rejects PDU establishment with 5GSM cause value #82 "maximum data rate per UE for user-plane integrity protection is too low". SMF triggers N11 response including SmContextCreateError with 403 forbidden--INTEGRITY_PROTECTED_MDR_NOT_ACCEPTABLE failure message.

For details on the configuration of UPIP status and data rates, see the Configuring UP Integrity Protection, on page 678 section.

If the CLI command is configured to continue, then call will be continued without enabling UPIP. This CLI is applicable to UPIP status "REQUIRED" only.

SMF marks interworking functionality (IWK) as disabled if the UPIP indication is sent as “required” in N2 Security Indication in the N2 setup request during PDU session establishment. For such sessions, the EBI assignment procedure is not triggered and MappedEpsbearerContext is not included in ePCO.

SMF rejects N11 retrieve message with 403 forbidden, if IWK is marked as disabled. NR to Wi-Fi HO is rejected if UPIP is active in NR with indication set to “required”. CSR from Wi-Fi RAT with HI=1 is rejected with cause "Denied in RAT"

Session create request in 4G or Wi-Fi RAT is rejected with cause “Denied in RAT", if UDM subscription indicates UPIP is “required” or if configuration indicates UPIP is “required”.

Session create request in 4G or Wi-Fi RAT is accepted if UDM subscription or local configuration indicates that UPIP is “preferred”.

4G to 5G Handover (HO) for a UPIP active session with “preferred” is accepted, but UPIP is not enabled if UE capable data rate is not available.

UE triggers an N1 modification to update data rate and SMF enables UPIP during subsequent N2 setup (that is, idle mode exit or subsequent HO to 5G).

SMF includes N2 security indication with UPIP indication and UPIP data rate in N2 message during UE triggered service request procedure if the UPIP enforcement status indicates one of the following values:

- required
- preferred:performed

- preferred:not-performed

UPIP Status Handling in Handovers and Other Procedures

This section describes how the UPIP enforcement value is calculated and UPIP is negotiated during the different handover scenarios and other procedures.

In the case of first HO to NR from EUTRA, hSMF extracts UPIP data rate and applies the algorithm to decide UPIP enforcement values.

If UPIP enforcement value is preferred and if the gNB is unable to fulfill the data rate, vSMF includes NotifyList in HSMFUpdateData with notification cause set as UP_SEC_NOT_FULFILLED and forwards the security result that is received from gNB to hSMF in securityResult IE in N16 HSMFUpdateData.

UPIP Negotiation During Xn Handover

Path switch transfer IE in path switch request contains user plane security information which has Security Result and Security Indication. If the locally stored value is different from what is received in path switch, SMF includes the local value in Security Indication in Path Switch Acknowledge Transfer message. The SMF logs this event as a warning. If the Security Indication that is received in the path switch acknowledge is different than what is already applied, target gNB corrects the value and sends N2 modification indication.

If the target gNB is unable to provide the UPIP which was active in source gNB before Xn handover for “upip required” case, the SMF triggers the release of specific PDU sessions by including “pdu session resource failed to setup list” with the corresponding PDU session ID in the path switch request. If the target gNB unable to provide UPIP for any of the active sessions, then it rejects the handover attempt and source gNB decides to release the session.

SMF changes the UPIP status from not-performed to performed during Xn HO, if the source gNB indicates the incapability to support the requested UPIP before HO and security result in path switch indicates “performed”.

UPIP Negotiation During 4G or Wi-Fi to 5G Handover

For preferred cases, UPIP is disabled during HO from 5G to 4G or Wi-Fi. Similarly, UPIP is enabled during HO from 4G or Wi-Fi to 5G.

UPIP Negotiation During Idle to Active Transition

If N2 setup failure is received with cause “UE maximum integrity protected data rate reason”, SMF triggers session release. UPIP status is enabled (performed) or disabled (not-performed) during idle mode exit and the UPIP status is updated in CDL.

UPIP Negotiation During N2 Handover

SMF sends the UP security policy of UE to the target gNB through the target AMF. The target gNB rejects all PDU sessions if it cannot comply with the corresponding UP security policy and indicates the reject cause to the SMF through the target AMF. For all other PDU sessions, the target gNB activates UP integrity protection per DRB according to the UP security policy. If N2 failure is received with cause “UE maximum integrity protected data rate reason”, SMF triggers session release.

SMF receives indication on the integrity protection rate capability from gNB by including security result in PDU Resource Modify Indication Transfer message. SMF updates the UPIP enforcement action (performed or not-performed) in “preferred” case based on the integrity protection rate capability. SMF does not take any other action on receiving this. This is applicable only for preferred case.

Standards Compliance

The User Plane Integrity Protection feature complies with the following standards:

- *3GPP specification 24.501, Version 15.4.0*
- *3GPP specification 38.413, Version 15.4.0*
- *3GPP specification 29.503, Version 15.4.0*
- *3GPP specification 29.502, Version 15.4.0*

Configuring UP Integrity Protection

SMF applies UP Integrity Protection at gNB based on UP integrity protection parameters.

To configure the UP integrity protection parameters, use the following sample configuration:

```
config
    profile dnn dnn_profile_name
        upip status { required | preferred | not-needed }
        upip data-rate dl { 64kbps | max-ue-rate | null } ul { 64kbps |
max-ue-rate | null } restrict-action { continue | terminate } }
        end
```

NOTES:

- **upip status { required | preferred | not-needed }**—Specify local configuration for UPIP if not received in subscription from UDM.
- **upip data-rate dl { 64kbps | max-ue-rate | null } ul { 64kbps | max-ue-rate | null } restrict-action { continue | terminate } }**—Configure the UPIP data rate for downlink and uplink traffic.

  Specify one of the following actions to be taken based on the configured data rate and UE capable data rate.

  - continue
  - terminate

  Default action is terminate for UPIP status=required and continue for other UPIP status.

  If continue is configured, then call will be continued without enabling UPIP. Please note that retrict-action configuration is applicable only for UPIP status “REQUIRED”.

The following is an example of the UP integrity protection configuration.

```
profile dnn intershat
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:47
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 dcnr true
 upip status required
 upip data-rate dl max-ue-rate ul max-ue-rate restrict-action terminate
 exit
```

Verifying UP Integrity Protection Configuration

To display the UPIP enforcement status and the UPIP enforcement data rates, use the **show subscriber** command at the global configuration level.

The following is an output of the **show subscriber** command.

```
Upip-enforcement-status: [required|preferred]: [performed|not-perfomed]

Upip-enforcement-datarate-dl: 64kbps/max-ue-rate
Upip-enforcement-datarate-ul: 64kbps/max-ue-rate
```

Note The performed/not-performed details are applicable only to “preferred” UPIP status which is updated based on the gNB response. The data rates are visible only in UPIP enabled cases (required/preferred:performed).

To display the number of subscribers with UPIP enforcements active, use the **show subscriber count** command. This output is updated on receiving N2 Modification indication with fulfil or not-fulfil.

To display the number of sessions activated with UPIP, use the **subscriber namespace smf count upip true** command.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics are available in support of UP Integrity Protection feature.

- smf_service_stats: This statistics includes “upip_active” label to indicate whether or not UPIP is activated for the session.

  This statistic also includes new failure reasons for the following scenarios:

  - 5G to 4G HO failure when UPIP has been enabled in 5G with status=REQUIRED – “upip_req_denied_in_rat”
  - NR to WIFI HO failure when UPIP has been enabled in 5G with status=REQUIRED – “nr_to_untrusted_wifi_upip_status_req_denied_in_rat”.

- smf_disconnect_stats: This statistics includes new failure reasons for the following failure scenarios.
  - 5G call failure when UE requested data rate is less than the SMF supported data rate for enabling UPIP with status=REQUIRED – “disc_pdusetup_integrity_protected _mdr_not_acceptable”.
  - 4G or Wi-Fi call failure when UDM subscription response has UPIP status=REQUIRED – “disc_pdnsetup_upip_ status_req_denied_in_rat”.
  - 5G to 4G HO failure when UPIP has been enabled in 5G with status=REQUIRED – “upip_ req_denied_in_rat”.
  - NR to Wi-Fi HO failure when UPIP has been enabled in 5G with status=REQUIRED – “nr_to_untrusted_wifi_upip_status _req_denied_in_rat”.

- smf_n2_message_stats: This statistics includes these cause values “n2_cause” – “_UP_integrity_protection_not_possible” or “_Encryption_and_or_integrity_

protection_algorithms_not_supported” if failure response received from gNB for N2 setup request indicating enable UPIP with status=REQUIRED.

N7 Interface

The N7 interface is the reference point between the SMF and the Policy Control Function (PCF) during session establishment or modification.

PCF uses the policy control for session management. This network function implements N7 interface to trigger session management policies towards SMF. SMF controls the User plane Function (UPF) and translates policies that it receives from PCF to the information that the UPF understands and then forwards it to the UPF.

Error Handling with HTTP Error Codes

Feature Description

SMF supports error responses and the related HTTP error codes for the SM Policy Update Notify service towards PCF with this release. For this feature, SMF complies with 3GPP TS 29.512, section 4.2.3.2—SM Policy Association Update request.

How it Works

SMF responds with the error details and HTTP error codes to the SM Policy Update Notify service from PCF.

Call Flows

This section describes the call flow of the SM Policy Update Notify service from PCF.

Figure 159: SM Policy Update Notify Service from PCF

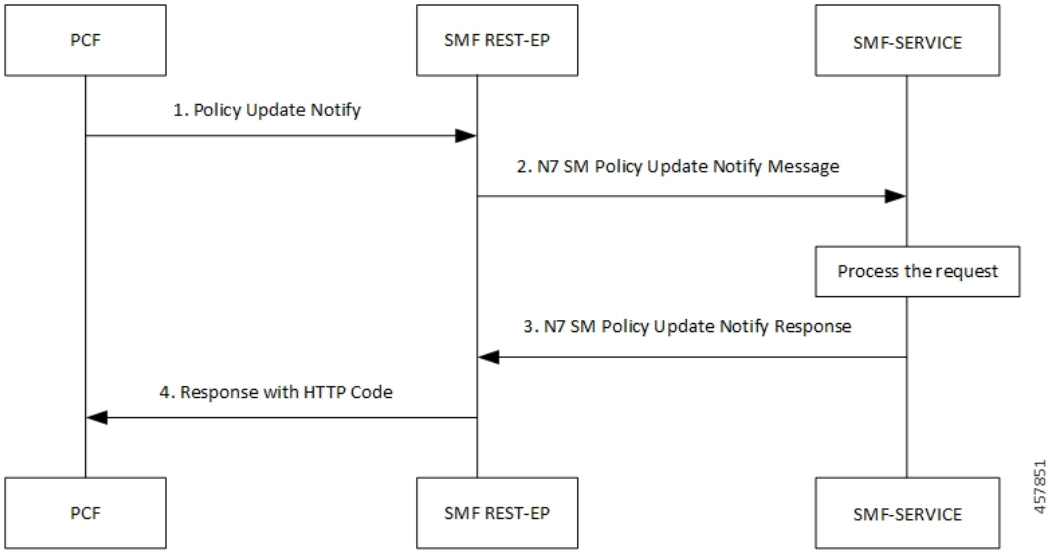


Table 261: SM Policy Update Notify Service from PCF Call Flow

Step	Description
1	PCF sends the Policy Update Notify request to SMF REST-EP.
2	SMF REST-EP sends the N7 SM Policy Update Notify message to SMF-service for processing.
3	SMF-service processes the request and sends a response with either success details or failure details to PCF.
4	SMF-RESTEP processes a response with HTTP codes and the required data structures, and then sends the response to PCF.

SMF Error Handling

SMF handles the HTTP error codes towards PCF through the following validations:

- SMF handles the RuleStatus enumeration in the RuleReport data structure. This data structure works on the following guidelines:
  - Validate the installed or activated Policy and Charging Control (PCC) rule for a PDU session. If the validation fails, the RuleStatus enumeration shows the configuration as "inactive".
  - Validate the updated PCC rule in a PDU session. If the validation fails, the RuleStatus enumeration shows the configuration as "active".
- SMF handles the RuleStatus enumeration in the SessRuleReport data structure. This data structure works on the following guidelines:
  - Validate that an installed or activated Session Rule exists for PDU session. If the validation fails, then the SessionRuleStatus attribute shows the configuration as "inactive".
  - Validate that the updated Session Rule exists after activation or installation in a PDU session. If the validation fails, then the SessRuleStatus attribute shows the configuration as "active".
- SMF handles the cause by using the FailureCause enumeration in ProblemDetails when a PCC rule fails due to validation.
  - Use PCC_RULE_EVENT for PCF to retry connection with SMF. You can view the error details in the "InvalidParams" attribute.
- SMF handles the cause by using the FailureCause enumeration in ProblemDetails when a SessionRule fails due to validation.
  - Use RULE_PERMANENT_ERROR for PCF to retry connection with SMF. You can view the error details in the “InvalidParams” attribute.
- SMF handles SessionRuleFailureCode in the SessionRuleReport data structure, which works on the following guideline:
  - Use only UNSUCC_QOS_VAL as the supported value for this release.

- SMF handles SessionRuleFailureCode in the SessionRuleReport data structure, which works on the following guideline:
  - Use UNSUCC_QOS_VAL as the supported value.
- SMF supports the ProblemDetails JSON object to show error details in the HTTP response body. With this object, the SMF service includes a "Content-Type" header field configured to "application/problem+json".

Error Codes

Following table lists the error codes that SMF uses for error handling:

Table 262: Error Codes with Details

Number	Enum	Details	SMF Support
1	UNK_RULE_ID	Indicate that the preprovisioned PCC rule isn't activated. This error occurs when SMF has no information on the PCC rule identifier.	Yes
2	RA_GR_ERR	Indicate that the PCC rule isn't activated or enforced. This error occurs when the PCC rule referring to the specified Rating Group, in the Charging Data policy decision, is unknown or invalid.	Yes
3	SER_ID_ERR	Indicate that the PCC rule isn't activated or enforced. This error occurs when PCC rule referring to the specified service identifier, in the Charging Data policy decision, is invalid, unknown, or not applicable to the service being charged.	Yes
4	NF_MAL	Indicate that the PCC rule isn't installed, activated, or enforced due to SMF or UPF functionality issues. The PCC rule installation is for the rules provisioned from PCF. The PCC rule activation is for the rules predefined in SMF. The PCC rule enforcement is for the installed rules.	No
5	RES_LIM	Indicate that the PCC rule isn't installed, activated, or enforced due to limitation of resources at the SMF or UPF.	No

Number	Enum	Details	SMF Support
6	MAX_NR_QoS_FLOW	Indicate that a PDU session has reached the maximum number of QoS flows.	Yes
7	MISS_FLOW_INFO	Indicate that the PCC rule isn't installed. This error occurs when PCF fails to specify either the "flowInfos" attribute or the "appId" attribute in the PccRule data structure during the first installation request of the PCC rule.	Yes
8	RES_ALLO_FAIL	Indicate that the PCC rule isn't installed or maintained. This error occurs due to the QoS flow establishment, modification failure, or release of the QoS flow.	Yes
9	UNSUCC_QOS_VAL	Indicate QoS validation failure or when the Guaranteed Bandwidth is more than the maximum requested bandwidth.	Yes
10	INCOR_FLOW_INFO	Indicate that the PCC rule isn't installed or modified at SMF. This error occurs when the network doesn't support the flow information, such as IP address or an IPv6 prefix doesn't correspond to the applicable IP version for the PDU session.	Yes
11	PS_TO_CS_HAN	Indicate that the PCC rule isn't maintained due to packet switched (PS) to circuit switched (CS) handover.	No
12	APP_ID_ERR	Indicate that the PCC rule isn't installed or enforced. This error occurs due to invalid, unknown, or nonapplicable application identifier that an application requires for detection.	No
13	NO_QOS_FLOW_BOUND	Indicates that no QoS flow exists for the SMF to associate the PCC rules to.	Yes

Number	Enum	Details	SMF Support
14	FILTER_RES	Indicates that the SMF is unable to handle the flow information in "flowInfos". This error occurs when the restrictions defined in subclause 5.4.2 of 3GPP TS 29.212 [23] aren't met.	Yes
15	MISS_REDI_SER_ADDR	Indicate that the PCC rule isn't installed or enforced at the SMF. This error occurs when PCF doesn't provide a valid redirect server address in the Traffic Control Data policy decision for the PCC rule and no pre-configured redirection address for this PCC rule exists at the SMF.	No
16	CM_END_USER_SER_DENIED	Indicate that the charging system denied the service request due to service restrictions. For example, termination of rating group or end-user related limitations, such as the end-user account doesn't include the requested service.	No
17	CM_CREDIT_CON_NOT_APP	Indicate that the charging system determined that the service can be granted to the end user. However, no credit control is applicable for the service. For example, a service is free of charge or available for offline charging.	No
18	CM_AUTH_REJ	Indicate that the charging system denied the service request to terminate the service for which an end user requested a credit.	No
19	CM_USER_UNK	Indicate that an end-user information in unavailable in the charging system.	No
20	CM_RAT_FAILED	Indicate that the charging system can't rate the service request. This error occurs due to insufficient rating input, incorrect AVP combination, or because of an unrecognized or unsupported attribute value in the rating.	No

Number	Enum	Details	SMF Support
21	UE_STA_SUSP	Indicates that the UE is in the suspended state. **Note** This error is applicable only to the interworking scenario, as defined in Annex B of the 3GPP specification.	No

Configuration-based Control of PCF Messages

Feature Description

SMF provides flexibility to the operator to either include or exclude certain optional Information Elements (IEs) in the PCF messages. Operators can choose the IEs through the CLI configuration commands.

A particular peer NF may not support an optional IE in the PCF messages. In this case, the SMF configures the **skip optional-ies** CLI command in the PCF message handling profile configuration. The SMF always sends the optional IEs to the PCF through the N7 interface.

Important The controlled inclusion of IEs is limited to only the userLocationInfoTime IE.

The PCF message is a combination of the following messages.

- smPolicyControlCreate
- smPolicyControlUpdate
- smPolicyControlDelete

For details on the configuration commands, see the Configuring Control for Optional IEs, on page 686 section.

How it Works

SMF supports PCF message handling profile configuration. With this configuration, you can control the optional IEs. SMF sends these IEs to PCF in the SM Policy Control Create, SM Policy Control Update, and SM Policy Control Delete messages.

Feature Configuration

The feature for configuration-based control of PCF messages includes the following steps:

1. Configuring Message Handling Profile, on page 685
2. Configuring Control for Optional IEs, on page 686

Configuring Message Handling Profile

To configure the PCF message handling profile, use the following sample configuration:

```
config
  profile network-element pcf pcf_profile_name
```

```
nf-client-profile profile_name
message-handling-profile message_handling_profile_name
end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the PCF client profile. *profile_name* must be an alphanumeric string representing the corresponding PCF profile name.
- **message-handling-profile** *message_handling_profile_name*: Specify the message handling profile name for PCF messages.

Configuration Verification

Use the following command to verify if the message handling profile is configured.

show running-config profile message-handling nf-type pcf mh-profile

If the message handling profile is configured, then the value appears as part of the **message-handling-profile** configuration in the following output.

```
smf(config)# show running-config profile message-handling nf-type pcf mh-profile
 profile network-element pcf nfprf-pcf1
 nf-client-profile udm-profile
 message-handling-profile MHPCF
 exit
```

Configuring Control for Optional IEs

To configure the control to skip the optional IEs, use the following sample configuration:

```
config
  profile message-handling message_handling_name
    nf-type pcf
      mh-profile mh_profile_name
        service name type npcf-smpolicycontrol
          message type { PcfSmpolicycontrolCreate |
PcfSmpolicycontrolDelete | PcfSmpolicycontrolUpdate }
            skip optional-ies [ userLocationInfoTime ]
            end
```

NOTES:

- **mh-profile** *mh_profile_name* : Specify the PCF message handling profile configuration.
- **service name type npcf-smpolicycontrol**: Specify the policy control service name type.
- **message type { PcfSmpolicycontrolCreate | PcfSmpolicycontrolDelete | PcfSmpolicycontrolUpdate }**: Specify the message type as PCF SM Policy Control Create, PCF SM Policy Control Delete, or PCF SM Policy Control Update.
- **skip optional-ies [userLocationInfoTime]**: Specify the parameter that you want to skip for the selected PCF message.

Important The controlled inclusion of IEs is limited to only the userLocationInfoTime IE.

Configuration Verification

To verify if the control to skip the optional IEs is configured, use the following command at the Exec mode:

show running-config profile message-handling nf-type pcf

You can also verify the feature configuration using the following show command at the Global Configuration mode.

show full-configuration profile message-handling nf-type pcf

The following is an example output of the **show running-config profile message-handling nf-type pcf** command.

```
[smf] smf# show running-config profile message-handling nf-type pcf
profile message-handling nf-type pcf
 mh-profile mh1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolUpdate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolDelete
    skip optional-ies [ userLocationInfoTime ]
   exit
  exit
 exit
exit
```

The following is an example output of the **show full-configuration profile message-handling nf-type pcf** command.

```
[smf] smf(config)# show full-configuration profile message-handling nf-type pcf
profile message-handling nf-type pcf
 mh-profile mh1
  service name type npcf-smpolicycontrol
   message type PcfSmpolicycontrolCreate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolUpdate
    skip optional-ies [ userLocationInfoTime ]
   exit
   message type PcfSmpolicycontrolDelete
    skip optional-ies [ userLocationInfoTime ]
   exit
  exit
 exit
exit
```

In the preceding examples, check the **skip optional-ies** configuration to determine whether or not the optional IEs are skipped and the message types where this configuration is enabled.

N10 Interface

During session establishment or modification, the SMF communicates with the PCF over the N7 interface and the subscriber profile information that is stored in the Unified Data Management (UDM) function on the N10 interface.

Configuration-based Control of UDM Messages

Feature Description

SMF provides flexibility to the operator to either include or exclude certain URI query parameters in the UDM message through the CLI configuration commands.

A particular query parameter may not be included in the UDM message (N10 Get Subscription Request message). In this case, the SMF configures the **skip uri-query-params** CLI command in the UDM message handling profile configuration. By default, the SMF sends all the query parameters to the UDM through the N10 Get Subscription Fetch Request message.

For details on the configuration commands, see the Configuring Control for URI Parameters, on page 689 section.

Feature Configuration

The feature for configuration-based control of UDM messages includes the following steps:

1. Configuring Message Handling Profile, on page 688
2. Configuring Control for URI Parameters, on page 689

Configuring Message Handling Profile

To configure the UDM message handling profile, use the following sample configuration:

```
config
  profile network-element udm udm_profile_name
    nf-client-profile profile_name
    message-handling-profile message_handling_profile_name
    end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the UDM client profile. *profile_name* must be an alphanumeric string representing the corresponding UDM profile name.
- **message-handling-profile** *message_handling_profile_name*: Specify the message handling profile name for UDM messages.

Configuration Verification

To verify if the UDM message handling profile is configured, use the following command:

show running-config profile network-element udm

If the message handling profile is configured, then the value appears as part of the **message-handling-profile** configuration in the following output.

```
[smf] smf# show running-config profile network-element udm
profile network-element udm udm1
 nf-client-profile udm12
 failure-handling-profile fh1
 query-params [ dnn ]
 message-handling-profile MHUDM
 response-timeout 5000
exit
```

Configuring Control for URI Parameters

To configure the control to skip the URI query parameters, use the following sample configuration:

```
config
  profile message-handling message_handling_name
    nf-type udm
      mh-profile mh_profile_name
        service name type nudm-sdm
          message type UdmSdmGetUESMSubscriptionData
            skip uri-query-params
            end
```

NOTES:

- **mh-profile** *mh_profile_name* : Specify the UDM message handling profile configuration.
- **service name type nudm-sdm**: Specify the service name type as nudm-sdm from the available options for UDM.
- **message type UdmSdmGetUESMSubscriptionData**: Specify the message type as UDM SDM Get UE SM Subscription Data.
- **skip uri-query-params**: Specify the parameter to skip for the selected UDM message.

Configuration Verification

To verify if the configuration to skip the URI parameters is enabled, use the following command:

show running-config profile message-handling nf-type udm

The following is an example output of the **show running-config profile message-handling nf-type udm** command.

```
[smf] smf# show running-config profile message-handling nf-type udm
profile message-handling nf-type udm
 mh-profile MHUDM
  service name type nudm-sdm
   message type UdmSdmGetUESMSubscriptionData
    skip uri-query-params [ snssai dnn plmnid ]
   exit
  exit
 exit
exit
```

In the preceding example, check the **skip uri-query-params** configuration to determine the URI query parameters that are configured to be excluded in the N10 Get Subscription Request message.

3GPP Release 16-Compliant N10 Attributes

Table 263: Feature History

Feature Name	Release Information	Description
3GPP Release 16-Compliant Generic UDM Enhancements	2024.01	SMF supports the following enhancements in compliance with 3GPP 29.503, Release 16. • Subscription Level 3GPP Charging Characteristics: When this attribute is available in DNN configuration, this attribute takes precedence over the one received in the SessionManagementSubscriptionData. • ePDG Indication and NF Registration Time: UDM message handling configuration includes additional keyword options to allow or ignore ePDG Indication access information and NF Registration time in the N10 Registration Request. **Default Setting**: Not Applicable

The ePDG indication (epdgInd) and NF registration time (registrationTime) attributes are added to the N10 Registration Request message in compliance with 3GPP TS 29.503, Release 16.

You can disable these attributes using **skip optional-ies** command in the UDM configuration. For more information on the configuration, see the Configuration to Disable Optional IEs secion.

S-NSSAI Validation Against the UDM Subscription S-NSSAI

The SMF uses the Single Network Slice Selection Assistance information (S-NSSAI) from UDM subscription response to reselect the subscriber policy. The SMF matches the S-NSSAI based on the Slice or Service Type (SST) and Slice Differentiator (SD) parameters.

The S-NSSAI subscription selection is based on the following criteria:

- If both the parameters match, then SMF selects the S-NSSAI subscription with both SST and SD matched (fully matched).
- If only SST matches and SD is unavailable in either the requested S-NSSAI or in UDM subscription S-NSSAI, then SMF selects the subscription with SST only matched (partially matched).
- If the requested S-NSSAI partially matches with the SMF local configuration S-NSSAI (allowed snssai under SMF profile), then the local configuration S-NSSAI is used for validating with the UDM subscription response. This criteria is applicable for the 5G call.

The following table lists the validation criteria for selecting subscription from UDM N10 subscription.

Table 264: Validation Criteria for Subscription Selection from UDM N10 Subscription Response

Serving RAT	Selected S-NSSAI before N10 Subscription	S-NSSAI in Subscription	Final S-NSSAI after N10 Subscription
5G	Requested S-NSSAI that is received in Create message	Single S-NSSAI in subscription	Subscribed S-NSSAI, which matches with requested S-NSSAI.
5G	Requested S-NSSAI that is received in Create message	Multiple S-NSSAI in subscription	Subscribed S-NSSAI, which matches with requested S-NSSAI.
4G or Wi-Fi	Requested S-NSSAI (default S-NSSAI configured under DNN profile. If the default S-NSSAI isn't available, then one of the allowed S-NSSAIs available under SMF profile is selected).	Single S-NSSAI in subscription	Subscribed S-NSSAI, which matches with the requested S-NSSAI or the requested DNN or APN available in the Create Session Request (CSR).
4G or Wi-Fi	Requested S-NSSAI (default S-NSSAI configured under DNN profile. If the default S-NSSAI isn't available, then one of the allowed S-NSSAIs available under SMF profile is selected)	Multiple S-NSSAI in subscription	Subscribed S-NSSAI, which matches with the requested S-NSSAI or the requested DNN or APN available in the Create Session Request (CSR).

The following table provides details on SMF and UDM behavior based on the availability of the query parameters in the N10 Subscription Request message.

Table 265: URI Query Parameters in UDM N10 Get Subscription Request

Configuration	URI Parameters in N10 Subscription	UDM Behavior	SMF N10 Subscription Response Handling
Default or no configuration	PLMN, Selected SNSSAI, DNN	UDM uses requested PLMN and sends subscription that matches the S-NSSAI and DNN.	SMF selects the S-NSSAI subscription that matches the requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from the selected subscription.
Skip PLMN	Selected S-NSSAI, DNN	UDM uses home PLMN and sends subscription that matches the S-NSSAI and DNN.	SMF selects S-NSSAI subscription that matches with the requested S-NSSAI and selects the DNN configuration that matches the requested DNN from selected subscription.

Configuration	URI Parameters in N10 Subscription	UDM Behavior	SMF N10 Subscription Response Handling
Skip S-NSSAI	PLMN, DNN	UDM uses requested PLMN and responds with the S-NSSAI subscriptions that match DNN.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from the selected subscription.
Skip DNN	Selected S-NSSAI, PLMN	UDM uses the requested PLMN and sends S-NSSAI subscriptions that match S-NSSAI.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from selected subscription.
Skip PLMN, S-NSSAI	DNN	UDM uses home PLMN and sends all the S-NSSAI subscriptions that match DNN.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from selected subscription.
Skip PLMN, DNN	S-NSSAI	UDM uses home PLMN and sends S-NSSAI subscriptions matching S-NSSAI.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from selected subscription.
Skip S-NSSAI, DNN	PLMN	UDM uses requested PLMN and sends all the S-NSSAI subscriptions.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from selected subscription.
Skip PLMN, S-NSSAI, DNN	None	UDM uses home PLMN and sends all the S-NSSAI subscriptions.	SMF selects S-NSSAI subscription that matches with requested S-NSSAI and selects the DNN configuration that matches with the requested DNN from selected subscription.

N11 Interface

The N11 interface is the reference point between the Access and Mobility Management Function (AMF) and SMF.

To request a new session, both the UE and the gNB use the Next Generation Application Protocol (NGAP) to carry Non Access Stratum (NAS) messages across the N1 or N2 interface. AMF receives these requests

and handles the connectivity and mobility management. Then, the AMF forwards the session management related requirements over the N11 interface to the SMF. The AMF identifies the SMF that can handle the connection request by querying the Network Repository Function (NRF).

The messages that SMF receives over the N11 interface are the requests to add, modify, or delete a PDU session across the user plane.

ProblemDetails JSON Object

Feature Description

SMF supports sending and receiving the ProblemDetails JSON object on the N11 interface and supports roaming.

An application error can prevent the SMF service, acting as an HTTP server, from completing the HTTP request. In this case, the SMF service maps the application error to the similar 4xx or 5xx HTTP status.

An HTTP status code determines the cause of the error. However, sometimes these status codes don't have adequate information about an error. In this case, the SMF service acting as the HTTP server provides more application-related error information to the SMF service acting as an HTTP client. This SMF service provides the additional information by including the representation of “ProblemDetails” data structure in the response body.

3GPP specification defines JSON as one of the document formats. HTTP APIs reuse this format to identify various problem types based on the requirement.

The ProblemDetails structure specified for N11 interface is sent on the N16 interface for roaming call flows on hSMF. After receiving ProblemDetails from hSMF, the vSMF rejects the corresponding message from AMF and saves the ProblemDetails that vSMF receives from hSMF.

Supported Attributes

For this feature, SMF supports the following attributes:

- status—Specifies the HTTP status code for the occurrence of a problem. The HTTP status has the format of 4xx and 5xx, such as 403 and 504.
- cause—Specifies a machine-readable application error cause based on the occurrence of a problem. The 5G core SBI API specifications define the application error causes. As per the specifications, this attribute uses the UPPER_WITH_UNDERSCORE case format, such as UNSPECIFIED_NF_FAILURE",” DNN_NOT_SUPPORTED.
- title—Provides the summary of the problem type. This attribute remains same from one occurrence of the problem to another occurrence. This attribute includes summary, such as invalid parameters, network failure, and mandatory, optional, or conditional IE is missing.
- detail—Provides the human-readable information that is specific to the occurrence of the problem. This attribute includes information, such as UDM registration failure, UDM subscription failure, and sending of invalid parameter in SM Context Create.

Note

- For this feature, SMF supports the title and detail attributes.
- For this feature, SMF does not support the invalidParams attribute.

How it Works

This section describes how this feature works.

If a response includes a payload body with the ProblemDetails data structure, then the SMF service includes a "Content-Type" header field configured to "application/problem+json". The SMF service generates the HTTP response.

Sending Problem Details

SMF sends the problem details to AMF in the following N11 messages.

- SM Context Create Error
- SM Context Update Error
- POST Response to SM Context Release
- POST Response to SM Context Retrieve

Handling Problem Details

SMF handles the problem details structure that SMF receives from AMF and provides roaming support on other SMFs.

EBI Assignment Error with Problem Details

SMF handles this N11 message by not storing any EBIs for the ARP values with the failed EBI assignment. For example, SMF handles an EBI assignment error from AMF with problem details and “EBI_EXAUSTED” cause along with failure details.

N1N2 Transfer Acknowledgment with Problem Details

SMF handles the acknowledgment N11 message according to the HTTP status and cause values in the problem details. For example, SMF handles the N1N2 acknowledgment message with HTTP status as 404 and cause as “CONTEXT_NOT_FOUND” from AMF.

Roaming Between SMFs

The home SMF (hSMF) and visited SMF (vSMF) communicate with each other over the N16 interface. The following sections describe how the ProblemDetails structure specified for N11 interface is sent on N16 interface for roaming call flows for hSMF and vSMF.

Call Flows

This section describes the following call flows:

- Create Service Operation on hSMF Call Flow
- Create Service Operation on vSMF Call Flow
- Update Service Operation towards hSMF Call Flow
- Update Service Operation towards vSMF Call Flow

Create Service Operation on hSMF Call Flow

The Create service operation creates a PDU session in the hSMF for home-routed roaming scenarios. The NF Service Consumer, such as vSMF, creates a PDU session by using the HTTP POST method.

This section describes the Create service operation on hSMF call flow.

Figure 160: Create Service Operation on hSMF Call Flow

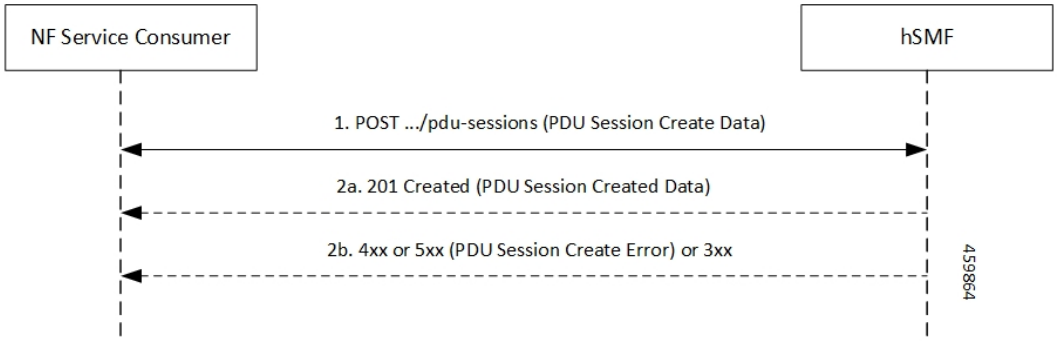


Table 266: Create Service Operation on hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to create a PDU session in hSMF.
2	If the PDU session creation is successful, the hSMF sends the "201 Created" to NF Service Consumer.
3	If the PDU session establishment fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for PDU Session Creation Error table. For the 4xx or 5xx response, the message body contains a PDU Session Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 267: HTTP Status Codes for PDU Session Creation Error

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SUBSCRIPTION _DENIED	UDM_Subscription _Fetch_Failed	Network _Failure
PDU Session Create Error	403	SNSSAI_ DENIED	SNSSAI_Not_ Supported_By_SMF	Network _Failure
PDU Session Create Error	500	UNSPECIFIED _NF_FAILURE	UDM_Notification _Failed	Network _Failure
PDU Session Create Error	404	SUBSCRIPTION _NOT_FOUND	UDM_Subscription _Failed	Network _Failure
PDU Session Create Error	504	NETWORK_ FAILURE	SLA_Txn _Timeout	Network _Failure
PDU Session Create Error	403	DNN_DENIED	DNN_Not_Subscribed	Network _Failure

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SSC_NOT_ SUPPORTED	SSC_Mode_Not _Supported_By_SMF	Network _Failure
PDU Session Create Error	403	SSC_DENIED	SSC_Mode_Denied _From_UDM	Network _Failure
PDU Session Create Error	403	PDUTYPE_DENIED	UDM_Rejected _PDU_Type	Network _Failure

Create Service Operation on vSMF Call Flow

The Create SM Context service operation creates an SM context for a PDU session either in the SMF or in the vSMF for home-routed roaming scenarios. The NF Service Consumer, such as AMF, creates an SM context by using the HTTP POST method.

This section describes the Create service operation on vSMF call flow.

Figure 161: Create Service Operation on vSMF Call Flow

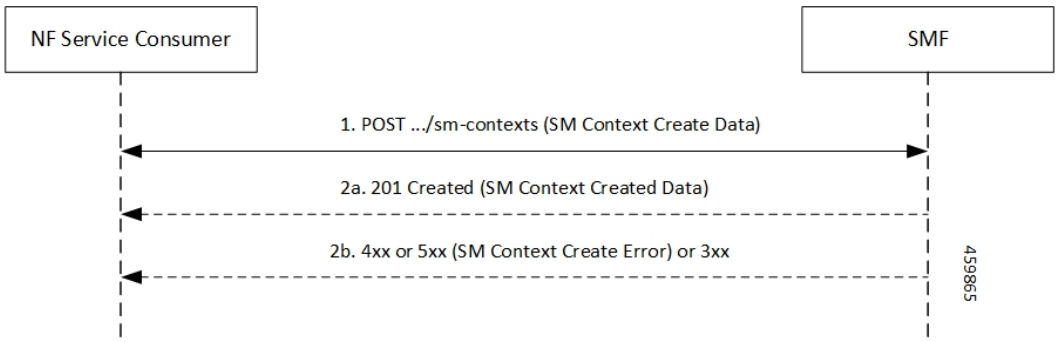


Table 268: Create Service Operation on vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as AMF, sends a POST request to create SM Context to the resource that represents the SM contexts collection resource of the vSMF.
2	If the PDU session creation is successful, the SMF sends the "201 Created" to the NF Service Consumer.
3	If the PDU session establishment fails, the SMF sends the HTTP status code, as listed in the HTTP Status Codes for SM Context Creation Error table. For the 4xx or 5xx response to the NF Service Consumer, the message body contains an SM Context Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 269: HTTP Status Codes for SM Context Create Error

Data Type	HTTPS Status Code	Cause	Details	Title
SM Context Create Error	403	PDUTYPE_ NOT_SUPPORTED	PDU_Type_Not _Supported_ By_SMF	Network _Failure
SM Context Create Error	500	REQUEST_ REJECTED_ UNSPECIFIED	Charging_Response _Failure	Network _Failure
SM Context Create Error	504	NETWORK_ FAILURE	SLA_txn _timeout	Network _Failure
SM Context Create Error	400	MANDATORY_IE _MISSING	PDU_Session_ ID_Not_Sent	Mandatory_IE _Missing

Update Service Operation Towards hSMF Call Flow

The NF Service Consumer, such as vSMF, updates a PDU session in the hSMF. The NF Service Consumer also provides the hSMF with information that NF Service Consumer receives from vSMF in the N1 SM signalling from the UE. The NF Service Consumer uses the HTTP POST method to receive this information.

This section describes the Update service operation towards hSMF call flow.

Figure 162: Update Service Operation Towards hSMF Call Flow

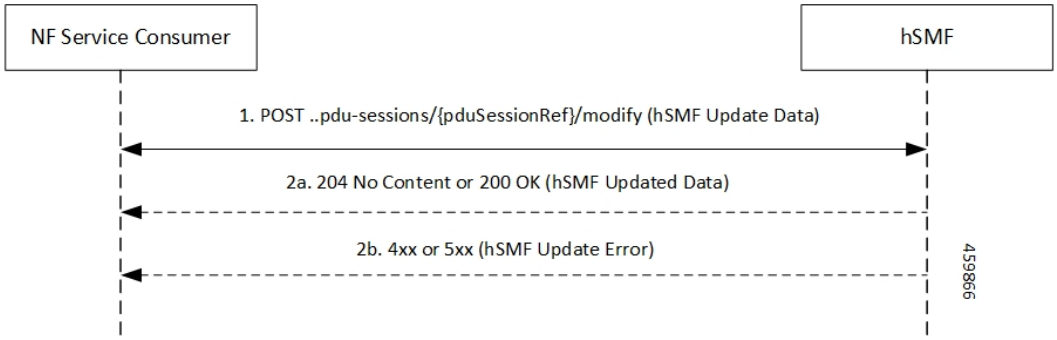


Table 270: Update Service Operation Towards hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the hSMF.
2	If the PDU session update is successful, the hSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.

Step	Description
3	If the PDU session update fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for hSMF Update Error table. For the 4xx or 5xx response, message body contains a hSMF Update Error structure, including the ProblemDetails structure with the "cause" attribute.

Table 271: HTTP Status Code for hSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
hSMF Update Error	404	CONTEXT_NOT _FOUND	PDU_Context _Not_Found	Network _Failure

Update Service Operation Towards vSMF Call Flow

The NF Service Consumer, such as hSMF, updates a PDU session in the vSMF. The NF Service Consumer also provides the required information for the V-SMF to send the N1 SM signalling to the UE by using the HTTP POST method.

This section describes the Update service operation towards vSMF call flow.

Figure 163: Update Service Operation Towards vSMF Call Flow

Table 272: Update Service Operation Towards vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as hSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the vSMF.
2	If the PDU session update is successful, the vSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the vSMF sends the HTTP status code, as listed in the HTTP Status Codes for vSMF Update Error table. For the 4xx or 5xx response, the message body contains a vSMF Update Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 273: HTTP Status Codes for vSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
vSMF Update Error	400	UNSPECIFIED _NF_FAILURE	Ngap_Decode _failed	Invalid_Param
vSMF Update Error	500	UNSPECIFIED _NF_FAILURE	Failure_N4 _Response	Network _Failure
vSMF Update Error	500	SYSTEM_ FAILURE	Procedure _Aborted	Network _Failure
vSMF Update Error	500	INSUFFICIENT_ RESOURCES	Failed_Due_ To_Insufficient_ Resounces_At_Gnb	Network _Failure
vSMF Update Error	400	UNSPECIFIED_ NF_FAILURE	Qfi_Failed _List_Invalid	Network _Failure

Supported Status and Cause Codes

The following table lists the supported status and cause codes for this feature.

Table 274: Supported Status and Cause Codes

Title	Details	HTTP Status	Cause	Message
Network Failure	UDM_Registration _Failed	403	SUBSCRIPTION_ DENIED	SMContext CreateError
Network Failure	SNSSAI_Not_ Supported_By_SMF	403	SNSSAI_ DENIED	
Network Failure	UDM_Subscription _Failed	404	SUBSCRIPTION_ NOT_FOUND	
Network Failure	SLA_Txn_Timeout	504	NETWORK_ FAILURE	
Network Failure	PDU_Type_ Not_Supported _By_SMF	403	PDUTYPE _NOT _SUPPORTED	
Network Failure	UDM_Rejected _PDUTYPE	403	PDUTYPE _DENIED	
Network Failure	DDN_Not_Supported _By_SMF	403	DNN_NOT _SUPPORTED	
Network Failure	DDN_Denied_By _UDM_Or_UDM_ Sent_Different_ DNN	403	DDN_DENIED	
Network Failure	SSC_Not_Supported _By_SMF	403	SSC_NOT _SUPPORTED	
Network Failure	SSC_Denied_ From_UDM	403	SSC_DENIED	
Network Failure	N26_HO_Failure _N4_Response	504	NETWORK_ FAILURE	
Mandatory_IE _Missing	PDU_Session_ID _Not_Sent	400	MANDATORY _IE _MISSING	
Network Failure		403		

Title	Details	HTTP Status	Cause	Message
	N26_HO_Movement _Default_Bearer _Inactive		DEFAULT_EPS_ BEARER_ INACTIVE	
Network Failure	Failed_Due_To _Insufficient_ Resources_At _Gnb	500	INSUFFICIENT _RESOURCES	SMContext UpdateError
Network Failure	No_Resource_Is_ Allocated_By_The _Target_NGRAN	403	HANDOVER_ RESOURCE_ ALLOCATION_ FAILURE	
Network Failure	SLA_Txn_Timeout	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	N2HO_N4 _Reject	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	XNHO_N4_Reject	500	UNSPECIFIED_ NF_FAILURE	
Network Failure	SLA_Txn_Timeout	500	UNSPECIFIED_ NF_FAILURE	POST Response SMContext Release
Network Failure	SLA_Txn_Timeout	504	NETWORK_ FAILURE	POST Response to SMContext Retrieve

Standards Compliance

The ProblemDetails JSON object support feature complies with the following standards.

- *3GPP TS 29.502—5G System; Session Management Services*
- *3GPP TS 29.518—5G System; Access and Mobility Management Services*
- *3GPP TS 29.571—5G System; Common Data Types for Service Based Interfaces*
- *3GPP TS 29.501—5G System; Principles and Guidelines for Services Definition*

Cause Information Elements

Feature Description

SMF supports cause IE on N11 interface message. With this feature:

- SMF supports sending and handling the received causes, which are available in Cause IE. For this support, SMF complies with the 3GPP TS 29.502 version 15.4.0.0, section 6.1.6.3.8.
- SMF supports the following 3GPP Change Requests (CR):
  - 3GPP TS 29.502, CR 0097 to send the new "INSUFFICIENT_UP_RESOURCES" cause information.
  - 3GPP TS 29.518 CR 161 not to support the UE_IN_NON_ALLOWED_AREA cause in N1N2 Message Transfer Error from AMF.
- SMF supports the statistics for the causes on the N11 interface messages.

How it Works

This feature works with the following support:

- Cause sending and handling support
- 3GPP CR support for CR0097 and CR 161
- Statistics support

Cause Sending and Handling

SMF supports sending and handling of the following received causes:

- REL_DUE_TO_HO
- EPS_FALLBACK
- REL_DUE_TO_UP_SEC
- DNN_CONGESTION
- S_NSSAI_CONGESTION
- REL_DUE_TO_REACTIVATION
- 5G_AN_NOT_RESPONDING
- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_DUPLICATE_SESSION_ID
- PDU_SESSION_STATUS_MISMATCH
- HO_FAILURE
- INSUFFICIENT_UP_RESOURCES
- PDU_SESSION_HANDED_OVER

Cause Description and Scenarios

This section provides information on the causes that SMF receives from AMF through N11 interface messages and the relevant scenarios of those causes.

REL_DUE_TO_HO

The following table describes the release due to handover cause and scenario.

Table 275: Release due to Handover Cause and Scenario

Cause	REL_DUE_TO_HO
Cause Description from 3GPP TS 29.502	Release due to handover
Scenario of occurrence	Handover from 5GS to EPG or ePDG during roaming
Message Used	vsmfUpdateData
Message Direction	H-SMF to V-SMF
Comments and Specification References	3GPP TS 29.502 • 5.2.2.8.3 Update service operation towards V-SMF • 5.2.2.8.3.4 Handover between 3GPP and untrusted non-3GPP access, from 5GC-N3IWF to EPS or from 5GS to EPC/ePDG If the request indication in the request is configured to NW_REQ_PDU_SES_REL and if the Cause IE indicates the release due to handover cause, then the V-SMF initiates the release of RAN resources reserved for the PDU session, if any. However, SMF doesn't send a PDU session release command to the UE. The V-SMF doesn't release the SM context for the PDU session. **Note** • SMF doesn't support the roaming feature for this cause. • This cause is available in the SmContext release request after the N2 handover. SMF supports this scenario.

EPS_FALLBACK

The following table describes the mobility due to EPS fallback for IP Multimedia Subsystem (IMS) voice cause and the scenario of occurrence of the cause:

Table 276: Release due to EPS Fallback Cause and Scenario

Cause	EPS_FALLBACK
Cause description from 3GPP TS 29.502	Mobility due to ongoing EPS fallback for IMS voice.
Scenario of occurrence	IMS voice configuration in roaming scenario

Message used	VsmfUpdatedData This message is used in the qosFlowsFailedtoAddModList attribute, which is the Cause IE of QosFlowItem.
Message direction	V-SMF to H-SMF
Comments and Specification References	SMF supports the following scenarios for this cause as per the specification: • 3GPP TS 23.502, Section 4.13.6.1 for EPS fallback for IMS voice. The PDU Session Response message towards the SMF receives the QoS flow for IMS voice through AMF. For roaming scenario, this message is sent towards H-SMF through V-SMF. NG-RAN rejects the PDU Session modification to configure the QoS flow for IMS voice indicating the ongoing mobility due to fallback for IMS voice. • 3GPP TS 23.502 If the NG-RAN rejects the establishment of a voice QoS flow due to EPS Fallback for IMS voice, as defined in 3GPP TS 23.502 [3], clause 4.13, the V-SMF returns the cause. V-SMF indicates the cause as ongoing mobility due to EPS fallback for IMS voice for the corresponding flow in the qosFlowsFailedtoAddModifyList IE. **Note** This scenario doesn't support roaming.

REL_DUE_TO_UP_SEC

The following table describes the release due to unfulfilled security requirements from User Plane cause and the scenario of occurrence of the cause:

Table 277: Release due to User Plane Cause and Scenario

Cause	REL_DUE_TO_UP_SEC
Cause description from 3GPP TS 29.502	Release due to unfulfilled User Plane security requirements.
Scenario of occurrence	AMF-initiated release when the NG-RAN is unable to fulfill the required User Plane security enforcement.
Message used	Release SM Context service operation
Message direction	AMF to SMF
Comments or Specification References	3GPP 29.502, Section 5.2.2.4, Release SM Context service operation The REL_DUE_TO_UP_SEC cause is available in SM Context Release Request when NG-RAN is unable to fulfill the required User Plane security enforcement.

DNN_CONGESTION

The following table describes the release due to the DNN-based congestion control cause and the scenario of occurrence of the cause:

Table 278: Release due to DNN Congestion Cause and Scenario

Cause	DNN_CONGESTION
Cause Description from 3GPP TS 29.502	Release due to the DNN-based congestion control.
Scenario of occurrence	SMF detects congestion for the requested DNN and performs an overload control for the DNN that restricts the establishment of the PDU session.
Message Used	SM Context Create Error and SM Context Update Error
Message Direction	SMF to AMF
Comments or Specification References	Not supported.

S_NSSAI_CONGESTION

The following table describes the release due to the S-NSSAI-based congestion control cause and the scenario of occurrence of the cause:

Table 279: Release due to S NSSAI Cause and Scenario

Cause	S_NSSAI_CONGESTION
Cause description from 3GPP TS 29.502	Release due to the S-NSSAI-based congestion control.
Scenario of occurrence	SMF detects congestion for the requested S-NSSAI and performs overload control for the S-NSSAI that restricts the establishment of the PDU session.
Message used	SM Context Create Error and SM Context Update Error
Message direction	SMF to AMF
Comments or specification references	Not supported.

REL_DUE_TO_REACTIVATION

The following table describes the release due to PDU session reactivation cause and scenario of its occurrence:

Table 280: Release due to Reactivation Cause and Scenario

Cause	REL_DUE_TO_REACTIVATION
Cause Description from 3GPP TS 29.502	Release due to PDU session reactivation.

Scenario of occurrence	3GPP TS 29.502, Section 5.2.2.3.10, P-CSCF Restoration Procedure via AMF. The POST request contains the release IE configured to True and the cause IE configured to REL_DUE_TO_REACTIVATION.
Message used	Update SM Context service operation
Message direction	AMF to SMF
Comments or specification references	After receiving the cause from AMF, SMF sends the 5GSM cause as Reactivation Required towards UE.

5G_AN_NOT_RESPONDING

The following table describes the cause when 5G access network (AN) doesn't respond to network-initiated request and the scenario of occurrence of the cause:

Table 281: Release due to 5G AN Not Responding Cause and Scenario

Cause	5G_AN_NOT_RESPONDING
Cause Description from 3GPP TS 29.502	The 5G AN doesn't respond to the network-initiated request.
Scenario of occurrence	None.
Message Used	SM Context Status Notification or Status Notification
Message Direction	SMF to AMF
Comments or Specification References	SMF supports the following scenarios for this cause: • When UE is activated on network, SMF sends the SM Context Status Notification or Status Notification message in the statusInfo cause during UE or network-initiated PDU session release. • While the activation of UE PDU session from a deactivated state, SMF waits for the PDU RES STP RES from gNB and if GNB doesn’t respond to AMF or SMF, AMF sends the SM Context Update with UP CXT State as DEACTIVATED with this cause. AMF sends the Update SM Context service operation to SMF.

REL_DUE_TO_SLICE_NOT_AVAILABLE

The following table describes the release due to unavailability of the associated S-NSSAI cause and the scenarios of the occurrence of the cause:

Table 282: Release due to Slice not Available Cause and Scenario

Cause	REL_DUE_TO_SLICE_NOT_AVAILABLE
Cause Description from 3GPP TS 29.502	Release due to the associated S-NSSAI is unavailable.

Scenario of occurrence	The following are the scenarios of the occurrence of the cause: • Scenario 1—UDM-initiated slice information change notification to AMF when PDU is activated. • Scenario 2—UDM-initiated slice information change notification to AMF when PDU is deactivated.
Message Used	The following are the messages used for these scenarios: • Scenario 1—Update SM Context service operation. • Scenario 2—Release SM Context service operation.
Message Direction	AMF to SMF
Comments or Specification References	SMF supports the following scenarios for this cause as per the specification: • 3GPP TS 29.502, Section 5.2.2.3.12 AMF requested PDU Session Release due to slice not available. The POST request includes the release IE configured to True and the the cause IE configured to REL_DUE_TO_SLICE_NOT_AVAILABLE. • 3GPP TS 29.502, Section 5.2.2.4, Release SM Context service operation. As defined in 3GPP TS 23.501 [2], clause 5.15.5.2.2, a change of the set of network slices occur for a UE where a network slice instance is unavailable and the PDU session isn't activated.

REL_DUE_TO_DUPLICATE_SESSION_ID

The following table describes the release due to UE request for new PDU session establishment cause and the scenario of the occurrence of the cause:

Table 283: Release due to Duplicate Session ID Cause and Scenario

Cause	REL_DUE_TO_DUPLICATE_SESSION_ID
Cause Description from 3GPP TS 29.502	Release due to a UE request to establish a new PDU session with an identical PDU session ID.
Scenario of occurrence	AMF-requested PDU Session Release due to duplicate PDU Session ID.
Message Used	Update SM Context service operation
Message Direction	AMF to SMF

Comments or Specification References	SMF supports the following scenario: As defined in 3GPP TS 24.501 [7], clause 5.4.5.2.5, when the AMF receives an initial request with the existing PDU Session ID in the PDU session context of the UE, AMF requests the SMF to release the existing PDU Session. After receiving the SM context status notification indicating that the deletion of the SM context in the SMF, the AMF releases the stored context for the PDU session. Then, the AMF sends the initial request with the PDU Session ID. The POST request includes the release IE configured to True and the cause IE configured to REL_DUE_TO_DUPLICATE_SESSION_ID. **Note** SMF doesn't send the NAS signaling to UE for the PDU session release in this procedure.

PDU_SESSION_STATUS_MISMATCH

The following table describes the release due mismatch of PDU session status between UE and AMF cause and the scenario of the occurrence of the cause:

Table 284: Release due to PDU Session Status Mismatch Cause and Scenario

Cause	PDU_SESSION_STATUS_MISMATCH
Cause Description from 3GPP TS 29.502	Release due to mismatch of PDU Session status between UE and AMF.
Scenario of occurrence	UE service request procedure.
Message Used	SM Context Release Data
Message Direction	AMF to SMF
Comments or Specification References	SMF supports the following scenario: As defined in 3GPP TS 24.501, Section 5.2.2.4, Release SM Context service operation, in case of mismatch of the PDU session status between the UE and the AMF, the AMF starts Release operation towards SMF to release the PDU context from network.

HO_FAILURE

The following table describes the handover preparation failure cause and the scenario of the occurrence of the cause:

Table 285: Release due to HO Failure Cause and Scenario

Cause	HO_FAILURE
Cause Description from 3GPP TS 29.502	Handover preparation failure.

Scenario of occurrence	5GS to EPS handover over N26 interface and if no resources can be assigned in EPS for any attempted PDU session to be handed over.
Message Used	SM Context Update
Message Direction	AMF to SMF
Comments or Specification References	SMF supports the following scenario: AMF updates the SMF with the information that the handover preparation failed by sending a POST request with the cause attribute configured to HO_FAILURE and with an empty list of EPS bearer contexts. This procedure doesn't include the dataForwarding IE. Then, SMF releases the resources prepared for the handover and proceeds with the PDU session.

INSUFFICIENT_UP_RESOURCES

The following table describes the activation failure for User Plane connection due to insufficient resources cause and the scenario of the occurrence of the cause:

Table 286: Release due to Insufficient UP Resources Cause and Scenario

Cause	INSUFFICIENT_UP_RESOURCES
Cause Description from 3GPP TS 29.502	Failure to activate the User Plane connection of a PDU session due to insufficient user plane resources.
Scenario of occurrence	During an idle mode exit procedure.
Message Used	SM Context Updated Data
Message Direction	SMF to AMF
Comments or Specification References	3GPP TS 129.502 , Section 5.2.2.3.2.2, Activation of User Plane connectivity of a PDU session SMF supports the following scenario: As defined in 3GPP TS 38.413 [9], clause 9.3.4.16 5G-AN sends the N2 SM information to SMF including the cause of the failure or if the resources failed to establish the PDU session. After SMF receives this information, SMF considers that the activation of the User Plane connection has failed and configures the upCnxState attribute to DEACTIVATED. In case the activation of the User Plane connection fails due to insufficient resources, the cause is included in the problem details response and configured to INSUFFICIENT_UP_RESOURCES with status code as 500.

PDU_SESSION_HANDED_OVER

The following table describes the handover of PDU session cause and the scenario of the occurrence of the cause:

Table 287: Release due to PDU Session Handed Over Cause and Scenario

Cause	PDU_SESSION_HANDED_OVER
Cause Description from 3GPP TS 29.502	The PDU session is handed over to another system or access.
Scenario of occurrence	5GC to EPS mobility without N26 interface Handover from 5GS to EPC or ePDG
Message Used	SM Context Status Notification
Message Direction	SMF to AMF
Comments or Specification References	SMF supports the following specification for this cause: • As defined in 3GPP TS 23.502, SMF supports Section 4.11.2.2 5GC to EPS mobility without N26 interface and 4.11.4.2 Handover from 5GS to EPC or ePDG • As defined in 3GPP TS 29.502, Section 5.2.2.5 Notify SM Context Status service operation, SMF sends a POST request to the SM Context Status callback reference that the NF Service Consumer provides during the subscription of this notification. The payload body of the POST request contains the notification payload. If the PDU session handover triggers the notification, the notification payload contains the Cause IE with the PDU_SESSION_HANDED_OVER value. **Note** • SMF doesn't support the 5GC to EPS mobility without N26 interface • SMF supports sending of SM Context Status Notification with this cause during handover from 5GS to EPCor ePDG.

3GPP Change Requests

SMF supports the following change requests (CR) as per 3GPP specification:

- SMF complies with 3GPP TS 29.502 CR 0097 to support sending of the "INSUFFICIENT_UP_RESOURCES" cause to AMF. The INSUFFICIENT_UP_RESOURCES table describes this cause and scenario.
- SMF complies with 3GPP TS 29.518 CR 161 not to support the UE_IN_NON_ALLOWED_AREA cause in N1N2 Message Transfer Error from AMF. This transfer error occurs due to gateway timeout.

Statistics

SMF supports statistics for the following causes on the N11 interface messages that it receives from AMF.

SM Context Release Request:

- REL_DUE_TO_UP_SEC

- PDU_SESSION_STATUS_MISMATCH

SM Context Update Request when you configure the Release flag to True:

- REL_DUE_TO_SLICE_NOT_AVAILABLE
- REL_DUE_TO_REACTIVATION
- REL_DUE_TO_DUPLICATE_SESSION_ID

The following is an example showing the statistics for the REL_DUE_TO_SLICE_NOT_AVAILABLE cause:

smf_service_amf_msg_total{app_name="smf",cause_code=

"REL_DUE_TO_SLICE_NOT_AVAILABLE",cluster="smf",

data_center="smf",direction="inbound",instance_id="1",message_type="pdu_session_release_request_amf",

procedure_type="PDU Session Release - AMF initiated Mod Req",service_name="smf-service"} 2

Standards Compliance

The cause IE support on N11 interface feature complies with the following standards:

- *3GPP TS 29.502 version 15.4.0.0 (section 6.1.6.3.8) —5G; 5G System; Session Management Services; Stage 3*
- *3GPP TS 29.502 (CR 0097)—5G; 5G System; Session Management Services; Stage 3*
- *3GPP TS 29.518 (CR 161)—5G; 5G System; Access and Mobility Management Services; Stage 3*

N16 Interface

The N16 interface is the reference point between two SMFs in a roaming scenario, where one SMF is in the visited network and the other SMF is in the home network.

For details on roaming between SMFs, see Roaming Between SMFs, on page 694.

ProblemDetails JSON Object

Feature Description

SMF supports sending and receiving the ProblemDetails JSON object on the N11 interface and supports roaming.

An application error can prevent the SMF service, acting as an HTTP server, from completing the HTTP request. In this case, the SMF service maps the application error to the similar 4xx or 5xx HTTP status.

An HTTP status code determines the cause of the error. However, sometimes these status codes don't have adequate information about an error. In this case, the SMF service acting as the HTTP server provides more application-related error information to the SMF service acting as an HTTP client. This SMF service provides the additional information by including the representation of “ProblemDetails” data structure in the response body.

3GPP specification defines JSON as one of the document formats. HTTP APIs reuse this format to identify various problem types based on the requirement.

The ProblemDetails structure specified for N11 interface is sent on the N16 interface for roaming call flows on hSMF. After receiving ProblemDetails from hSMF, the vSMF rejects the corresponding message from AMF and saves the ProblemDetails that vSMF receives from hSMF.

How it Works

This section describes how this feature works.

If a response includes a payload body with the ProblemDetails data structure, then the SMF service includes a "Content-Type" header field configured to "application/problem+json". The SMF service generates the HTTP response.

Handling Problem Details

SMF handles the problem details structure that SMF receives from AMF and provides roaming support on other SMFs.

Roaming Between SMFs

The home SMF (hSMF) and visited SMF (vSMF) communicate with each other over the N16 interface. The following sections describe how the ProblemDetails structure specified for N11 interface is sent on N16 interface for roaming call flows for hSMF and vSMF.

Call Flows

This section describes the following call flows:

- Create Service Operation on hSMF Call Flow
- Create Service Operation on vSMF Call Flow
- Update Service Operation towards hSMF Call Flow
- Update Service Operation towards vSMF Call Flow

Create Service Operation on hSMF Call Flow

The Create service operation creates a PDU session in the hSMF for home-routed roaming scenarios. The NF Service Consumer, such as vSMF, creates a PDU session by using the HTTP POST method.

This section describes the Create service operation on hSMF call flow.

Figure 164: Create Service Operation on hSMF Call Flow

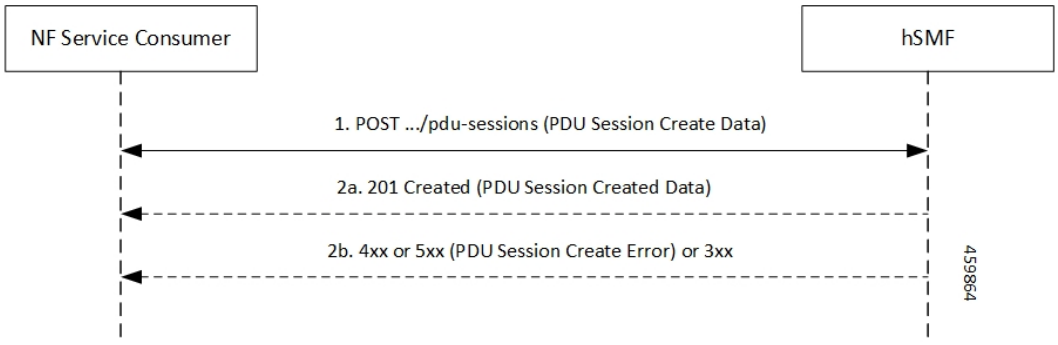


Table 288: Create Service Operation on hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to create a PDU session in hSMF.
2	If the PDU session creation is successful, the hSMF sends the "201 Created" to NF Service Consumer.
3	If the PDU session establishment fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for PDU Session Creation Error table. For the 4xx or 5xx response, the message body contains a PDU Session Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 289: HTTP Status Codes for PDU Session Creation Error

Data Type	HTTPS Status Code	Cause	Details	Title
PDU Session Create Error	403	SUBSCRIPTION _DENIED	UDM_Subscription _Fetch_Failed	Network _Failure
PDU Session Create Error	403	SNSSAI_ DENIED	SNSSAI_Not_ Supported_By_SMF	Network _Failure
PDU Session Create Error	500	UNSPECIFIED _NF_FAILURE	UDM_Notification _Failed	Network _Failure
PDU Session Create Error	404	SUBSCRIPTION _NOT_FOUND	UDM_Subscription _Failed	Network _Failure
PDU Session Create Error	504	NETWORK_ FAILURE	SLA_Txn _Timeout	Network _Failure
PDU Session Create Error	403	DNN_DENIED	DNN_Not_Subscribed	Network _Failure
PDU Session Create Error	403	SSC_NOT_ SUPPORTED	SSC_Mode_Not _Supported_By_SMF	Network _Failure
PDU Session Create Error	403	SSC_DENIED	SSC_Mode_Denied _From_UDM	Network _Failure
PDU Session Create Error	403	PDUTYPE_DENIED	UDM_Rejected _PDU_Type	Network _Failure

Create Service Operation on vSMF Call Flow

The Create SM Context service operation creates an SM context for a PDU session either in the SMF or in the vSMF for home-routed roaming scenarios. The NF Service Consumer, such as AMF, creates an SM context by using the HTTP POST method.

This section describes the Create service operation on vSMF call flow.

Figure 165: Create Service Operation on vSMF Call Flow

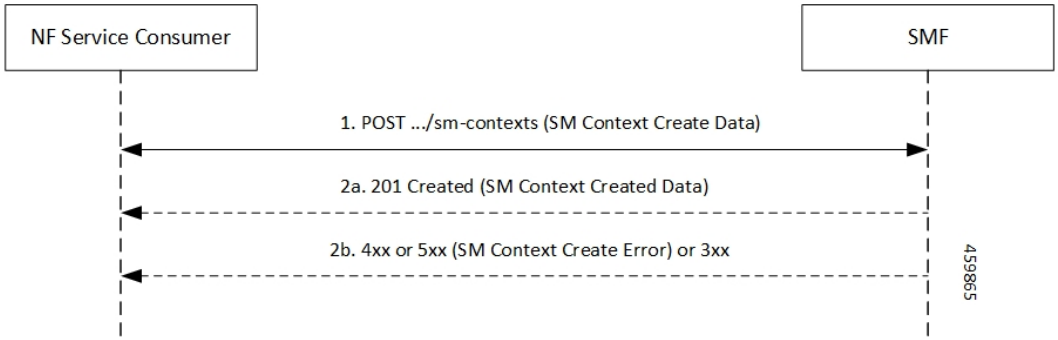


Table 290: Create Service Operation on vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as AMF, sends a POST request to create SM Context to the resource that represents the SM contexts collection resource of the vSMF.
2	If the PDU session creation is successful, the SMF sends the "201 Created" to the NF Service Consumer.
3	If the PDU session establishment fails, the SMF sends the HTTP status code, as listed in the HTTP Status Codes for SM Context Creation Error table. For the 4xx or 5xx response to the NF Service Consumer, the message body contains an SM Context Create Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 291: HTTP Status Codes for SM Context Create Error

Data Type	HTTPS Status Code	Cause	Details	Title
SM Context Create Error	403	PDUTYPE_ NOT_SUPPORTED	PDU_Type_Not _Supported_ By_SMF	Network _Failure
SM Context Create Error	500	REQUEST_ REJECTED_ UNSPECIFIED	Charging_Response _Failure	Network _Failure
SM Context Create Error	504	NETWORK_ FAILURE	SLA_txn _timeout	Network _Failure
SM Context Create Error	400	MANDATORY_IE _MISSING	PDU_Session_ ID_Not_Sent	Mandatory_IE _Missing

Update Service Operation Towards hSMF Call Flow

The NF Service Consumer, such as vSMF, updates a PDU session in the hSMF. The NF Service Consumer also provides the hSMF with information that NF Service Consumer receives from vSMF in the N1 SM signalling from the UE. The NF Service Consumer uses the HTTP POST method to receive this information.

This section describes the Update service operation towards hSMF call flow.

Figure 166: Update Service Operation Towards hSMF Call Flow

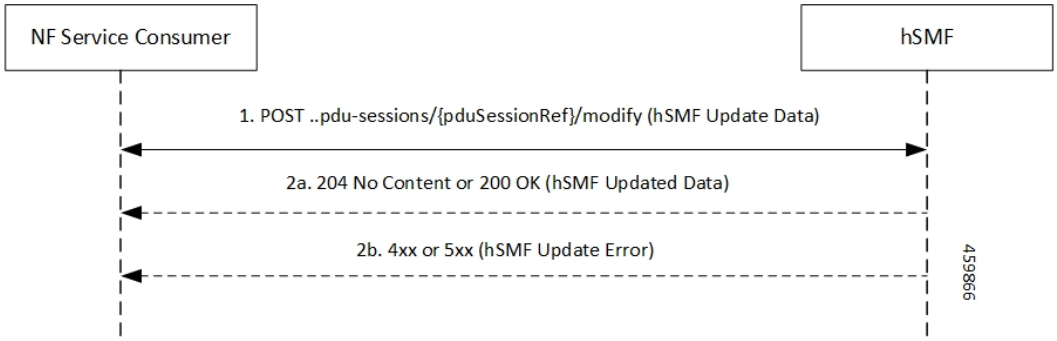


Table 292: Update Service Operation Towards hSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as vSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the hSMF.
2	If the PDU session update is successful, the hSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the hSMF sends the HTTP status code, as listed in the HTTP Status Codes for hSMF Update Error table. For the 4xx or 5xx response, message body contains a hSMF Update Error structure, including the ProblemDetails structure with the "cause" attribute.

Table 293: HTTP Status Code for hSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
hSMF Update Error	404	CONTEXT_NOT _FOUND	PDU_Context _Not_Found	Network _Failure

Update Service Operation Towards vSMF Call Flow

The NF Service Consumer, such as hSMF, updates a PDU session in the vSMF. The NF Service Consumer also provides the required information for the V-SMF to send the N1 SM signalling to the UE by using the HTTP POST method.

This section describes the Update service operation towards vSMF call flow.

Figure 167: Update Service Operation Towards vSMF Call Flow

Table 294: Update Service Operation Towards vSMF Call Flow Description

Step	Description
1	NF Service Consumer, such as hSMF, sends a POST request to modify a PDU session to the resource representing a PDU session resource in the vSMF.
2	If the PDU session update is successful, the vSMF sends "204 No Content" or "200 OK" to the NF Service Consumer.
3	If the PDU session update fails, the vSMF sends the HTTP status code, as listed in the HTTP Status Codes for vSMF Update Error table. For the 4xx or 5xx response, the message body contains a vSMF Update Error structure, including a ProblemDetails structure with the "cause" attribute.

Table 295: HTTP Status Codes for vSMF Update Error

Data Type	HTTPS Status Code	Cause	Details	Title
vSMF Update Error	400	UNSPECIFIED _NF_FAILURE	Ngap_Decode _failed	Invalid_Param
vSMF Update Error	500	UNSPECIFIED _NF_FAILURE	Failure_N4 _Response	Network _Failure
vSMF Update Error	500	SYSTEM_ FAILURE	Procedure _Aborted	Network _Failure
vSMF Update Error	500	INSUFFICIENT_ RESOURCES	Failed_Due_ To_Insufficient_ Resounces_At_Gnb	Network _Failure
vSMF Update Error	400	UNSPECIFIED_ NF_FAILURE	Qfi_Failed _List_Invalid	Network _Failure

N40 Interface

The N40 interface is the reference point between SMF and the Charging Function (CHF). The communication between SMF and CHF enable online and offline charging.

As the N40 interface is located between the SMF and CHF in the HPLMN, home routed roaming and non-roaming scenarios are supported in the same manner.

Nnrf Interface

For NF management, the Network Repository Function (NRF) system provides the service processing functions through HTTP2-based Nnrf Service-based interface (SBI). The Nnrf interface is displayed by NRF on 3GPP 5G system architecture. NRF provides the following services processing functions:

- NF Service Registration—Manage 5G Core service information that an NF instance provides.
- NF Service Discovery—Provide NF instance information that supports 5G Core SBI.
- Access Token—Provide authentication and authorization tokens for use of 5G Core services.

Configuration-based Control of NRF Messages

Feature Description

SMF provides flexibility to the operator to either include or exclude optional Information Element (IE), such as locality, in the NRF messages. Operators can choose the IE through the CLI configuration commands.

SMF sends the **skip optional-ies locality** CLI command in the NRF message handling profile configuration to exclude sending the locality parameter in the NRF registration and NRF update messages.

The NRF message is a combination of the following messages.

- nf-deregister
- nf-list-retrieval
- nf-profile-retrieval
- nf-register
- nf-status-notify
- nf-status-subscribe
- nf-status-unsubscribe
- nf-update

For details on the configuration commands, see the Configuring Control for Optional IEs, on page 718 section.

Feature Configuration

The feature for configuration-based control of NRF messages includes the following steps:

1. Configuring Message Handling Profile, on page 718
2. Configuring Control for Optional IEs, on page 718

Configuring Message Handling Profile

To configure the NRF message handling profile, use the following sample configuration

```
config
  profile message-handling message_handling_profile_name
    nf-type nf_type_name
    mh-profile message_handling_profile_name
    end
```

NOTES:

- **nf-type** *nf_type_name*: Specify the NF type as NRF. *nf_type_name* must be an alphanumeric string representing the corresponding NRF profile name.
- **mh-profile** *message_handling_profile_name*: Specify the message handling profile name for the NRF messages.

Configuration Verification

Use the following command to verify if the message handling profile is configured.

show running-config profile message-handling nf-type nrf mh-profile

If the message handling profile is configured, then the value appears as part of the **message-handling-profile** configuration in the following output.

```
smf(config)# show running-config profile message-handling nf-type nrf mh-profile
 message-handling-profile mhnrf
 exit
```

Configuring Control for Optional IEs

To configure the control to skip the optional IEs, use the following sample configuration:

```
config
  profile message-handling message_handling_name
    nf-type nrf
      mh-profile mh_profile_name
        service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm }
          message type { nf-deregister | nf-list-retrieval |
nf-profile-retrieval | nf-register | nf-status-notify | nf-status-subscribe
 | nf-status-unsubscribe | nf-updatenf-register }
            skip optional-ies locality
            end
```

NOTES:

- **mh-profile** *mh_profile_name* : Specify the NRF message handling profile configuration.
- **service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm }**: Specify the NRF service name type as nnrf-at, nnrf-bs, nnrf-nfd, and nnrf-nfm.
- **message type { nf-deregister | nf-list-retrieval | nf-profile-retrieval | nf-register | nf-status-notify | nf-status-subscribe | nf-status-unsubscribe | nf-update | nf-register }**: Specify the message type as as NF Deregister, NF list retrieval, NF profile retrieval, NF register, NF status notify, NF status subscribe, NF status unsubscribe, NF update, and NF regsiter.
- **skip optional-ies locality**: Specify the locality parameter to skip for the selected NRF message.

Note By default, the SMF sends the **locality** parameter in the NRF Registration or Update messages. The **profile message-handling** *message_handling_name* CLI command gives the provision to skip sending the **locality** parameter in the NRF messages.

Configuration Verification

To verify if the control to skip the optional IEs is configured, use the following command at the Exec mode:

show running-config profile message-handling nf-type nrf

You can also verify the feature configuration using the following show command at the Global Configuration mode.

show full-configuration profile message-handling nf-type nrf

The following is an example output of the **show running-config profile message-handling nf-type nrf** command.

```
[smf] smf# show running-config profile message-handling nf-type pcf
profile message-handling nf-type nrf
 mh-profile mhnrf
  service name type nnrf-nf
   message type nf-register
    skip optional-ies locality
   exit
exit
```

In the preceding example, the **skip optional-ies locality** configuration is enabled for SMF to skip the the optional IE for locality in the NRF message.

RADIUS Interface

Remote Authentication Dial-In User Service (RADIUS) is a protocol that manages network access. This protocol provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

For authentication and authorization, when a user sends a request to NAS to gain access to a network resource using access credentials, the credentials are passed to the NAS device through the link layer protocol. For example, Point-to-Point Protocol (PPP). Then, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access through the RADIUS protocol.

For accounting, when NAS grants network access to the user, NAS sends an Accounting Start packet to the RADIUS server to signal the start of the user network access.

S2b Interface

In wireless applications, the S2b interface is a 4G interface between the Packet Data Network Gateway (PGW) and Evolved Packet Data Gateway (ePDG). This interface uses the PMIPv6 protocol to establish WLAN sessions between the UE and the PGW.

S5 Interface

The S5 interface provides user plane tunnelling and tunnel management between Serving Gateway (SGW) and PDN gateway. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PDN gateway for the required PDN connectivity.

S5 and S8 Interfaces

Both the S5 and S8 interfaces are used within the Evolved Packet Core (EPC) for LTE and exist between the SGW and PGW. Based on functionality, both the S5 and S8 are same interfaces except that S8 interface is used when roaming between different operators while S5 interface is a internal to the network.

SBA Interface

The 5G architecture is based on a Service-Based Architecture (SBA). This architecture provides a modular framework from which you can deploy common applications using components of multiple sources and suppliers. The 3GPP defines the SBA for a 5G core network as delivered by a set of interconnected Network Functions (NFs), such as SMF. A network function can access services of other network functions.

The NFs communicate with each other through Service Based Interfaces (SBI). The SBI is the Application Programming Interface (API)-based communication (REST interface) that uses the HTTP/2 protocol.

HTTP/2 with TLS

Feature Description

The HTTP/2 TLS Support for SBA Interfaces feature enables support for SMF with HTTP/2 over a TLS secure channel for all the SBA interfaces toward the other NFs, for example, PCF, AMF, and so on.

This feature supports the following functionality:

- A CLI support to configure HTTPS (Hypertext Transfer Protocol Secure) Port on SBA interfaces.
- SMF uses TLS version 1.2 for transport layer protection and all inbound and outbound HTTP/2 transport.
- A CLI support to enter a TLS certificate for each SBA interface.
- HTTP/2 over a TLS secure channel for all the SBA interfaces toward the other NFs.

Note SMF also supports HTTP without TLS for backward compatibility. This is the default behaviour.

- Server and Client HTTPS requests for SMF.
- If there is no signed certificate available, the default behavior is to support a self-signed certificate.

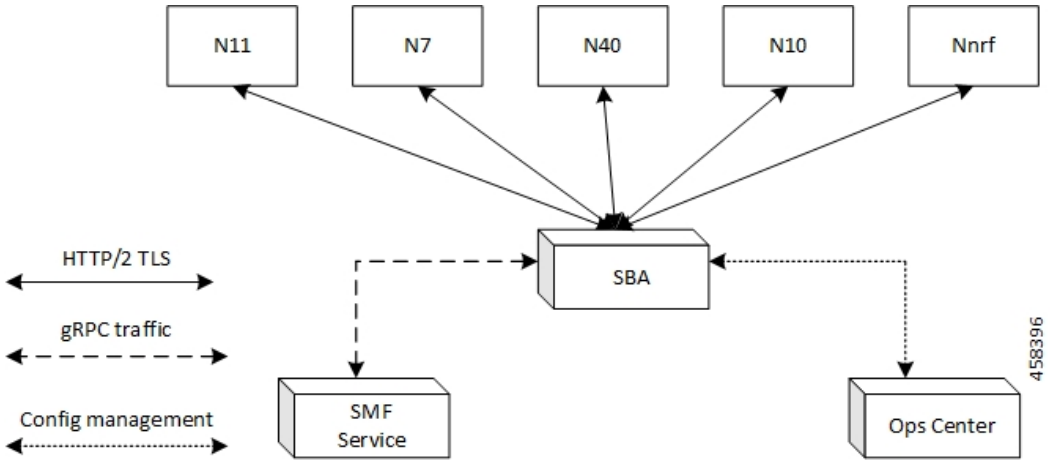
Note Currently, there is no support for persisting configured certificates.

- Generate appropriate alarms when a certificate is about to expire.

Architecture

The SMF Ops Center supports the HTTP/2 REST endpoints, which have TLS enabled for all the outbound interfaces, for example, N7, N10, N11, N40, Nnrf. If a multi-vendor support is required, each of the NF endpoints can independently select the TLS certificate.

Figure 168: SMF HTTP2 TLS Support for SBA Interfaces



Configuring HTTP/2 TLS for SBA Interfaces

This section describes the commands for configuring the HTTP/2 TLS support for SBA interfaces.

Configuring CA Certificates

Use the following sample configuration to configure the CA certificates:

```
config
   nf-tls ca-certificates certificate_name
      cert-data certificate_data
   exit
exit
```

NOTES:

- **nf-tls ca-certificates** *certificate_name*: Specifies the CA certificate name.
- **cert-data** *certificate_data*: Specifies the CA certificate data in the PEM format.

Configuring Server or Client Certificates

Use the following sample configuration to configure the server or client certificates:

```
config
   nf-tls certificates certificate_name
      cert-data certificate_data
      private-key certificate_private_key
   exit
exit
```

NOTES:

- **nf-tls ca-certificates** *certificate_name*: Specifies the CA certificate name.
- **cert-data** *certificate data*: Specifies the CA certificate data in the PEM format.
- **private-key** *certificate_private_key*: Specifies the CA certificate private key in the PKCS 8 format.

To obtain a private key from a certificate, perform the following the steps:

1. Convert the certificate from PEM to PKCS12 format.

   openssl pkcs12 -export -out *pkcscertificate.p12* **-inkey** *certificatekey.pem* **in** *inputcertificate.pem*

2. Extract the private key from PKCS12 certificate created in the preceding step.

   openssl pkcs12 -in *pkcscertificate.p12* **nocerts -nodes -out** *privatekey.pem*

3. Convert the private key to PKCS8 key.

   openssl pkcs8 -in *privatekey.pem* **-topk8 -nocrypt -out** *privatekey.p8*

To enable HTTPS, the rest-endpoint uri-scheme is configured to HTTPS. The default value of the uri-scheme is HTTP. If the uri-scheme is configured as HTTPS, then the SMF requires the server certificate name.

Associating Configured Certificate to Interface

Use the following sample configuration to associate a configured certificate to an interface. You can view the configured certificate names through the **nf-tls certificates** CLI command.

```
config
  endpoint sbi certificate-name configured_certificate_name
  exit
exit
```

NOTES:

- **endpoint sbi certificate-name** *configured_certificate_name*: Shows the list of configured certificate names.

SMF uses the server certificate name for the SBI messages. These certificates are used during the starting of smf-rest-ep pod to configure SSL context for the REST SBI server. When SMF as a client initiates requests, such as N7, N10, and nNRF requests, the protocol is mentioned in the endpoint profile.

Configuring Mutual TLS for SBI Interfaces

To configure mutual TLS for SBI interfaces, use the following sample configuration:

```
config
  instance instance-id instance_id
    endpoint sbi
      interface [ bfd | bgp | coa-nas | geo-external | geo-internal |
gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11
 | sxa | x1 | x2 ]
        mtls-enable [ true | false ]
          certificate name [ clientCert | prem-server-cert | serverCert
 | x1client | x1server ]
        end
```

NOTES:

- **endpoint sbi**: Configure the endpoint for the LI interface.
- **interface [bfd | bgp | coa-nas | geo-external | geo-internal | gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11 | sxa | x1 | x2]** : Specify the SBI interface for the configured endpoint.
- **mtls-enable [true | false]** : Configure mTLS to provide a transport layer encryption between the nodes for the security compliance purposes. By default, the value of **mtls-enable** is configured to **false** .
- **certificate name [clientCert | prem-server-cert | serverCert | x1client | x1server]**: Specify the alias name for certificate from the available options. SMF uses the certificate name for HTTPS messages. The certificate name is used during the start-up of REST-EP pods to configure the SSL context and TLS handshake when messages are exchanged on the SBI interfaces.

Verifying Configured Certificates

Use the **show running-config endpoint sbi** command to verify the certificates configured on the SBA interface.

The following is an example output of the **show running-config endpoint sbi** command.

```
smf# show running-config endpoint sbi
  endpoint sbi
    replicas         2
    uri-scheme       https
    certificate-name smf-server
    vip-ip 209.165.200.225
  exit
```

Monitoring and Troubleshooting

This section provides information for troubleshooting any issues that might arise during the feature operation.

The SMF maintains various logs such as trace logs, event logs, and so on. Check the datastore pod health and the logs for any issues that are related to failures with message routing. Use information in the logs for diameter-ep-rx and datastore or session DB pods to debug issues with this feature.

show nf-tls certificate-status

To see the list of certificates, which are configured and their remaining validity period in days, use the following command:

```
show nf-tls certificate-status
```

Following is the sample output:

```
CERTIFICATE
NAME         DAYS
-------------------
ca           3631
smf-server   355
smfclient    355
```

SCP Interface

The Service Communication Proxy (SCP) is the routing control point that mediates all signaling and Control Plane messages in the network core. SCP is responsible for optimizing routing of NF discovery requests to the Network Repository Function (NRF), load balancing, traffic prioritization, and message management.

Communication Models for NF and NF Services Interaction

For a 3GPP 5GC enhanced SBA (eSBA) network, 3GPP defines four communication models that NF and NF services (Consumer NF and a Producer NF) can use to interact which each other. These communication models are Model A, B, C, and D.

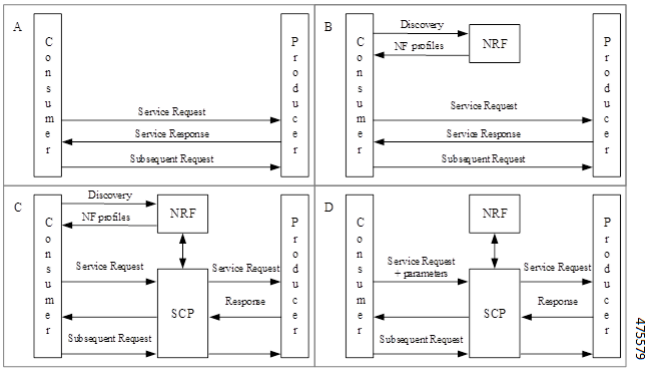
Note SMF supports Models A, B, and D.

The following table lists the communication models, their usage, and how they relate to the usage of an SCP.

Table 296: Communication Models for NF and NF Services Interaction

Communication Between Consumer NF and Producer NF	Service Discovery and Request Routing	Communication Model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services, no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the set can be delegated to SCP. Routing is done through SCP.	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request. Routing is done through SCP.	D

Figure 169: Communication Models for NF and NF Services Interaction



In Model A, there is a direct communication without the NRF interaction. No NRF or SCP is used. The consumers are configured with the producer NF profiles and directly communicate with the producer of their choice.

In Model B, there is a direct communication with the NRF interaction. Consumers perform discovery by querying the NRF. Based on the discovery result, the consumer does the selection. The consumer sends the request to the selected producer.

In Model C, there is an indirect communication without the delegated discovery. Consumers perform discovery by querying the NRF. Based on discovery result, the consumer does the selection of an NF Set or a specific NF instance of NF set. The consumer sends the request to the SCP containing the address of the selected service producer pointing to a NF service instance or a set of NF service instances. The SCP routes the request to the selected NF service producer instance.

In Model D, there is an indirect communication with the delegated discovery. Consumers do not perform any discovery or selection. The consumer adds the required discovery and selection parameters to find an appropriate producer to the service request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a appropriate producer instance. The SCP can perform discovery with an NRF and obtain a discovery result.

Indirect Communication for NFs through SCP Model D

Feature Description

SMF performs indirect communication for network functions (NFs) through Model D. By default, SMF performs the NRF discovery to select the NF peer, such as PCF, CHF, and AMF. If the NRF discovery fails and if the local configuration is available for the peer, SMF selects the local configured peer.

Note In a network, SMF supports 12 SCPs theoretically and up to 5 SCPs in the practical scenarios.

How it Works

With the SCP Model D support, the SMF send requests to SCP endpoints. SCP performs the NRF discovery and finds the correct peer NF and sends the request to the NF. For the NRF discovery, the discovery parameters are sent in the HTTP header.

You can configure the indirect communication through Model D per peer type and by priority. You can configure the priority for Models A, B, and D.

Standards Compliance

The indirect communication for NFs through SCP Model D feature complies with the following standards:

- *3GPP TS 29.500, version 16.9.0.*

Supported HTTP Headers

3gpp-Sbi-Discovery Header

If you have configured the Model D, the SMF doesn't trigger the NF discovery and sends the message with the discovery parameters to SCP for the peer selection.

By default, SUPI and target NF type are added. SMF includes the 3gpp-Sbi-Discovery HTTP header for each query parameter that is configured in the network element profile in following format:

```
3gpp-Sbi-Discovery-<query-param>
```

Following are the examples of the 3gpp-Sbi-Discovery header:

```
3gpp-Sbi-Discovery-dnn: internet
```

```
3gpp-Sbi-Discovery-snssais: [{"sst": 1, "sd": "A08923"}, {"sst": 1, "sd": "0023F1"}]
```

Note

- Both **3gpp-Sbi-Discovery-target-plmn** and **3gpp-Sbi-Discovery-source-plmn** are always included for the inter-PLMN discovery. However, these parameters aren't supported.
- The 3gpp-Sbi-Discovery-supi header must be added to all the messages.

Authority Header

SMF includes the authority HTPP header in the messages to SCP. This header is populated in the following cases:

- If the scheme is "https" from the configuration, then the authority header carries the FQDN from the endpoint name configuration.
- If the scheme is "http", then the authority carries the FQDN or IP address. The priority is given to the IP address configuration.

3gpp-Sbi-Target-apiRoot Header

While sending notification to peer NF, the SMF replaces the "api root" of the "target api" with the "scp api root" and includes the "target api root" in the "3gpp-sbi-target-apiRoot" header.

For example, if the SMF sends the notification "POST https://scp.com/a/b/c/notification" to the SCP, with the "3gpp-sbi-target-apiRoot" header set to "https://example.com", then the SCP sends the request "POST https://example.com/a/b/c/notification" to the NF Service Producer, without the "3gpp-sbi-target-apiRoot" header.

Note SMF doesn't support the SCP "apiPrefix".

The SMF doesn't include the "3gpp-sbi-target-apiRoot" header in the initial request to the peer NF for a specific session. SMF extracts the "target api" prefix of the resource from the "location" header of the response. Then, SMF includes this prefix in the "3gpp-sbi-target-apiRoot" header in a subsequent message to the peer NF for the same session.

For example, When the SMF receives the following "location" header in the N7 Create Response:

http://209.165.200.230:9082/npcf-smpolicycontrol/v1/sm-policies/
ism.14.imsi-310260157090153.1660028704.43993.7129768994171956185

Then, the SMF sends the following SMPolicy Update message:

http://scpIP:port/npcf-smpolicycontrol/v1/sm-policies/

ism.14.imsi-310260157090153.1660028704.43993.7129768994171956185

Where

"authority header" is "scpIP"

"3gpp-sbi-target-apiRoot" is 209.165.200.230:9082

Note SMF also includes "3gpp-sbi-target-apiRoot" header in the messages that are intended to operate on a resource that the peer has already created. For example, when the SMF sends the N10 Deregistration message to UDM, the SMF uses the "location" header that the SMF receives in N10 Registration response to populate the "3gpp-sbi-target-apiRoot" header.

3gpp-Sbi-Callback Header

The SMF populates the "3gpp-Sbi-Callback" header in the callback requests with the callback service name for the SCP to provide the differentiated services.

Following is the format of this header:

"N<NF>_<service name>_<name of the callback service operation in the corresponding OpenAPI specification file>"

Some of the examples are as follows:

- Notification to AMF is sent as "Nsmf_PDUSession_smContextStatusNotification"
- Notification to vSMF is sent as "Nsmf_PDUSession_StatusNotify"

Server Header

The SMF includes "Server" header in all the error responses to peer NF for information on the source of error. Following is the format of this header:

UDM:"nf-instance-id"

For example, UDM:"54804518-4191-46b3-955c-ac631f953ed8"

On receiving an error response, SMF as a client, extracts the NFType from the "Server" header and triggers the SCP failure handling. If you have configured the Model D and if the "Server" header indicates the NF peer, then the SMF ignores the "retry" failure handling action. If you have configured "retry-fallback" as SCP failure handling, then SMF falls back to the local configuration without any retry action. After the SMF fallback, any failure is handled according to the NF failure handling configuration.

Note

- If the "Server" header is not received or a timeout occurs, the SCP failure handling is applied.
- In case of timeout from a peer, the SCP populates the "Server" header with its own FQDN and the "504" error code is returned with the problem details including the cause, which is set to "TARGET_NF_NOT_REACHABLE". In this case too, the SCP failure handling is applied. Based on the configuration, SCP tries all the available peer NFs. If the SCP doesn't find any available peer NF, the SCP responds with the "504" error code and "TARGET_NF_NOT_REACHABLE" cause. However, there is a possibility that other SCPs may be able to reach the peer. If a use case to not try another SCP exists in such a case, an operator can configure the retry value to 0.
- In case of NF discovery errors between SCP and NRF, the SCP can set the cause as "NRF_NOT_REACHABLE" or "NF_DISCOVERY_ERROR". In such cases, the SMF falls back to Model-A, if configured.

3gpp-Producer-id Header

The SMF stores the "3gpp-producer-id" header that the SMF receives in the response from the NF peer. Then, the SMF includes this header in the subsequent messages to the peer NF for the same service for the same session.

SCP Model-D Fallback

If you have configured the SCP failure handling with the "retry" action, then SMF attempts an alternate SCP based on SCP configuration and the retry count configuration. After completion of the configured retry counts or unavailability of any alternate SCPs for retrying, the SMF does a fallback from model-D to model-A in the following scenarios:

- SCP triggers an error, with the "Server" header indicating "scp".
- The "retry-and-fallback" action is configured.
- NF client configuration for the peer is available.

Enabling SCP Model D

Perform the following procedures to enable the SCP model D feature:

- Configuring NF Selection Model
- Configuring SCP Profile

Configuring NF Selection Model

You must configure an NF selection model to enable the SCP model D feature in the network element profile. To enable SCP model D, use the following sample configuration:

```
config
  profile network-element network_element_name
    nf-client-profile client_profile_name
    failure-handling-profile failure_handling_profile_name
    nf-selection-model 1 model1_name
```

```
    nf-selection-model 2 model2_name
  exit
```

NOTES:

- **nf-selection-model 1** *model1_name*: Specify SCP as the first NF selection model.
- **nf-selection-model 2** *model2_name*: Specify another NF selection model, such as local, for the second NF selection model.

Configuring SCP Profile

You must configure an SCP profile under the DNN profile to enable the SCP model D feature . To enable SCP profile under the DNN profile, use the following sample configuration:

```
config
  profile dnn dnn_name
    network-element-profiles udm udm_profile_name
    network-element-profiles scp scp_profile_
  exit
```

NOTES:

- **network-element-profiles udm** *udm_profile_name*: Specify the UDM profile name.
- **network-element-profiles scp** *scp_profile_*: Specify the SCP profile name that is to be configured under the specific UDM profile.

Configuration Example

The following is an example configuration of enabling SCP model D in the network element profile:

```
profile network-element pcf pcf1
 nf-client-profile PP1
 failure-handling-profile FHPCF
exit
profile network-element pcf pcf1-scp
 nf-client-profile PP1
 failure-handling-profile FHPCF
 nf-selection-model 1 scp
 nf-selection-model 2 local
exit
```

The following is an example configuration of enabling SCP model D by adding the SCP profile under the DN profile:

```
profile dnn ims
 network-element-profiles udm udm-scp
 network-element-profiles scp scp-udm
exit
```

Configuring SCP Failure Handling Profile

You can configure one or multiple SCPs in SMF similar to configuring NFs. You can configure an SCP endpoint per service under the SCP profile. To configure SCP failure handling profile, use the following sample configuration:

```
config
  profile network-element scp scp_profile_name
    nf-client-profile scp_client_profile_name
```

```
failure-handling-profile failure_handling_scp_profile_name
end
```

NOTES:

- **profile network-element scp** *scp_profile_name*: Specify the SCP as the network element profile. *scp_profile_name* must an alphanumeric string representing the corresponding network element profile name.
- **nf-client-profile** *scp_client_profile_name*: Specify the SCP client profile.*scp_client_profile_name* must an alphanumeric string representing the corresponding NF client profile name.
- **failure-handling-profile** *failure_handling_scp_profile_name*: Specify the SCP failure handling network profile for the configured SCP. *failure_handling_scp_profile_name* must an alphanumeric string representing the corresponding SCP failure handling network profile name.

Configuration Example

The following is an example configuration of the SCP failure handling profile:

```
profile network-element scp scp1
    nf-client-profile scp_profile1
    failure-handling-profile FHSCP
 exit
```

Configuring SCP for NF Communication

To configure SCP for NF communication, use the following sample configuration:

```
config
  profile nf-client nf-type scp
     scp-profile scp_profile_name
        locality locality_name
           priority priority_value
           service name type service_name_type_value
              responsetimeout  responsetimeout_value
              endpoint-profile endpoint-profile_name
                 capacity capacity_value
                 priority priority_value
                 uri-scheme uri_scheme_value
                 endpoint-name endpoint_name/* FQDN */
                    priority priority_value
                    capacity endpoint-profile_name
                    primary ip-address ipv4 ipv4_address
                    primary ip-address port port_number
                    end
```

NOTES:

- **scp-profile** *scp_profile_name*: Specify the name of the SCP profile.
- **locality** *locality_name*: Specify the locality of SCP.
- **priority***priority_value*: Specify the priority value.
- **service name type** *service_name_type_value*: Specify the service name type.
- **responsetimeout** *responsetimeout_value*: Specify the response timeout value.

- **endpoint-profile** *endpoint-profile_name*: Specify the SCP endpoint profile name.
- **primary ip-address ipv4** *ipv4_address*: Specify the IPv4 address of the primary endpoint.
- **primary ip-address port** *primary_port_number*: Specify the port number of primary endpoint.

Configuration Example

The following is an example configuration of the SCP for NF communication:

```
profile nf-client nf-type scp
 scp-profile scp-profile1
  locality LOC1
   priority 30
   service name type <>
    responsetimeout 4000
    endpoint-profile EP1
     capacity 30
     priority 10
     uri-scheme http
     endpoint-name <> /* FQDN */
      priority 10
      capacity 50
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
    exit
   exit
  exit
 exit
exit
```

Configuring SCP Model D Fallback

To configure the SCP Model D fallback, use the following sample configuration:

```
config
  profile nf-client-failure nf-type scp
     profile failure-handling failure_handling_name
     service name type npcf-smpolicycontrol
        responsetimeout response_timeout_value
        message type { PcfSmpolicycontrolCreate }
        status-code httpv2 status_code
        retry retry_value
        action [ retry-and-fallback | retry-and-continue | continue |
terminate { nfaction terminate } | retry-and-terminate { nfaction terminate
 } ]
     exit
  exit
```

NOTES:

- **profile nf-client-failure nf-type scp** : Specify the NF type as SCP that is required after the NF client failure.
- **service name type npcf-smpolicycontrol**: Specify the service name type as npcf-smpolicycontrol.
- **responsetimeout** *response_timeout_value*: Specify the response timeout value in seconds.
- **message type { PcfSmpolicycontrolCreate }**: Specify the message type as **PcfSmpolicycontrolCreate**.

- **status-code httpv2** *status_code* : Specify the status code of the service. The *status_code* must be an integer in the range of 0–599.
- **retry** *retry_value*: Specify the number of retry attempts to the different available endpoints. The *retry_value* must be an integer in the range of 1–10.
- **action [retry-and-fallback | retry-and-continue | continue | terminate { nfaction terminate } | retry-and-terminate { nfaction terminate }]**: Specify the action as retry and fallback, retry-and-continue, continue, terminate, or retry and terminate for fallback from SCP Model D to Model A. The NF failure action used if the server header indicates that the action is from the NF peer. Action is used if the failure is from the SCP.

Note

- After a fallback, the subsequent messages for the same resource use the peer selected as part of fallback. For example, in case a fallback to SCP Model A happens during N10 registration, the SMF sends the subsequent N10 deregistration to the UDM selected as part of fallback.
- Currently, the **action [retry-and-fallback]** is recommended only for the SCP NF client failure handling template.

Configuration Example

The following is an example configuration of the SCP Model D fallback:

```
config
  profile nf-client-failure nf-type scp
    profile failure-handling FHSCP
    service name type npcf-smpolicycontrol
      responsetimeout 1800
      message type PcfSmpolicycontrolCreate
      status-code httpv2 504
        retry 1
        action retry-and-fallback
      exit
    exit
```

Dead SCP Detection

The existing dead peer detection framework in SMF is extended to detect a dead SCP.

Configuring Interfaces

To configure the endpoints for the SMF service and the interfaces to facilitate communication with other network functions, use the following sample configuration:

```
config
  instance instance-id instance_id
    endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime
 | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service
| sgw-service }
```

```
        replicas replica_id
        instancetype Dual
        nodes node_id
        interface { bfd | bgp | coa-nas | geo-external | geo-internal |
gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11
 | sxa }
           loopbackPort port_number
           vip-ip ipv4_address vip-port ipv4_port_number
           vip-ip6 ipv6_address vip-ipv6-port ipv6_port_number
           end
```

NOTES:

- **endpoint { bgpspeaker | diameter | dns-proxy | geo | gtp | gtpprime | li | nodemgr | pfcp | protocol | radius | radius-dns | sbi | service | sgw-service }**: Configure the endpoint based on the desired service.
- **interface { bfd | bgp | coa-nas | geo-external | geo-internal | gtpu | n4 | n7 | n10 | n11 | n16 | n40 | nrf | s2b | s5 | s5e | s8 | s11 | sxa }**: Specify the interface for the configured endpoint.
- **vip-ip** *ipv4_address* **vip-port** *ipv4_port_number*: Specify the IPv4 address and port of the interface.

  ipv4_address must be an IPv4 address in a dotted decimal notation.
- **vip-ip6** *ipv6_address* **vip-ipv6-port** *ipv6_port_number*: Specify the IPv6 address and port of the interface.

  ipv6_address must be an IPv6 address in colon-separated hexadecimal notation.

  At a given time, the SBI interfaces (N7, N10, N11, and N40) support only the IPv4 or IPv6 address. However, the N3, N4 and GTPC interfaces support either IPv4 or IPv6 address or both.

Note For 4G calls with legacy interfaces, peer SGW IPv4, IPv6, or IPv4v6 data address is supported.

Important Instance type must be configured as Dual to configure IPv6 for any interface, regardless of the interface supporting IPv4 or IPv6 at a time, or both IPv4 and IPv6 at the same time. This should be configured only at the endpoint level. All the interfaces configured under that endpoint will implicitly be configured as Dual type instance.

VIP IP or VIP IPv6 configured under SBI interfaces always override the VIP IP and VIP IPv6 configured at the endpoint level.

For the N4 and GTPC interfaces, the IP addresses (either IPv4 or IPv6 or both) configured under the interfaces overrides only the same type of IP address configured under an endpoint.

- Since simultaneous IPv4 and IPv6 addresses aren't supported for SBI interfaces, the discovery address transport type should be the same as the transport type configured at the endpoint or interface configuration.
- Configure the ports, IPv4, and IPv6 addresses at both endpoint and interface levels. The VIP IP and port combination must be unique across the interfaces. If the interface level configuration isn't available, the endpoint level configuration is considered.

Configuration Example

The following is an example of the IPv4 or IPv6 configuration for the interfaces.

```
config
 instance instance-id 1
  endpoint sbi
   replicas     1
   instancetype Dual
   nodes        1
   loopbackPort 7091
   vip-ip 209.165.200.225 vip-port 1234
   vip-ipv6 2001:DB8:1::1 vip-ipv6-port 2345
  interface nrf
   loopbackPort 7096
   vip-ip 209.165.200.226 vip-port 1235
  interface n11
   loopbackPort 7094
   vip-ip6 2001:DB8:0:ABCD::1 vip-ipv6-port 1212
   exit
  interface n7
   loopbackPort 7092
   vip-ip6 2001:DB8:1::FFFF vip-ipv6-port 1233
   exit
  interface n10
   loopbackPort 7093
   vip-ip 209.165.200.227 vip-port 4321
   exit
  interface n40
   loopbackPort 7095
   vip-ip 209.165.200.228 vip-port 4231
   end
```

Since dual stack is not supported, the NRF discovery address transport type must be the same as the transport type configured at endpoint or interface level configuration.

In the preceding configuration example, the PCF uses IPv6 address which is the same transport type as configured within the PCF profile.

```
config
 profile nf-client nf-type pcf
  pcf-profile PP100
   locality LOC1
    priority 30
    service name type npcf-smpolicycontrol
     endpoint-profile EP1
      capacity   30
      uri-scheme http
      endpoint-name EP1
       priority 56
       primary ip-address ipv6 2001:DB8:1::FEFF
       primary ip-address port 2223
      exit
      endpoint-name exit
      exit
     exit
    exit
 exit
exit
```

The following is an example of IPv6 configuration within UPF profile for the N4 interface.

```
config
 profile network-element upf UPF1
  node-id           SSI-UPF1
  n4-peer-address ipv6 2001:DB8:0:ACBD::1
  n4-peer-port      8805
  upf-group-profile upg1
  dnn-list          [ emergency intershat test ]
  capacity          1
  priority          100
  exit
 exit
exit
```

Configuration Verification

To verify the interface configuration, use the following commands:

show running-config instance instance-id *instance_id* **endpoint** *endpoint_name* **interface** *interface_name*

```
[smf] smf# show running-config instance instance-id 1 endpoint sbi interface nrf
instance instance-id 1
 endpoint sbi
  interface nrf
   loopbackPort 9050
   dscp         24
   vip-ip 209.165.200.232 vip-port 8095
  exit
 exit
exit
[smf] smf#
```

This example output shows the configuration for NRF interface. The value for **vip-ip** command indicates that the IPv4 address is configured for the NRF interface.

show peer

```
Thu Jul  7  07:53:23.422 UTC+00:00
GR                                                                          POD
   CONNECTED                                                     INTERFACE
INSTANCE  ENDPOINT      LOCAL ADDRESS    PEER ADDRESS           DIRECTION  INSTANCE     TYPE
  TIME        RPC     ADDITIONAL DETAILS                       NAME       VRF
-------------------------------------------------------------------------------------------
0         RadiusServer  -                10.1.4.72:1812         Outbound   radius-ep-0  Udp
   6 days      Radius  Status: Init,Type: Auth                 <none>     NA
0         RadiusServer  -                10.1.4.72:1813         Outbound   radius-ep-0  Udp
   6 days      Radius  Status: Init,Type: Acct                 <none>     NA
1         <none>        192.168.47.245   10.1.4.72:9014         Outbound   rest-ep-0    Rest
  6 days      CHF     <none>                                   n40        NA
1         <none>        192.168.47.245   10.1.4.72:9024         Outbound   rest-ep-0    Rest
  6 days      CHF     <none>                                   n40        NA
1         <none>        192.168.47.235   10.1.4.72:9011         Outbound   rest-ep-1    Rest
  6 days      UDM     <none>                                   n10        NA
1         <none>        192.168.47.235   10.1.4.72:9012         Outbound   rest-ep-1    Rest
  6 days      AMF     <none>                                   n11        NA
1         <none>        192.168.47.235   10.1.4.72:9060         Outbound   rest-ep-1    Rest
  6 days      SEPP    <none>                                   n32        NA
1         <none>        192.168.47.235   10.1.4.72:9010         Outbound   rest-ep-1    Rest
  6 days      NRF     <none>                                   nrf        NA
1         <none>        192.168.47.235   10.1.4.72:9013         Outbound   rest-ep-1    Rest
  6 days      PCF     <none>                                   n7         NA
1         <none>        192.168.47.245   10.1.4.72:9010         Outbound   rest-ep-0    Rest
```

```
  6 days      NRF     <none>                                  nrf        NA
1         <none>       192.168.47.245   10.1.4.72:9011       Outbound   rest-ep-0    Rest
  16 minutes  UDM     <none>                                  n10        NA
1         <none>       192.168.47.245   10.1.4.72:9012       Outbound   rest-ep-0    Rest
  6 days      AMF     <none>                                  n11        NA
1         <none>       192.168.47.245   10.1.4.72:9060       Outbound   rest-ep-0    Rest
  6 days      SEPP    <none>                                  n32        NA
1         <none>       192.168.47.235   10.1.4.72:9024       Outbound   rest-ep-1    Rest
  6 days      CHF     <none>                                  n40        NA
1         <none>       192.168.47.235   10.1.4.72:9014       Outbound   rest-ep-1    Rest
  6 days      CHF     <none>                                  n40        NA
1         <none>       192.168.47.245   10.1.4.72:9013       Outbound   rest-ep-0    Rest
  6 days      PCF     <none>                                  n7         NA
1         S2B          10.1.3.236:2123  172.31.4.72:2123      Inbound    nodemgr-0    Udp
   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: 100  S2B        NA
1         S2B          [1111::10:1:3:236]:2123       [1111::10:1:4:72]:2123  Inbound
nodemgr-0    Udp   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: N/A  S2B        NA

1         S2B          [1111::10:1:3:236]:2123       [1111::10:1:4:72]:2123  Inbound
nodemgr-1    Udp   6 days      ePDG    MaxRemoteRcChange: N/A,Recovery: N/A  S2B        NA
```

OAM Support

This section describes operations, administration, and maintenance information regarding support for interfaces in SMF.

Bulk Statistics Support

The following label is added into the existing statistics **smf_restep_http_msg_total**:

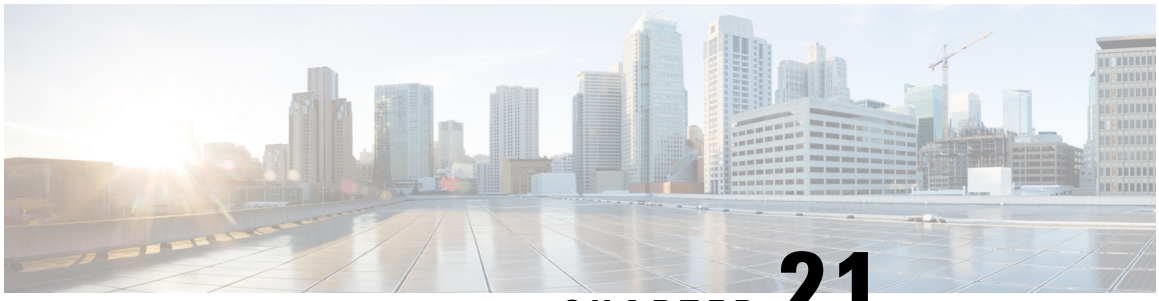
uri_version_mismatch—This metric is included when the URI version in an incoming message is not found in the configured URI versions in SMF.

OFCS_CDR_DROP_STATS — This metric is added to capture counter values whenever a CDR is suppressed due to Zero Suppression.

It displays the SMF procedure name along with trigger name when the suppression criterion is met.

Trigger names values are would be one of these:

- final-cdr
- external-trigger-cdr
- internal-trigger-cdr



CHAPTER 21

IP Address Management

- Feature Summary and Revision History, on page 737
- Feature Description, on page 739
- How it Works, on page 740
- IPAM Integration in SMF, on page 740
- Static IP Support, on page 759
- Dual-stack Static IP Support Through IPAM, on page 768
- IPAM Offline Mode Support, on page 769
- IPAM Redundancy Support Per UPF, on page 771
- IPAM Quarantine Timer, on page 772
- IP Address Validation with CDL Configuration, on page 773
- IPAM Data Reconciliation, on page 775
- Configuring IPAM Quarantine Qsize, on page 777
- Overlapping IP Address Pools, on page 778
- Auto-Reclamation of Under-Utilized IP Chunks, on page 779
- Unique IP Pools for UPFs, on page 782
- Reconciliation of IP Chunks between SMF and UPF, on page 786
- IP Chunk Throttling, on page 788
- Route Aggregation to Handle Switch Limit, on page 791
- NAT Support, on page 799
- Troubleshooting Information, on page 809

Feature Summary and Revision History

Summary Data

Table 297: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI

Feature Default Setting	• IPAM: Enabled – Always-on • Unique IP Pools for UPF: Disabled – Configuration required to enable • Auto-Reclamation of Under-Utilized IP Chunks: Disabled- Configuration required to enable • Identification of Corrupted Chunks: Disabled- Configuration required to enable. • Reconciliation of IP Chunks between SMF and UPF: Disabled- Configuration required to enable. • IP Chunk Auto-Throttle and ToD Chunk Clearance: Disabled- Configuration required to enable. • Route Aggregation to Handle Switch Limit: Disabled- Configuration required to enable. • NAT Support: Disabled- Configuration required to enable.
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 298: Revision History

Revision Details	Release
Added support for the following features: • Releasing N4 resources using a CLI • Network Address Translation (NAT) along with sending NAT binding updates in SMF.	2023.04.0
Added support for the following features: • Auto-Reclamation of Under-Utilized IP Chunks. • Identification of Corrupted Chunks. • Reconciliation of IP Chunks between SMF and UPF. • IP Chunk Auto-Throttle and ToD Chunk Clearance. • Route Aggregation to Handle Switch Limit.	2023.03.0
Nexthop forwarding address configuration added to IPv6 address range and prefix range.	2023.01.4

Revision Details	Release
Added support for the following features: • IPAM Periodic Reconciliation • UPF Fallback functionality	2023.01.0
Added support for the following features: • IPAM reconciliation CLI commands for IPAM hardening. • IP pool allocation per slice and DNN feature. • SMF to allocate UPFs with unique IP pools.	2022.04.0
Added support for the following features: • New calls with a static IP address. • Quarantine queue size. • IP address validation with CDL Configuration and statistics.	2021.02.0
IP Address Validation with CDL Configuration introduced.	2021.02.0
Updated quarantine time range to 3600 seconds.	2021.02.0
VRF Support introduced.	2020.02.5
First introduced.	Pre-2020.02.0

Feature Description

IP Address Management (IPAM) is a method of tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. Traditional IPAM functionalities are insufficient in Cloud-Native network deployments. Hence, IPAM requires additional functionalities to work with the Cloud-Native subscriber management system. The Cloud-Native IPAM system is used in various network functions, such as SMF and PCF.

The IPAM system includes the following functionalities to serve the Cloud Native and Control and User Plane Separation (CUPS) architecture:

- **Centralized IP Resource Management**—Based on the needs of the Internet Service Provider (ISP), the Control Plane (CP) is deployed either on a single (centralized) cluster or multiple (distributed) clusters. For multiple cluster deployments, the IPAM automatically manages the single IP address space across the multiple CPs that are deployed in the distributed environment.
- **IP Address Range Reservation per User Plane**—For subscribers connecting to the Internet core, the User Plane (UP) provides the physical connectivity. The UP uses the summary routes to advertise subscriber routes to the Internet core. For CPs that are managing multiple UPs, the CP reserves a converged

IP subnet to the UPs. In such a scenario, the IPAM splits the available address space into smaller address ranges and assigns it to different UPs.

- **IP Address Assignment from Pre-Reserved Address Ranges**—When subscribers request for an IP address, the IPAM assigns addresses from the pre-reserved address range of their respective UP.
- **IPv4 and IPv6 Pool Next Hop Address Ranges**—SMF supports next hop configuration for IPv4 and IPv6 pools along with address ranges and prefix ranges.

Note For uniform compatibility, the **nexthop-forwarding-address** configuration option is available in both the Internet Assigned Numbers Authority (IANA) and Identity Association for Prefix Delegation (IAPD) IPv6 configuration profiles. SMF does not use the IANA configuration but uses only the IAPD configuration. BNG uses the IANA IPv6 configuration..

How it Works

IPAM uses the following sub-modules for the Cloud-Native subscriber management system:

- IPAM Server—This module manages the complete list of pools and address space configurations. The IPAM server splits the configured address ranges into smaller address ranges statically or dynamically to distribute them to IPAM cache modules. The IPAM server is deployed as a centralized entity to serve group of Cloud-Native clusters or can be an integrated entity within a single cluster.
- IPAM Cache—This module receives the free address ranges from the IPAM server and allocates the individual IP addresses to the IPAM clients. Usually, the IPAM cache is deployed in a distributed mode running within each cluster to communicate with the co-located or remotely-located IPAM server. The IPAM cache also handles address range reservation per UP and pool threshold monitoring. The IPAM server and cache modules can run as an integrated mode.
- IPAM Client—This module handles the request and release of an individual IP address from the IPAM cache for each IP managed end-device. The IPAM client is tightly coupled with a respective network function.

IPAM Integration in SMF

Feature Description

The IP Address Management (IPAM) is a technique for tracking and managing the IP address space of a network. A core component of the subscriber management system, the IPAM, provides all the functionalities necessary for working with the Cloud-Native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions, such as the SMF and Policy Control Function (PCF).

Architecture

This section describes the IPAM integration in the SMF architecture.

IPAM Integration

The IPAM and SMF reside in the Application Services layer.

- SMF Node Manager Application—The SMF Node Manager application handles the UPF, ID resource, and IP address management. Hence, the SMF Node Manager application integrates IPAM cache and IPAM client modules. The UPF manager uses the IPAM client module for address range reservation per UPF.
- SMF Service Application— The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to Resource Manager (RMGR) in Node Manager, which receives (free) the IP from the IPAM module.
- IPAM Server Application—Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache.

Components

This section describes the different components of the IPAM system.

IPAM Sub-Modules

The IPAM system includes the following sub-modules:

- **IPAM Server** – The IPAM server module manages the complete list of pools and address space configuration. It splits the configured address ranges into smaller address ranges (statically and dynamically) and distributes it to the IPAM cache modules. You can deploy the IPAM server either as a centralized entity to serve a group of cloud native clusters or as an integrated entity within a single cluster.
- **IPAM Cache** – The IPAM cache acquires free address ranges from the IPAM server and allocates individual IP addresses to the IPAM clients. Deployed in a distributed mode running within each cluster, the IPAM cache communicates with co-located and remotely located IPAM servers. Additionally, the IPAM cache takes care of the address range reservation per data plane and pool threshold monitoring.
- **IPAM Client** – The IPAM client module handles the request and release of the individual IP addresses from the IPAM cache for each IP managed end-device. Based on the use cases, the IPAM client module caters the needs of specific network functions (such as SMF, PCF, and so on).

How it Works

This section describes the call flows pertaining to the integration of the IPAM in the SMF.

Call Flows

The following call flow depicts the integration of the IPAM in the SMF.

Figure 170: IPAM Integration Call Flow

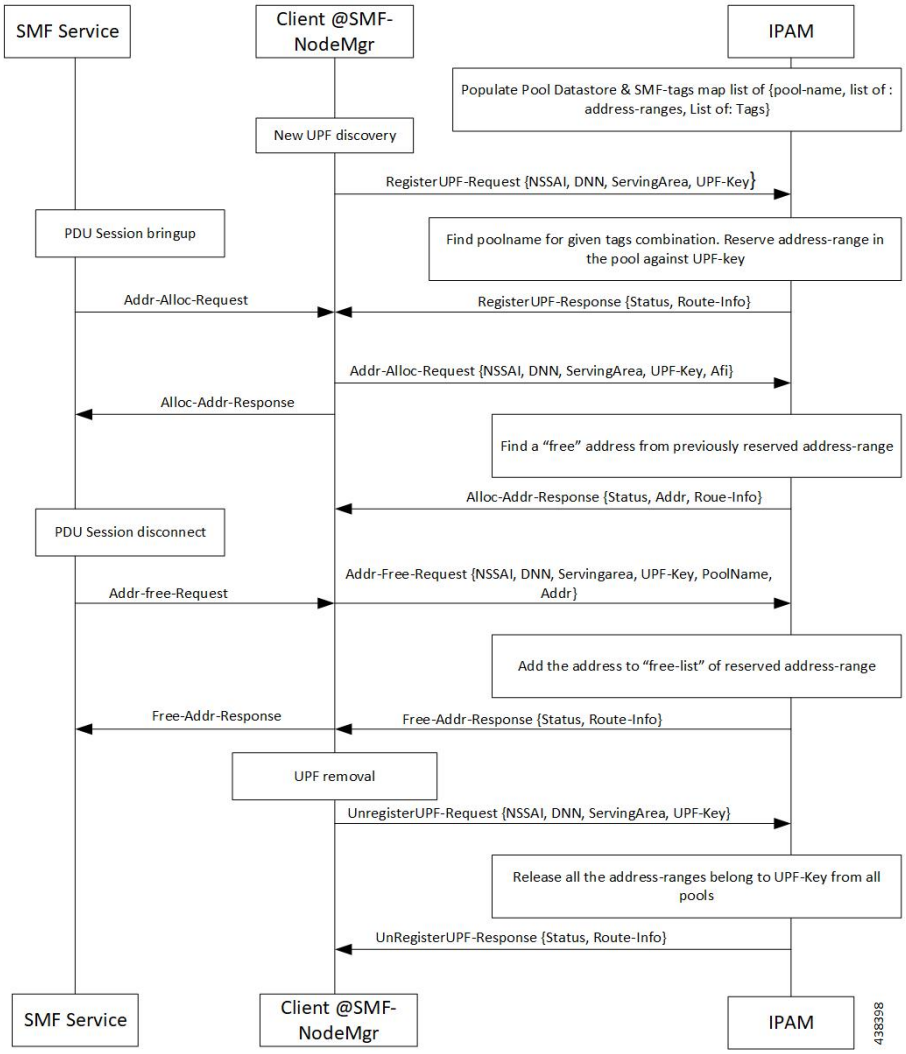


Table 299: IPAM Integration Call Flow Description

Step	Description
1	IPAM populates the local cache and cache pod with the data configured under IPAM pool configuration. Split the address ranges according to the split size configured under address range.
2	The Node Manager (NM) receives UPF discovery or registration request.
3	The NM forwards the UPF registration request to IPAM for a given DNN or address type.
4	IPAM finds the pool for the given tag and address type and allocates a free address range against the given UPF key.
5	Register the UPF response, status, and route information.
6	The SMF service performs bring up of PDU session. The NM forwards the request to IPAM for the address allocation request.

Step	Description
7	IPAM receives the request for address allocation for tag, UPF key, Authority and Format Identifier (AFI), and Group Identifier (GrID).
8	IPAM allocates free address from the previously allocated address range and responds with the status and allocated address, and route information.
9	The SMF service performs bring down of PDU session. The NM forwards the request to IPAM for address release request.
10	IPAM receives the request for address release for pool name, UPF key, AFI, and GrID.
11	IPAM adds the address to free list of the reserved address range and responds with the status and route information.
12	IPAM receives UPF deregistration request with tag, UPF key, and AFI.
13	Release all the address ranges from the pool associated to the tag, UPF key, and AFI. Then, move the address range to the free list.
14	IPAM sends the UPF deregistration response along with the status and route information.

Configuring IPAM

This section describes how to configure the IPAM in the SMF.

Configuring the IPAM in the SMF involves the following steps:

1. Configuring IPv4 Address Ranges, on page 744
2. Configuring IPv6 Address Ranges, on page 745
3. Configuring IPv6 Prefix Ranges, on page 745
4. Configuring SMF Tags, on page 749
5. Configuring IPv4 Address Range Threshold, on page 750
6. Configuring IPv6 Address Range Threshold, on page 751
7. Configuring IPv6 Prefix Range Threshold, on page 751
8. Configuring IPv4 Address Range Split, on page 752
9. Configuring IPv6 Address and Prefix Address Range Split, on page 753
10. Configuring Global Threshold, on page 754
11. Configuring IPAM Source, on page 755

Note In release 2021.02 and later, IPAM pools must be associated to a Geographic Redundancy (GR) instance. That is, you must configure GR instance ID in the IPAM Configuration mode. This configuration is not backward compatible. If you are upgrading SMF to 2021.02 or a later release from a release prior to 2021.02, make sure you first remove the old IPAM configuration and apply the new configuration after the Ops center is accessible.

Configuring IPv4 Address Ranges

To configure the IPv4 address ranges, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv4
               address-range start_ipv4_address end_ipv4_address
               commit
```

NOTES:

- **ipam**: Enter the IPAM configuration mode.
- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **vrf-name** *vrf_name*: Specify the virtual routing and forwarding (VRF) name of the pool.
- **ipv4**: Enter the IPv4 mode of the pool.
- **address-range** *start_ipv4_address end_ipv4_address*: Specify the start address and end address of IPv4 address range in dotted-decimal notation.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p1
                  vrf-name one
                  ipv4
                     address-range 209.165.200.225 209.165.200.253
                     address-range 209.165.201.1 209.165.201.30
                     end
```

Verifying the IPv4 Address Range of a Pool

Use the **show ipam** *pool_name* **ipv4-addr** command to view the IPv4 address ranges for the given pool name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a data plane (user plane) using this command.

The following is an example output of the **show ipam** *pool_name* **ipv4-addr** command.

```
show ipam pool p1 ipv4-addr
=====================================================================
Flag Indication: S(Static) O(Offline)
=====================================================================
```

```
StartAddress          EndAddress    AllocContext     Flag
=====================================================================
209.165.200.225    209.165.200.253  Upf-100
209.165.201.1      209.165.201.30   Upf-200
209.165.202.129    209.165.202.158  Free:NM1




=====================================================================
```

Configuring IPv6 Address Ranges

To configure the IPv6 address ranges, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
               address-range start_ipv6_address end_ipv6_address
               commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **vrf-name** *vrf_name*: Specify the VRF name of the pool.
- **ipv6**: Enter the IPv6 mode of the pool.
- **address-range** *start_ipv6_address end_ipv6_address*: Specify the start address and end address of IPv6 address range in colon-separated hexadecimal notation.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p1
                  vrf-name one
                  ipv6
                     address-range 1::1 1::1000
                     address-range 2::1 2::1000
                     end
```

Configuring IPv6 Prefix Ranges

To configure the IPv6 prefix ranges, use the following sample configuration:

```
config
   ipam
      instance instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
```

```
prefix-ranges
   prefix-range prefix_value prefix-length length
   commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of address pool. *pool_name* must be a string.
- **vrf-name** *vrf_name*: Specify the VRF name of the pool. *vrf_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.
- **prefix-ranges**: Enter the prefix ranges mode.
- **prefix-range** *prefix_value* **prefix-length** *length* : Specify the IPv6 prefix range and the IPv6 prefix length.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p3
                  vrf-name three
                  ipv6
                     prefix-ranges
                        prefix-range 1:1:: prefix-length 48
                        prefix-range 2:1:: prefix-length 48
                        end
```

Verifying the IPv6 Address Prefix Range of a Pool

Use the **show ipam pool** *pool_name* **ipv6-prefix** command to view the prefix ranges for the given pool name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a data plane (user plane) using this command.

The following is an example output of the **show ipam pool** *pool_name* **ipv6-prefix** command.

```
show ipam pool p1 ipv6-prefix
=================================================================================================
Flag Indication: S(Static) O(Offline)
=================================================================================================
StartAddress                 EndAddress                   AllocContext         Flag
=================================================================================================
aaaa:bbbb:ccc0::/64    aaaa:bbbb:ccc4::/64          Upf-100
aaaa:bbbb:dd00::/64    aaaa:bbbb:dd12::/64          Upf-200
bbbb:cccc:ee00::/64    bbbb:cccc:ee12::/64          Free:NM1
bbbb:cccc:ff00::/64    bbbb:cccc:ff12::/64          Free:NM0
xxxx:yyyy:zz00::/64    xxxx:yyyy:zz12::/64          Free:CP
```

Configuring IPv4 Address and Prefix Ranges with Next Hop Forwarding Address

To configure the IPv4 address with the next hop configuration for IPv4 pools/address ranges, use the following sample configuration:

```
configure
   ipam
      instance instance_id
         address-pool pool_name
            ipv4
```

```
          address-ranges
             address-range start_ipv4_address end_ipv4_address
nexthop-forwarding-address nexthop_forwarding_address
             prefix-range prefix_value length  prefix_length
nexthop-forwarding-address nexthop_forwarding_address
             split-size per-cache number_of_addresses
             split-size per-dp number_of_addresses
             commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv4**: Enter the IPv4 mode of the pool.
- **address-ranges**: Specify the starting address of the IPv4 address range. Enter the IPv4 address range and prefix range addresses with the next hop forwarding address.
  - **address-range** *start_ipv4_address end_ipv4_address* **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the starting and the ending addresses of the IPv4 address range with the next hop forwarding address.
  - **prefix-range** *prefix_value* **length** *prefix_length*: Specify the prefix value and the length within the IPv4 address.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the next hop forwarding address.
- **split-size per-cache** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for IPAM cache allocation. Specify in the power of 2. The IPAM server consumes this configuration. *number_of_addresses* must be an integer in the range of 2-262144.
- **split-size-per-dp** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for data plane allocation. Specify in the power of 2. The IPAM cache consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.

Configuration Example

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

Configuring IPv6 Address Ranges with Next Hop Forwarding Address

To configure the IPv6 address with the next hop configuration for IPv6 pools and address ranges, use the following sample configuration:

```
configure
   ipam
      instance instance_id
```

```
        address-pool pool_name
           ipv6
           address-ranges
              address-range start_ipv6_address end_ipv6_address
nexthop-forwarding-address nexthop_forwarding_address
              prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
               split-size per-cache number_of_addresses
               split-size per-dp number_of_addresses
               exit
               prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
              commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.
- **address-ranges**: Specify the IPv6 address ranges and prefix range addresses with the next hop forwarding address.

Note IANA IPv6 configuration is used by BNG.

  - **address-range** *start_ipv6_address end_ipv6_address* : Specify the starting and the ending addresses of the IPv6 address range.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the nexthop forwarding address.
  - **prefix-range** *prefix_value* **length** *prefix_length*: Specify the prefix value and length within the IPv6 address.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the next hop forwarding address.

- **prefix-ranges** : Specify the prefix ranges of an IPv6 address.

Note SMF supports only IAPD IPv6 configuration.

  - **split-size per-cache** *number_of_addresses*: Specify the number of IPv6 addresses per chunk for IPAM cache allocation.
  - **split-size-per-dp** *number_of_addresses*: Specify the number of IPv6 addresses per chunk for the Data plane allocation.
  - **prefix-range** *prefix_value* **length** *prefix_length* **nexthop-forwarding-address** *nexthop_forwardng_address*: Specify the prefix value and the length within the IPv6 address with the next hop forwarding address.

Configuration Example

The following is an example configuration.

```
ipam
 instance 1
  address-pool ISE-Pool1
   vrf-name ISP
   tags
    dnn cisco_vlan400.com
   exit
   ipv6
    address-ranges
      address-range 1000::1 1000::ffff nexthop-forwarding-address :9001::3
      prefix-range 2607:fc20:1010:: length 98 nexthop-forwarding-address :9001::3
    prefix-ranges
       split-size
         per-cache 32768
         per-dp    32768
       exit
       prefix-range 2607:fc20:1010:: length 44 nexthop-forwarding-address :9001::3
   exit
  exit
```

Configuring SMF Tags

To configure the SMF tags, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            tags
               nssai nssai_value
               dnn dnn_name
               serving-area serving_area_value
               commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **tags**: Specify the pool tags to set additional properties for a pool in generic manner.
  - **nssai** *nssai_value*: Specify the NSSAI tag for the pool. *nssai_value* must be a string.
  - **dnn** *dnn_value*: Specify the location DNN or DNN tag for the pool. *dnn_value* must be a string.

Note

- Based on **pool-selection nssai** configuration, the SMF sends the "slice + dnn" as tag to IPAM.
- The NSSAI value must match the SMF slice configuration name.

  - **serving-area** *serving_area_value*: Specify the serving area tag for the pool. *serving_area_value* must be a string.

Configuration Example for SMF tags

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool
                  tags
                     nssai one
                     dnn two
                     serving-area three
                     end
```

Configuration Example of IPAM Tag with same SMF slice configuration name

```
ipam
 instance 1
  address-pool p1
   tags
    nssai slice1
    dnn   dnn1

  address-pool p2
   tags
    nssai slice1
    dnn   dnn2
```

Configuring IPv4 Address Range Threshold

IPAM keeps monitoring the pool usage threshold. Based on the configured threshold value, IPAM requests for next free address range or releases the address range.

To configure the IPv4 threshold, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv4
               threshold
                  upper-threshold percentage
                  commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv4**: Enter the IPv4 mode of the pool.
- **threshold**: Enter the threshold sub-mode.
- **upper-threshold** *percentage*: Specify the IPv4 upper threshold value in percentage.

The following is a sample configuration.

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     threshold
```

```
                                upper-threshold 80
                                end
```

Verifying the Threshold of a Pool

Use the **show ipam pool** command to view the summary of current threshold of each pool.

The following is an example output of the **show ipam pool** command.

```
show ipam pool
=================================================================
PoolName   Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
=================================================================
  p1               80%            80%              0%
  p2               75%            0%               70%
=================================================================
```

Configuring IPv6 Address Range Threshold

To configure the IPv6 address range threshold, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               address-ranges
                  threshold
                     upper-threshold percentage
                     commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.
- **address-ranges**: Enter the IPv6 address ranges sub-mode.
- **threshold**: Enter the threshold sub-mode.
- **upper-threshold** *percentage*: Specify the IPv6 upper threshold value in percentage.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p2
                  ipv6
                     address-ranges
                        threshold
                           upper-threshold 75
                           end
```

Configuring IPv6 Prefix Range Threshold

To configure the IPv6 prefix range threshold, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               prefix-ranges
                  threshold
                     upper-threshold percentage
                     commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.
- **prefix-ranges**: Enter the IPv6 prefix ranges sub-mode.
- **threshold**: Enter the threshold sub-mode.
- **upper-threshold** *percentage*: Specify the IPv6 upper threshold value in percentage.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p3
                  ipv6
                     prefix-ranges
                        threshold
                           upper-threshold 78
                           end
```

Configuring IPv4 Address Range Split

To configure the IPv4 address range split, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv4
               split-size per-cache number_of_addresses
               split-size per-dp number_of_addresses
               commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv4**: Enter the IPv4 mode of the pool.
- **split-size per-cache** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for IPAM cache allocation. Specify in the power of 2. The IPAM server consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.

- **split-size-per-dp** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for data plane allocation. Specify in the power of 2. The IPAM cache consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

Configuring IPv6 Address and Prefix Address Range Split

To configure the IPv6 address and prefix address range split, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            ipv6
               address-ranges
                  split-size per-cache number_of_addresses
                  split-size per-dp number_of_addresses
                  exit
               prefix-ranges
                  split-size per-cache number_of_addresses
                  split-size per-dp number_of_addresses
                  commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.
- **address-ranges**: Enter the IPv6 address-ranges sub-mode.
- **split-size per-cache** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for IPAM cache allocation. Specify in the power of 2. The IPAM server consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.
- **split-size-per-dp** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for data plane allocation. Specify in the power of 2. The IPAM cache consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.
- **prefix-ranges**: Enter the IPv6 prefix ranges sub-mode.

The following is an example configuration.

```
config
   ipam
      instance 1
         address-pool p1
```

```
ipv6
   address-ranges
      split-size per-cache 4096
      split-size per-dp 1024
      exit
   prefix-ranges
      split-size per-cache 8192
      split-size per-dp 2048
      end
```

Configuring Global Threshold

To configure the global threshold, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         threshold
            ipv4-addr percentage
            ipv6-addr percentage
            ipv6-prefix percentage
            commit
```

NOTES:

- **threshold**: Enter the threshold sub-mode.
- **ipv4-addr** *percentage*: Specify the IPv4 threshold value in percentage.
- **ipv6-addr** *percentage*: Specify the IPv6 threshold value in percentage.
- **ipv6-prefix** *percentage*: Specify the IPv6 prefix threshold value in percentage.

The following is an example configuration.

```
config
   ipam
      instance 1
         threshold
                  ipv4-addr 80
                  ipv6-addr 75
                  ipv6-prefix 70
                  end
```

Verifying the Details of a Pool

This section describes how to verify the integration of IPAM in the SMF.

Use the **show ipam pool** *pool_name* command to view more details of a specific pool name.

The following is an example output of the **show ipam pool** *pool_name* command.

```
show ipam pool p1
-----------------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 7680 / 7680 / 80%
Ipv6Addr   [Total/Used/Threshold] = 0 / 0 / 0.00%
Ipv6Prefix [Total/Used/Threshold] = 512 / 512 / 80%
Instance ID = 1
-----------------------------------------------------------
```

Configuring IPAM Source

To configure the IPAM source, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         source local
            source external ipam
               host ip_address
               port port_number
               vendor type
               commit
```

NOTES:

- **source local**: Enter the local data store as the pool source.
- **source external ipam** : Enter the external IPAM server as the pool source.
- **host** *ip_address* : Specify the host name of the external IPAM server.
- **port** *port_number* : Specify the port of the external IPAM server.
- **vendor** *type*: Specify the vendor type of the external IPAM server.

The following is an example configuration.

```
config
   ipam
      instance 1
         source external ipam
            host 209.165.200.225
            port 10000
            vendor cisco
            end
```

Verifying the IPAM Integration Configuration

This section describes how to verify the integration of IPAM in the SMF.

Verifying the Details of a Data Plane

Use the **show ipam dp** *data_plane_name* command to view details of a specific data plane (user plane).

The following is an example output of the **show ipam dp** *data_plane_name* command.

```
show ipam dp UPF-100
-------------------------------------------------------
Ipv4Addr   [Total/Used/Threshold] = 512 / 100 / 20%
Ipv6Addr   [Total/Used/Threshold] = 0 / 0 / 0.00%
Ipv6Prefix [Total/Used/Threshold] = 512 / 300 / 70%
Instance ID = 1
-------------------------------------------------------
```

Verifying the Threshold for Data Plane

Use the **show ipam dp** command to view the summary of the current threshold for each data plane (User Plane).

The following is an example output of the **show ipam dp** command.

```
show ipam dp
=================================================================
DpName     Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
=================================================================
UPF-100          20%              40%                70%
UPF-200          40%              20%                20%
=================================================================
```

Verifying the IPv4 Address Range Assigned to a Data Plane

Use the **show ipam dp** *data_plane_name* **ipv4-addr** command to view the IPv4 address ranges assigned to a data plane.

The following is an example output of the **show ipam dp** *data_plane_name* **ipv4-addr** command.

```
show ipam dp UPF-100 ipv4-addr
=============================================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================================
StartAddress          EndAddress       AllocContext   Route              G:N/P   Utilization
   Flag
=============================================================================================================
209.165.200.225  209.165.200.253  Pool-1        209.165.200.224/27 1:1/0     99.60%

209.165.201.1    209.165.201.30   Pool-2        209.165.201.0/27   1:1/0     99.60%
 R
=============================================================================================================
```

Verifying the IPv6 Address Range Assigned to a Data Plane

Use the **show ipam dp** *data_plane_name* **ipv6-prefix** command to view the IPv6 address ranges assigned to a data plane.

The following is an example output of the **show ipam dp** *data_plane_name* **ipv6-prefix** command.

```
show ipam dp UPF-100 ipv6-prefix
=============================================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================================
StartAddress                 EndAddress               AllocContext       Route
         G:N/P    Utilization   Flag
=============================================================================================================
2001:DB80:8f20::            2001:fc20:8f20:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f20::/48
      1:1/0    99.60%
2001:fc20:8f21::            2001:fc20:8f21:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f21::/48
      1:0/1    99.80%
2001:fc20:8f22::            2001:fc20:8f22:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f22::/48
      1:0/1    0.00%         R
2001:fc20:8f23::            2001:fc20:8f23:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f23::/48
      1:1/0    0.00%         R
2001:fc20:8f49::            2001:fc20:8f49:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f49::/48
      1:1/0    34.42%
2001:fc20:8f4f::            2001:fc20:8f4f:ffff::    ims-ipv6-pool1(n6) 2001:fc20:8f4f::/48
      1:0/1    33.58%
=============================================================================================================
```

Configuring IP Pool Selection Method

Use the following configuration to configure an IP pool selection method.

```
config
nssai name nssai_name
    dnn dnn
    pool-selection [ pool_selection_method  ]
    sdt sdt_value
    sst sst_value
    tai-group-list tai_group_list
    end
```

NOTES:

- **pool-selection [** *pool_selection_method* **]**: Configure the IP pool selection method as DNN or NSSAI. The default value of **pool-selection** is *dnn*. If you configure **pool-selection [** *nssai* **]** for a slice, then in IPAM configuration for all the DNN for that UPF, "slice1+dnn" is to be configured.

Note The slice-based pool selection is not supported.

Configuration Example

The following is an example configuration of the IP pool selection method.

```
nssai name slice1
pool-selection [nssai]
exit

nssai name slice2
pool-selection [nssai dnn]
exit

nssai name slice3
exit
```

Note If no pool selection method is configured, then the default value of **pool-selection [** *dnn* **]** is used.

Configuring UPF Group Profile for IP Pool Selection

To configure the UPF group profile for IP pool selection, use the following sample configuration.

Note This configuration is required to support the slice-based IP pool.

```
config
  profile network-element upf upf_name
    upf-group-profile upf_group_profile_name
    dnn-list dnn_list_value
    end
```

NOTES:

- **profile network-element upf** *upf_name*: Specify a profile name for the UPF.
- **upf-group-profile** *upf_group_profile_name*: Specify the name of the UPF group configuration. The *upf_group_profile_name* value must be a string.
- **dnn-list** *dnn_list_value*: Specify the list of DNNs that the UPF node supports. The *dnn_list_value* value must be a string with a range of DNN list values.

Configuration Example

The following is an example configuration.

```
profile network-element upf upf1
   upf-group-profile group1
   dnn-list [dnn1, dnn2]
```

Configuring Slice Group List for IP Pool Selection

To configure the slice group list for IP pool selection, use the following sample configuration.

Note This configuration is required to support the slice-based IP pool.

```
config
   profile upf-group upf_group_profile_name
      slice-group-list slice_group_list_name
      end
```

NOTES:

- **profile upf-group** *upf_group_profile_name*: Specify the UPF group name that must be associated to the specified UPF network configuration. The *upf_group_profile_name* value must be an alphanumeric string.
- **slice-group-list** *slice_group_list_name*: Specify the list of slice groups that the UPF node supports. The *slice_group_list_name* value must be a string with a range of slice groups.

Configuration Example

The following is an example configuration.

```
profile upf-group group1
 slice-group-list [ slice1 ]
exit
```

Note Based on the NSSAI configuration of the IP pool selection, the SMF sends the "slice + dnn" as tag to IPAM.

Example

```
profile network-element upf upf1
upf-group-profile group1
 dnn-list [dnn1, dnn2, dnn3]

profile upf-group group1
 slice-group-list [slice1, slice2 slice3]
exit
```

Static IP Support

Feature Description

IPAM is the core component of the subscriber management system. Traditional IPAM functionalities prove insufficient in the Cloud Native network deployments. Hence, IPAM requires more functionalities to work with the Cloud Native subscriber management system.

The Static IP Support feature enables the support of static IP on the SMF using IPAM. This feature supports the following functionalities:

- Static pool configuration—dynamic addition and deletion of static IP pool or static IP address range when the system is running.
- Splits static address ranges into smaller chunks and associates them with the configured UPFs
- Enables program routes according to static address range reservation during UPF association
- Enables secondary authentication under the DNN profile
- Selects UPF based on reserved address range and Framed-IP received from the Authentication response
- Handle UPF addition, deletion, and Sx path failure
- Add a DNN to an existing UPF

Calls with Static IP Address

The SMF supports calls with static IP address and validates if the IP address belongs to the static pool.

The SMF supports Create Session Request with static IP address and also handles Create Session Request received with PAA. The SMF validates if the requested IP address is configured under static pool and assigns the same IP address for the session. If the IP address is not configured under static pool, then SMF rejects the session.

Important In Release 2021.02, the SMF does not support fallback to dynamic IP allocation.

The following behavior is applicable only to sessions with static IP address.

- If the SMF receives static IP in Subscription Response from UDM during the 5G Session Create procedure, it assigns the same IP address to the UE session if the IP is configured under static pool. If the IP address is not configured under static pool, then SMF rejects the session.
- If the RADIUS interface is enabled and if the RADIUS server returns the static IP address, then SMF ignores the IP address received in Create Session Request or Subscription Response.

How it Works

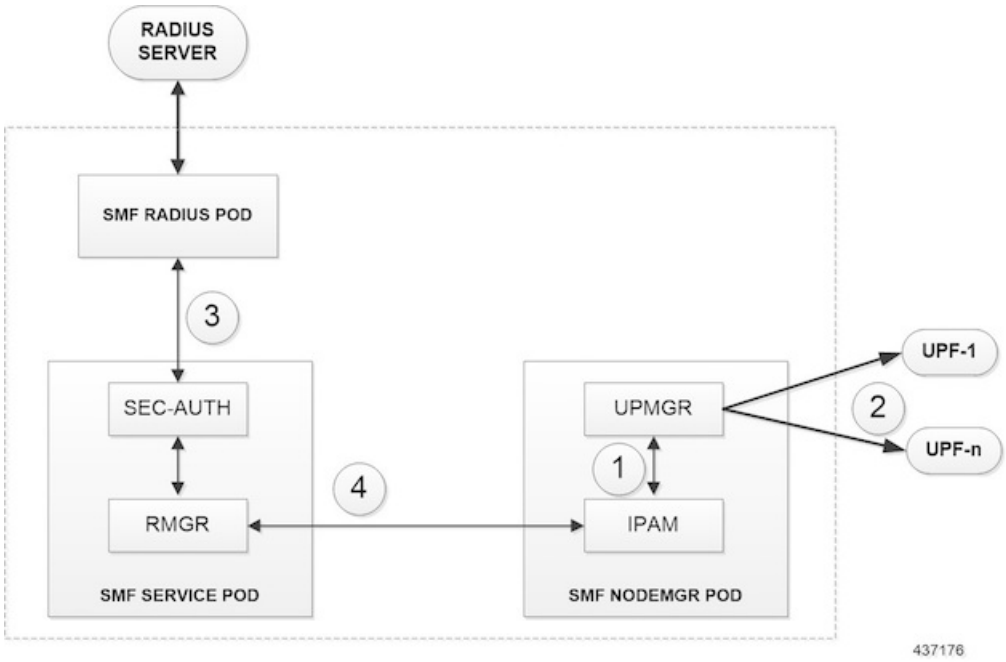
This section provides a brief of how the Static IP Support feature works.

The SMF receives a framed IP address of the subscriber from external AAA servers, such as RADIUS. While IPAM is not involved in individual IP address management in this scenario, it still handles the route management and UPF management for static address ranges.

IPAM splits the 'static' address ranges equally according to number of UPFs present in the SMF configuration. Unlike dynamic IP, IPAM splits all static IP address ranges and assigns them for all configured UPFs. IPAM involves and selects an UPF when the external AAA server returns the framed IP of the subscriber. IPAM looks for the route which includes this static IP and then selects the UPF where the route is already configured.

The following figure shows how the static IP address is assigned to the configured UPFs.

Figure 171: Static IP Address Management Procedure



1. IPAM splits the static ranges into equal number of address ranges based on the number of configured UPFs.
2. The UPMGR programs the corresponding static routes on the associated UPFs.
3. Subscribers get static IP from RADIUS server authorization response.
4. SMF service selects the right UPF based on address ranges and UPF map allocation from the Node Manager.

Address Range Split

Splitting a given address range into smaller address ranges is a key functionality of the IPAM server and IPAM cache. The following guidelines determine address range split:

- Size of a split address range depends on the configured value or the default value as per the Authority and Format Identifier (AFI) type.
- Size of a split address range must be a power of 2 or at least to the closest of it. That is, it should be able to represent the split range in subnet/mask notation such that a route can be added in the data plane (user plane) if required.
- Configured or default address range size must be at the power of 2.

The address range must be split into smaller ranges immediately on configuration or initial start-up. This helps in better sorting of address ranges based on size and faster allocation during actual address range allocation requests. The address range exchange between modules is always in the mentioned size.

Table 300: Examples of IPv4 Address Range Split

Address Range	Split Size (number of addresses per range)	Split Ranges (* Odd sized ranges)	Route Notation
209.165.200.225 - 209.165.200.254	128	[1] 209.165.200.225 – 209.165.200.254 [2] 209.165.202.129 – 209.165.202.158	[1] 209.165.200.224/27 [2] 209.165.202.128/27
209.165.201.1 – 209.165.201.30	256	[1] 209.165.200.224 – 209.165.200.254 [2] 209.165.201.0 – 209.165.201.30 [3] 209.165.202.128 – 209.165.202.158 ... [n] 209.165.200.225 – 209.165.200.253	[1] 209.165.201.1/27 [2] 209.165.200.224/27 [3] 209.165.202.128/27 ... [n] 209.165.201.0/27
209.165.200.229 – 209.165.200.253	256	[1] 209.165.201.1 – 209.165.201.30 * [2] 209.165.202.129 – 209.165.202.158 [3] 209.165.200.225 – 209.165.200.253 *	[1] 209.165.201.0/27 [2] 209.165.200.224/27 [3] 209.165.202.128/27

Table 301: Examples of IPv6 Address Range Split

Address Range	Split Size (number of addresses per range)	Split Ranges (* Odd sized ranges)	Route Notation

1:: - 1::1000	1024	[1] 1:: – 1::3FF [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF [4] 1::C00 – 1::FFF	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 [4] 1::C00/118
1::3 - 1::1DEF	1024	[1] 1::3 – 1::3FF * [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF … [n] 1::1C00 – 1::1DEF *	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 … [n] 1::1C00/118

Examples of IPv6 Address Range Split

Prefix split needs two length fields for performing the split.

- Network length
- Host length

Prefixes are split between these two length fields and a new route is calculated.

Example 1: network-length = 48, prefix-length = 64

Total (64-48) = 16 bits (that is, 65536 prefixes are available for the split)

Example 2: network-length = 32, prefix-length = 56

Total (56-32) = 24 bits (that is, 16 million prefixes available for the split)

Note For SMF, the host-length is hard-coded as ‘64’. Only network-length can be configured using the CLI.

Table 302: Examples of IPv6 Address Range Split

Prefix Range	Split Size (number of addresses per range)	Split Ranges (* Odd sized ranges)	Route Notation
1:2:3:: Nw-len = 48 Host-len = 64	8192	[1]1:2:3:: ... 1:2:3:1fff [2]1:2:3:2000:: ... 1:2:3:2fff:: [3]1:2:3:3000:: ... 1:2:3:3fff:: ...	[1]1:2:3::/51 [2]1:2:3:2000/51 [3]1:2:3:3000/51 ...

Call Flows

This section describes the static IP call flow.

The following figure shows the static IP address allocation call flow.

Figure 172: Static IP Call Flow

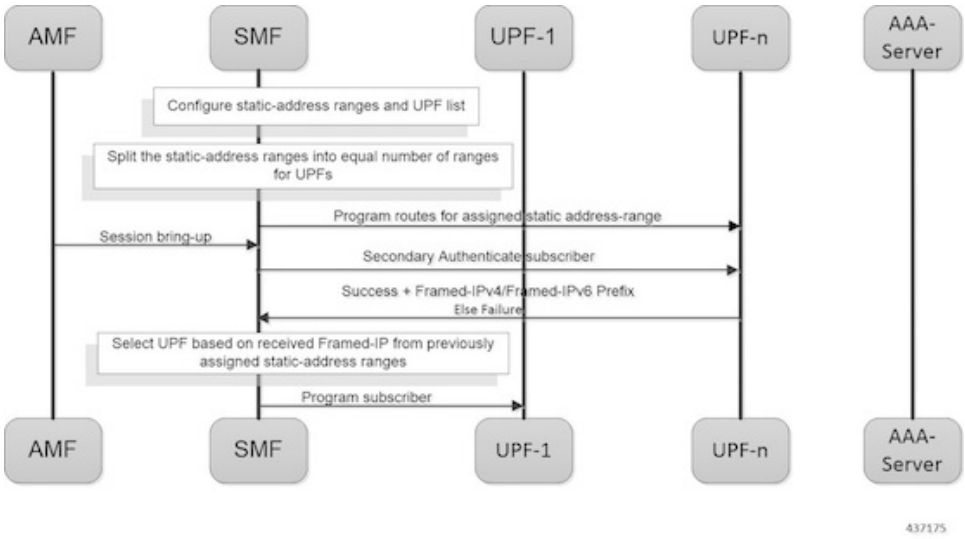


Table 303: Static IP Call Flow Description

Step	Description
1	Configure the static address ranges and UPF list.
2	Split the static address ranges into equal number of ranges for UPFs.
3	Enable program routes for the assigned static address range.
4	Bring up the session.
5	Enable secondary authentication under the DNN profile.
6	The SMF sends the Authentication Request to the RADIUS server. The RADIUS server sends an Authentication Response with the static IP of the subscriber. The SMF selects the UPF based on the static IP and continues with the programming.
7	Complete the subscriber programming.

Adding a DNN

This section describes the sequence of operations for adding a DNN.

1. Create a static IP pool in IPAM with the corresponding DNN.
2. Add a DNN Profile.
3. If applicable, add the UPFs.
4. Associate the IP address ranges of the DNN to the available UPFs.

Note The route is added as part of RegisterUpf requests during explicit Sx association.

Adding a Static IP Address Range

This section describes the sequence of operations for adding a static IP address range in SMF.

- If new static IP address range is added to a single stack IP pool, the IP address ranges are split according to the configuration and associated with available UPFs in load sharing manner.
  1. Similar to initial association, intermediate association is also done based on the number of IP addresses against the number of configured UPFs.
  2. If UPF is already registered with IPAM:
     - Route addition is triggered, or else
     - No immediate action is taken

- If a dual stack pool is configured, all IP address ranges, both IPv4 and IPv6 are associated with the UPF, which is the least loaded.
  - If UPF is already registered with IPAM:
    - Route addition is triggered, or else
    - No immediate action is taken

Adding a Static IP Pool

This section describes the sequence of operations for adding a static IP pool in SMF.

- If a single stack IP pool is configured, the IP address ranges are split according to the configuration and associated with available UPFs in load-sharing manner.
  1. Similar to initial association, intermediate association is also done based on the number of IP addresses against the number of configured UPFs.
  2. If UPF is already registered with IPAM:
     - Route addition is triggered, or else
     - No immediate action is taken

- If a dual stack pool is configured, all IP address ranges, both IPv4 and IPv6 are associated with the UPF, which is the least loaded.
  - If UPF is already registered with IPAM:
    - Route addition is triggered, or else
    - No immediate action is taken

Adding the UPF

This section describes the sequence of operations for adding the UPF.

1. When a UPF is added, NodeMgr sends the list of IPs to IPAM.
2. When new static IP pool or static IP address range is configured, this feature enables route association for UPFs based on load balancing model.

Note The same procedure is applicable when a new or existing DNN is added to a new or existing UPF respectively.

3. To redistribute existing static IP pools or ranges to the new UPF, use the following procedure:
   - Mark a pool/range offline
   - Clear the subscribers
   - Delete IP pool or range
   - Add the IP pool or range again.

     This step allocates the chunks to the new UPF.

Deleting the UPF

This section describes the sequence of operations for deleting an existing UPF.

1. To delete an existing UPF, it is first marked "offline".

   Run the appropriate CLI commands to manually clear the sessions.
2. The NodeMgr notifies IPAM about the UPF removal.
3. IPAM moves the static address ranges from all DNNs of the removed UPF to other available UPFs.
4. The Nodemgr initiates ReleaseUpf to IPAM. IPAM releases dynamic address ranges to the free list.
5. The Nodemgr sends an N4 Association Release message to UPF and to clean up UPF from the cache.

Note If the UPF is not marked offline and a manual clean-up is not performed before its removal, the system behavior might be erratic.

Deleting a Static IP Address Range

This section describes the sequence of operations for deleting a static IP address range in SMF.

1. To delete an IP address range from a static IP pool, it is first marked "offline".
2. Reject new calls, which have the IP address assigned from the offline IP address range.
3. Remove the existing subscribers. To remove the existing subscribers, run the following CLI commands:

```
clear subscriber ipv4-range { pool_name | start_of_range }
clear subscriber ipv6-range { pool_name | start_of_range }
```

4. Remove the static IP address range configuration and trigger route deletion to the registered UPFs.

Deleting a Static IP Pool

This section describes the sequence of operations for deleting a static IP pool in SMF.

1. To delete a static IP pool, it is first marked "offline".
2. Reject new calls, which have the IP address assigned from the offline IP pool.
3. Remove the existing subscribers. To remove the existing subscribers, run the following CLI commands:

```
clear subscriber ipv4-pool pool_name
clear subscriber ipv6-pool pool_name
```

4. After all the subscribers are deleted, remove the IP pool configuration and trigger route deletion to the registered UPFs.

Removing Sx Association with an Offline UPF

This section describes the sequence of operations for removing association with an offline UPF.

1. Set UPF as offline in **profile-network-element-upf** configuration.

   SMF stops selecting and associating dynamic IPs to the specific UPF for new sessions.
2. NodeMgr receives configuration change notification about an offline UPF.

   SMF stops selecting and associating static IPs to the specific UPF for new sessions or associations.
3. NodeMgr acknowledges the heart-beat messages for an already associated UPF.
4. NodeMgr acknowledges the N4 association update from the UPF with release indication.

   This step does not impact the static and dynamic chunk allocations for IPAM.

   The IPAM module is unaware of the offline status for the UPF. It might include the offline UPF to add new IP pool or address ranges.

Sx Path Failure on UPF

This section describes the sequence of operations for Sx path failure on UPF.

1. The NodeMgr initiates the **clear subscriber** command.
2. The NodeMgr sends UnRegisterUpf to IPAM.
3. IPAM releases any dynamic IP address ranges and moves it to free range list.
4. IPAM retains any static IP address ranges for the UPF. Sx path failure does not impact static IP address mappings.

Limitations

The Static IP Support feature has the following limitations:

- Change of a pool from dynamic to static, and from static to dynamic is not supported when the system is in running mode.
- Addition or removal of UPF is not supported when the system is in running mode.
- The address range split must be optimal based on the number of UPFs and number of addresses in the ranges.

  For example:

  If there are 2 UPFs and 1024 addresses specified in the range, then specify the per-dp-split-size as 512.

  If there are 3 UPFs and 1024 addresses, then specify the per-dp-split-size as 256.
- When the system is running, the DNN cannot be removed from a UPF.
- Changing dual-stack IPAM pool to single-stack or changing single-stack IPAM pool to dual-stack is not supported.

Configuring Static IP Support

To configure the Static IP Support feature, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            static
            end
```

NOTES:

- **ipam**: Enter the IPAM configuration mode.
- **address-pool** *pool_name*: Specify the name of the address pool to enter the pool configuration. *pool_name* must be a string.
- **static**: Enable the static IP mode.

Statistics Support

The smf_service_resource_mgmt_stats and smf_service_node_mgr_stats provide details on static IP allocation type information.

The ip_req_type attribute in these statistics supports the following labels:

- ip-static-subscription—Static IP allocation information based on subscription
- ip-static-radius—Static IP allocation information based on RADIUS

Dual-stack Static IP Support Through IPAM

Feature Description

The SMF supports dual-stack static IP using IPAM. For dual-stack sessions, the AAA server sends both the IPv4 and IPv6 address prefixes as part of the Access-Accept message. In the SMF-IPAM configuration, both the IPv4 and IPv6 address prefixes are added in the same pool. The IPAM assigns both the IPv4 and IPv6 routes to a single UPF.

During the UPF selection, the Node Manager application uses the UPF for both the IPv4 and IPv6 addresses from the IPAM to handle them accordingly.

How it Works

The SMF supports dual-stack static IP through IPAM in the following ways:

- Pool to UPF mapping—Based on the number of UPFs available, the IPv4 address ranges and IPv6 prefix ranges are split into smaller chunks. Then, the pair (chunk) is configured into the same IPAM pool.

  IPAM assigns all the addresses and prefixes that are configured in one dual-stack pool to a UPF in the manner they are received. The AAA server returns the dual-stack addresses from the same pair. From these addresses, SMF selects one UPF for dual-stack programming.

  The load-balancing of number of addresses and prefixes are managed. IPAM performs only the dual-stack static-pool to UPF mapping.

- Address range no-split configuration—IPAM uses the "no-split" configuration to prevent the splitting of address ranges into smaller chunks. This configuration helps to prevent having multiple routes programming for a specific range.

The following table lists the errors or exceptions and how to handle them:

Table 304: Error and Exception Handling

Error or Exception	Exception Handling
IPv4 UPF and IPv6 UPF are configured incorrectly	**1.** Select an active UPF. In case both the UPFs are active, select the UPF with the IPv4 address. **2.** Reset the IP information of the other stack and update the PDU session type accordingly.
IPv4 address is invalid or null	Select the UPF with IPv4 address and update the PDU session type accordingly.
IPv6 prefix is invalid or null	Select the UPF with IPv6 address and update the PDU session type accordingly.
IPv4 address and IPv6 prefix are invalid	Reject both the IPv4 address and IPv6 prefix.

Limitations

The Dual-stack Static IP Support feature has the following limitation:

- The change in ‘no-split' configuration is not supported when the system is in running mode.

Configuring Dual-stack Static IP

This section describes how to configure the dual-stack static IP support using IPAM.

Configuring IPAM No-Split

To configure the IPAM no-split, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
         ipv4
            split-size no-split
            exit
         ipv6 prefix_ranges
            split-size no-split
            exit
         exit
```

NOTES:

- **split-size no-split**: Prevent the IPv4 address ranges or IPv6 prefix ranges from splitting into smaller chunks.

IPAM Offline Mode Support

Feature Description

SMF supports addition of a dynamic pool, IPv4, or IPv6 address-range to a dynamic pool by default. The new chunks are added to the respective tags, such as DNN, and are assigned from the same pool.

How it Works

Following is the process to delete a dynamic pool or an IPv4 or IPv6 address range from a dynamic pool:

1. Configure the pool or address range as offline. The IPAM then stops assigning addresses from the respective pool or address range.
2. Use the following **clear subscriber** CLI commands to delete the subscribers based on respective pool or address range that are configured to offline mode:
   - **clear subscriber ipv4-pool** *pool_name*
   - **clear subscriber ipv4-range** *pool_name/start_of_range*

- **clear subscriber ipv6-pool** *pool_name*
- **clear subscriber ipv6-range** *pool_name/start_of_range*

3. Use the following **cdl show** CLI commands and wait until all the subscribers are deleted:
   - **cdl show sessions count summary filter { key ipv4-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv4-range:** *pool_name/start_of_range* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-pool:** *pool_name* **condition match }**
   - **cdl show sessions count summary filter { key ipv6-range:** *pool_name/start_of_range* **condition match }**
   - **cdl show sessions count summary slice-name** *slice_name*
4. After all the subscribers are deleted, delete the pool or address range from the IPAM configuration.

Configuring the IPAM Offline Mode

This section describes how to configure the IPAM offline feature for pool, IPv4 address range, and IPv6 prefix ranges.

Configuring Pool to Offline Mode

To configure the entire pool to offline mode, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            offline
            end
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the pool to enter the pool configuration. *pool_name* must be a string.
- **offline**: Configure the pool to offline mode.

Setting IPv4 Address Range to Offline Mode

To configure the IPv4 address range to offline mode, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv4
```

```
address-range start_ipv4_address end_ipv4_address offline
end
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the pool to enter the pool configuration. *pool_name* must be a string.
- **ipv4**: Enter the IPv4 mode.
- **address-range** *start_ipv4_address end_ipv4_address* **offline**: Specify the IP addresses for the start and end IPv4 address range.
  - **offline**: Set the selected address range to offline mode.

Setting IPv6 Prefix Ranges to Offline Mode

To configure IPv6 prefix range to offline mode, use the following sample configuration:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
         vrf-name vrf_name
            ipv6
               prefix-ranges
                  prefix-range prefix_valuelength prefix_lengthoffline
                  end
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the pool to enter the pool configuration. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode.
- **prefix-ranges**: Enter the prefix ranges mode.
- **prefix-range** *prefix_value* **length** *prefix_length* **offline**: Specify the prefix range and prefix length of the IPv6 prefix range.
  - **offline**: Set the selected address range to offline mode.

IPAM Redundancy Support Per UPF

Feature Description

The SMF supports IPAM redundancy and load balancing for each UPF. The IPAM running in the Node Manager microservice has two IPAM instances that are associated to each UPF. When one IPAM instance is inactive, the other IPAM instance manages the address allocation requests for the UPF.

How it Works

This section provides a brief of how the IPAM redundancy support per UPF feature works.

- Peer Selection—The Node Manager peer is selected during the UPF association.
- UPF Registration with Peer IPAM—IPAM is notified with the instance ID of the peer for the UPF during the registration of the UPF call. IPAM allocates routers from the local data for the specific DNN and checks if the peer IPAM instance is in active or inactive state.

  If the peer IPAM instance is active, a REST call is sent to it to register to the same UPF in the local instance and to receive the routes as response.

  If the peer IPAM instance is inactive, the local instance takes over the IPAM context of the remote instance. Then, the local instance registers to the UPF, receives the routes, and keeps the data back in the cache pod. After the peer instance is active, it restores the same data from the cache pod.

  Routes from both the instances are sent to UPF for load-balanced address allocations from both the instances.
- Address Allocation in Load-Balanced Model—As one UPF is registered to two IPAM servers, SMF sends the address allocation requests to any peer that is load-balanced. Respective IPAM instances assign new addresses from their local address bitmap. If one peer instance is inactive, the other peer instance handles all the requests.
- Address Release Request Handling—In IPAM, the Address Release request is sent to the instance that had allocated the IP the first time. If that peer is inactive, the Address Release request is sent to the peer IPAM.

  The IPAM instance that receives the address releases for remote instances, keeps buffering these instances locally and updates the cache pod periodically. After the remote peers are active, they handle the buffered address release requests.
- Release of the UPF—When a peer IPAM is active during the release of a UPF, a REST call is sent to clear the data. If the peer IPAM is inactive, the existing IPAM instance takes over the operational data of the remote IPAM, clears the UPF information, and updates the cache pod.

IPAM Quarantine Timer

Feature Description

The IPAM Quarantine Timer Support feature supports the IPAM quarantine timer for the IP pool address. This feature keeps the released IP address busy until the quarantine timer expires to prevent the reuse of that IP address. Each IP pool must be configured with a timer value. This value determines the duration of a recently released address to be in the quarantine state before it is available for allocation. After the timer expires, the IP address is available in the list of free addresses for allocation by the subscriber. A released IP address with no address quarantine timer is considered to be in use for allocation. If a subscriber attempts to reconnect when the address quarantine timer is armed even if it is the same subscriber ID, the subscriber does not receive the same IP address.

Configuring IPAM Quarantine Timer

This section describes how to configure the IPAM quarantine timer.

Configuring IPAM Quarantine Timer

This section describes how to configure the IPAM quarantine timer.

```
config
   ipam instance instance_id
      address-pool pool_name
         address-quarantine-timer quarantine_timer_value



         end
```

NOTES:

- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **address-quarantine-timer** *quarantine_timer_value*—Specifies the value of the quarantine timer in seconds. *quarantine_timer_value* must be in the range of 4-3600 seconds. The default value is 4.

IP Address Validation with CDL Configuration

This section describes how to validate IP Address with CDL configurtation.

System Diagnostics IP Validation

This section describes how to enable/disable System Diagnostics IP Validation.

```
config
   system-diagnostics ip-validation enable ignore-mismatch-responses
   exit
```

NOTES:

system-diagnostics ip-validation ignore-mismatch-responses — Ignores any CDL inconsistencies during address validation.

IP validation ignore mismatch responses is meant for avoiding duplicate IPs. If this feature is enabled, SMF Nodemgr checks if the current IP is already used by any other records in CDL. If no records are found, then IP address is assigned to the UE. If CDL record is found, then a new IP is assigned to the UE.

Important Enabling validation ignore mismatch responses may have certain performance impact.

Statistics

nodemgr_diag_ip_verify

Description: Display Nodemgr to CDL IP-Validation query related statistics

Metrics-Type: Counter

Query: sum(nodemgr_diag_ip_verify{namespace="$namespace"}) by (status)

Labels:

Label: status

Value: success | duplicate_record_found | cdl_ipc_failure | ipv4_alloc_failed | ipv6_alloc_failed | unknown

- success Record not found in CDL
- duplicate_record_found Duplicate record found in CDL
- cdl_ipc_failure Search IPC request to CDL failed
- ipv4_alloc_failed IPV4 address-request failed, unable to get free-IP, twice
- ipv6_alloc_failed IPV6 prefix-request failed, unable to get free-IP, twice
- unknown IPC request to CDL failed twice, give-up and return the IP to smf-service

IPAM_Quarantine_Statistics

Description: Display IPAM Quarantine IP Batch related statistics

Metrics-Type: Counter

Query: sum(IPAM_Quarantine_Statistics{namespace="$namespace"}) by (addressType, type)

Labels:

Label: pool

Value: <name-of-pool>

Label: upf

Value: <name-of-upf>

Label: addressType

Value: IPv4 | IPv6PD

Label: type

Value: start_batch_qsize | end_batch_qsize | pop_count_qtime | pop_count_qsize | avg_qtime_secs

- start_batch_qsize - Number of IPs in QT-queue at the start of batch processing
- end_batch_qsize - Number of IPs in QT-queue at end of batch processing
- pop_count_qsize - Number of IPs removed from QT-queue due to qsize limit
- pop_count_qtime - Number of IPs removed from QT-queue due to qtime limit
- avg_qtime_secs - Average time-in-seconds the IPs were in QT-queue before removing

IPAM Data Reconciliation

Feature Description

The SMF supports the IPAM data reconciliation feature to reconcile IPAM data with the CDL records. This feature is triggered through the EXEC mode CLI. IPAM reconciliation is triggered at instance level, pool level, and chunk level.

Triggering IPAM Reconciliation

This sections describes how to trigger the IPAM reconciliation on instance level, pool level, and chunk level.

Triggering IPAM Reconciliation at Instance Level

To trigger IPAM reconciliation at an instance level, use the following CLI command:

reconcile ipam instance *instance_id*

NOTES:

- **reconcile ipam instance** *instance_id*: Trigger IPAM reconciliation for a specific GR instance ID.

Triggering IPAM Reconciliation at Pool Level

To trigger IPAM reconciliation at a pool level, use the following CLI command:

reconcile ipam instance *instance_id* **pool-name** *pool_name*

NOTES:

- **pool-name** *pool_name* : Trigger IPAM reconciliation for a specific address pool.

Triggering IPAM Reconciliation at Chunk Level

To trigger IPAM reconciliation at a chunk level, use the following CLI command:

reconcile ipam instance *instance_id* **pool-name** *pool_name* **chunk-start-ip** *chunk_start_ip_address*

NOTES:

- **chunk-start-ip** *chunk_start_ip_address* : Specify the IPAM reconciliation chunk starting IP address.

IPAM Periodic Reconciliation

The IPAM reconciliation can be triggered manually through the CLI. It also gets triggered on the nodemgr startup or after the GR role-switchover.

This process needs upgradation to a system or a software-dependent procedure. It requires a support to provide the IPAM reconciliation configuration, to run a time-driven activity, periodically in the background.

You can schedule to run a daily IPAM reconciliation activity, using the CLI configuration framework for the following:

- Specific GR instances ID
- Specific address pool under a GR instance ID

The IPAM reconciliation process performs multiple queries to the CDL and fetches subscriber sessions to sync or to update the IPAM cache-data data.

Limitations

This feature has the following limitations:

- Schedule the periodic IPAM reconciliation, during the time when the system has less traffic load management.
- Scheduling multiple reconciliations at the same time of the day isn't supported.
- The nodemgr can trigger only one instance of the reconciliation process at a time.
- Multiple reconciliation schedules can be set across pools, by ensuring at least with a gap of five minutes between two triggers.
- The IPAM reconciliation is supported only for non-static pools.

Feature Configuration

The updated IPAM configuration CLI framework supports the following:

- Scheduling of the reconciliation for GR Instance ID
- Specific address pool support

To configure this feature, use the following configuration:

```
config
    ipam
        instance <gr_instance_id>
            reconcile-schedule
                tod-hour <time_of_day_hour_value>
                tod-minute <time_of_day_minute_value>
…
        address-pool <pool_name>
            reconcile-schedule
                tod-hour <time_of_day_hour_value>
                tod-minute <time_of_day_minute_value>
                end
```

NOTES:

- **ipam**—Enter the IPAM configuration.
- **instance** <*gr_instance_id*>—Specify the IPAM reconciliation for a specific GR instance ID.
- **address-pool** <*pool_name*>—Specify the name of the pool to enter the pool configuration. The <*pool_name*> must be the name of the address pool.

- **reconcile-schedule**—Specify the required schedule for reconciliation. You can configure the time-of-day value in hours and minutes, to set the time for triggering the daily reconciliation at that specified time.
- **tod-hour** <*time_of_day_hour_value*>—Specify your required time of the day in hours. You can configure the specified hour in a 24-hour format 0–23.
- **tod-minute** <*time_of_day_minute_value*>—Specify your required time of the day in minutes. You can configure the specified minute in a 60 minute format 0–59.

Configuration Example

The following example configuration allows the IPAM to set a daily schedule to trigger reconciliation for gr-instance-id 1 at midnight 00:00.

```
config
 ipam
  instance 1
   reconcile-schedule
    tod-hour   0
    tod-minute 0
   exit
```

The following example configuration allows the IPAM to set a daily schedule to trigger reconciliation for testPool1 for gr-instance-id 1 at 10:30 p.m. daily.

```
config
 ipam
  instance 1
   address-pool testPool1
    reconcile-schedule
     tod-hour   22
     tod-minute 30
    exit
    ipv4
     split-size
      per-cache 8192
      per-dp    1024
     exit
     address-range 209.165.200.225 209.165.200.254
    exit
   exit
  exit
```

Configuring IPAM Quarantine Qsize

This section describes how to configure the IPAM quarantine queue size support feature.

Configuring IPAM Quarantine Queue Size

This section describes how to configure the IPAM quarantine timer.

```
config
   ipam instance instance_id
      address-pool pool_name
         address-quarantine-qsize quarantine_queue_size
```

```
 exit
exit
```

NOTES:

- **ipam**—Enter the IPAM configuration.
- **address-pool** *pool_name*—Specifies the name of the pool to enter the pool configuration. *pool_name* must be the name of the address pool.
- **address-quarantine-qsize** *quarantine_queue_size*—Specifies the value of the quarantine queue size. The default value is 0.

  During QT processing, excess IP addresses in quarantine-queue are released to Free-list irrespective of quarantine-timer expiry by force.

Overlapping IP Address Pools

Feature Description

The Overlapping IP Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

You can configure overlapping IP address range across different pools with unique DNN and VRF type.

Configuring Overlapping IP Address Pools

Use the following example configuration to configure overlapping static IP address pools.

```
config
ipam instance instance_id 1
source local
address-pool pool1
  static
  vrf-name vrf1@ISP
  tags
   dnn dnn1
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
address-pool pool2
  static
  vrf-name vrf2@ISP
  tags
   dnn dnn2
  exit
  ipv4
   split-size
    per-cache 256
```

```
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
exit
```

The following is an example configuration for overlapping IP address pools.

```
config
ipam instance instance_id 1
source local
address-pool pool1
  vrf-name vrf1@ISP1
  tags
   dnn dnn1
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
address-pool pool2
  vrf-name vrf2@ISP2
  tags
   dnn dnn2
  exit
  ipv4
   split-size
    per-cache 256
    per-dp    256
   exit
   address-range 209.165.200.225 209.165.200.254
  exit
exit
exit
```

Auto-Reclamation of Under-Utilized IP Chunks

Feature Description

SMF supports auto-reclamation of under-utilized IP chunks that are allocated to various UPF nodes. By configuring the Utilization Threshold and Inactivity Threshold, SMF can trigger the auto-reclamation process periodically or on an instant basis.

The under-utilization and inactivity of IP chunks are detected based on the inactivity timer configuration. When inactivity and under-utlization are detected, SMF triggers IP chunk reclamation by clearing all the subscribers using the IP chunk. SMF also triggers route deletion to UPF.

Limitations

Following are the known limitations of auto-reclamation of under-utilized IP chunks in SMF:

- During reclamation of under-utilized IP chunk, all released IPs must undergo configured address pool level Quarantine Time (QT time).
- If an IP from the reclaimed IP chunk is associated with an active subscriber session, SMF tears down the subscriber session and is expected to see session discontinuity.
- Rolling update must be avoided during scheduled reclamation procedure.

Configuring Instant Reclamation Process for Under-Utilized IP Chunks

Use the following configuration to execute instant reclamation of under-utilization of IP chunks:

exec-ipam reclaim-chunk { utilization-threshold *utilization_threshold* **inactivity-threshold** *inactivity_threshold* **[instance** *grInstance* **] [pool-name** *poolName* **] [chunk-start-ip** *ip* **] }**

NOTES:

- **exec-ipam**—This command executes IPAM commands.
- **reclaim-chunk**—This CLI executes IP chunk reclamation procedure.
- **utilization-threshold** *utilization_threshold*—This CLI is used to configure the utilization threshold for reclamation.
- **inactivity-threshold** *inactivity_threshold*—This CLI is used to configure the inactivity threshold for reclamation.
- **instance** *grInstance*—This CLI allows configuring GR instance ID.
- **pool-name** *poolName*—This CLI allows defining the pool name.
- **chunk-start-ip** *ip*—This CLI allows defining the Chunk Start IP of a specific pool.

Configuration Example

Following is the sample configuration for instant IP chunk reclamation process:

```
exec-ipam reclaim-chunk utilization-threshold 2 inactivity-threshold 180 instance 1 pool-name
 poolv4 chunk-start-ip 209.165.201.1
```

Configuring Periodic Reclamation Process for Under-Utilized IP Chunks

Use the following configuration to trigger periodic reclamation of under-utilization of IP chunks:

```
config
   ipam
      instance instance_id
         chunk-reclamation { schedule tod-hour tod_hour_value schedule
tod-minute tod_min_value utilization-threshold utilization_threshold
inactivity-threshold inactivity_threshold }
         exit
      exit
   exit
```

NOTES:

- **chunk-reclamation**—This CLI is used to configure periodic IP chunk reclamation.
- **schedule**—This CLI is used to configure Time of Day values for the chunk-reclamation process.
- **tod-hour** *tod_hour_value*—This CLI is used to configure the Time-of-day hour value for the chunk-reclamation process. The value range for **tod-hour** is <0-23>.
- **tod-minute** *tod_min_value*—This CLI is used to configure the Time-of-day minute value for the chunk-reclamation process. The value range for **tod-minute** is <0-59>.
- **utilization-threshold** *utilization_threshold*—This CLI is used to configure the utilization threshold for reclamation. The value range for **utilization-threshold** is <0-20>. The default value is 2.
- **inactivity-threshold** *inactivity_threshold*—This CLI is used to configure the inactivity threshold for reclamation. The value range for **inactivity-threshold** is <0-3600>. The default value is 1800.

Note It is suggested to configure Time-of-day when traffic is expected to be low.

Configuration Example

Following is the sample configuration for periodic IP chunk reclamation process:

```
config
  ipam
    instance <instance>
      chunk-reclamation
        schedule tod-hour <0..23> tod-minute <0..59>
        utilization-threshold <0..20>
        inactivity-threshold  <0..3600>
      exit
    exit
  exit
exit
```

Configuration Verification

To verify the confiuration, following show command should be used:

```
[smf] smf# show running-config ipam instance 1 chunk-reclamation
Tue May  16 20:36:58.887 UTC+00:00
ipam
instance 1
  chunk-reclamation
   schedule tod-hour 22
   schedule tod-minute 10
   utilization-threshold 5
   inactivity-threshold  600
  exit
exit
exit
```

OAM Support

This section discusses the metrics supported in this feature.

Bulk Statistics

Following counters are supported as part of chunk reclamation process:

IPAM_chunk_reclamation_count: It is a counter that specifies the total IP chunks reclaimed. It is triggered when an IP chunk gets reclaimed. This metric shall be maintained at GR-Instance, IP pool, address-type, UPF, remote instance, and trigger state levels.

disc_ip_chunk_reclamation: This counter is added as a reason under **smf_active_call_disconnect_stats** and **smf_disconnect_stats** statistics. This metric is introduced for sessions cleared due to chunk reclamation.

Unique IP Pools for UPFs

Feature Description

With this feature, SMF enables you to perform the following tasks:

- Allocate specific set of IP pools for edge UPFs in such a way that the UPFs do not share the same IP pool
- Fall back to centrally located UPF when the edge UPF is down

For unique IP pool assignment to UPFs, SMF uses tag with IP address pools in the IPAM configuration based on the location DNN. Then, the SMF associates this tag name while configuring UPF selection for each DNN.

To implement the fall back to central UPF, SMF provides option to configure a central UPF if edge UPF is down.

Configuring SMF for Unique IP Pools

This section provides the configurations that are required to ensure unqiue IP address allocation to the UPFs.

Configuring this feature involves the following steps:

- Configuring Tags Based on Location DNN, on page 782
- Enabling UPF Fallback, on page 783

Configuring Tags Based on Location DNN

To define the location-based DNN profile, use the following sample configuration:

```
config
   profile location-dnn location_dnn_name
      location-area-group la_group_name profile dnn_profile_name
      end
```

NOTES:

- **profile location-dnn** *location_dnn_name*—Specify the name of the location-based DNN profile.
- **location-area-group** *la_group_name* **profile** *dnn_profile_name*—Specify the name of location area group where the subscriber belongs to and the DNN profile.

Based on the location defined in this profile, SMF tags the IP pools and selects the UPF for each DNN.

Enabling UPF Fallback

To enable the UPF fallback functionality with unique IP pools, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      dnn rmgr dnn_name fallback secondary_dnn_name
      end
```

NOTES:

- **profile dnn** *dnn_profile_name*—Specify the name of the DNN profile.
- **dnn rmgr** *dnn_name* **fallback** *secondary_dnn_name*—Specify the name of primary and secondary DNNs.

  SMF enables the fallback to centrally located UPF based on the DNN when any of the following conditions are fulfilled:

  - IP pool and UPF selected based on location fails.
  - UPF of the configured DNN is down.
  - Location of the UE isn't configured.

Configuration Example

The following is an example of the configuration used for unique IP pool allocation.

```
config
profile location-area-group lag1
 tai-group tai-grp
exit
profile location-area-group lag2
 tai-group tai-grp2
exit
profile location-dnn dnnloc-1
 location-area-group  lag1 profile dnnprof-ims-1
 location-area-group  lag2 profile dnnprof-ims-2
exit
policy dnn polDnn
 dnn ims profile dnnprof-ims //fallback dnn profile
 dnn ims location-dnn-profile  dnnloc-1 //location-based dnn profile
exit
profile upf-group upf-group1
 location-area-group-list [ lag1 ] //grouping upf based on location
 failure-profile FHUP
exit
profile upf-group upf-group2
 location-area-group-list [ lag2 ] //grouping upf based on location
 failure-profile FHUP
exit
profile upf-group upf-group3 // central upf group - no location tag
 failure-profile FHUP
exit

profile network-element upf nfprf-upf1
 node-id           n4-peer-DAUI0301
```

```
 n4-peer-address ipv4 209.165.201.3
 n4-peer-port      8805
 upf-group-profile upf-group1//ims-lag1 picks upf-group1, based on location
 dnn-list          [ ims-lag1 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf3
 node-id           n4-peer-DAUI0303
 n4-peer-address ipv4 209.165.201.4
 n4-peer-port      8805
 upf-group-profile upf-group1//ims-lag1 picks upf-group1, based on location
 dnn-list          [ ims-lag1 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf5
 node-id           n4-peer-DAUI0305
 n4-peer-address ipv4 209.165.201.5
 n4-peer-port      8805
 upf-group-profile upf-group2//ims-lag2 picks upf-group2, based on location
 dnn-list          [ ims-lag2 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf7
 node-id           n4-peer-DAUI0307
 n4-peer-address ipv4 209.165.201.6
 n4-peer-port      8805
 upf-group-profile upf-group2//ims-lag2 picks upf-group2, based on location
 dnn-list          [ ims-lag2 magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit
profile network-element upf nfprf-upf8
 node-id           n4-peer-DAUI0308
 n4-peer-address ipv4 209.165.201.7
 n4-peer-port      8805
 upf-group-profile upf-group3//ims-central picks upf-group3, if location is not available
 dnn-list          [ ims-central magenta-ims-dnn sos-pool-ipv6 ]
 capacity          10
 priority          1
exit

profile dnn dnnprof-ims-1//dnn profile, where ip pool and upf is selected based on location
dnn ims-lag1 network-function-list [ upf ]
dnn rmgr ims-lag1 fallback ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.
session skip-ind false
upf apn ims-lag1
qos-profile 5qi-to-dscp-mapping-table-IMS
.
.
.

profile dnn dnnprof-ims-2//dnn profile, where ip pool and upf is selected based on location
dns primary ipv4 209.165.200.225
dns primary ipv6 fd00:976a::9
dns secondary ipv4 209.165.200.226
dns secondary ipv6 fd00:976a::10
dnn ims-lag1 network-function-list [ upf ]
```

```
dnn rmgr ims-lag1 fallback ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.
profile dnn dnnprof-ims//dnn profile, where ip pool and upf selected based on location fails
 but falls back based on dnn based on precedence
dns primary ipv4 209.165.200.227
dns primary ipv6 fd00:976a::9
dns secondary ipv4 209.165.200.228
dns secondary ipv6 fd00:976a::10
dnn ims-central network-function-list [upf ]
dnn rmgr ims-central
timeout up-idle 3600 cp-idle 7320
.
.
.


config
 ipam
  instance 1
   source local
   address-pool ims-ipv6-pool1
   address-quarantine-timer 3600
    vrf-name                n6
    tags
     dnn ims-lag1//ip pool for upf-group1 and dnn profile dnnprof-ims-1
    exit
    ipv4
    address-range 1.1.1.0 1.1.10.254
    exit
    ipv6
    prefix-ranges
     split-size
      per-cache 65536
      per-dp    65536
     exit
    exit
   exit
   address-pool ims-ipv6-pool2
   address-quarantine-timer 3600
    vrf-name                n6
    tags
     dnn ims-lag2//ip pool for upf-group2 and dnn profile dnnprof-ims-2
    exit
    ipv4
    address-range 2.1.1.0 2.1.10.254
    exit
   ipv6
    prefix-ranges
    split-size
    per-cache 65536
    per-dp    65536
   exit
    prefix-range 2607:fc20:8aa0:: length 44
   exit
   exit
   address-pool ims-ipv6-pool3
   address-quarantine-timer 3600
    vrf-name                n6
    tags
    dnn ims-central//ip pool for upf-group3 and dnn profile dnnprof-ims
    exit
   ipv4
```

```
address-range 3.1.1.0 3.1.10.254
exit
ipv6
prefix-ranges
 split-size
 per-cache 65536
 per-dp    65536
exit
prefix-range 3607:fc20:8aa0:: length 44
exit
exit
exit
```

Reconciliation of IP Chunks between SMF and UPF

Feature Description

In some unforeseen scenarios, there is a possibility of mismatch between the list of DP chunks allocated at SMF and UPF. This can lead to the allocation of duplicate IPs in the network.

SMF supports reconciliation of IP chunks that allows to avoid duplicate IP allocation.

How It Works

As part of the new DP chunk allocation to UPF, the following mechanism must be followed:

1. Allocate a free DP chunk to the UPF.
2. Clear the subscribers from the node manager to CDL to free subscriber sessions matching the following criteria:
   - Newly allocated DP chunk (ipv4-startrange / ipv6-startrange as the non-unique keys for freeing the sessions).
   - Sessions created before the current system time.
3. Trigger N4 Association update with Route Deletion Request to all other UPFs serving the specific DNN, except for the UPF selected as part of the new chunk allocation.

Note All these steps must be triggered in-parallel.

4. During **clear subscriber** trigger, use the new correlation Id as CorrelationIdDpChunkAuditLocal (0xFF0D), which must be used as part of the metrics during session deletion.
5. The DNN can be Resource Manager DNN /Incoming DNN.

Note In a sunny day scenario, **clear subscriber** from the node manager to CDL should not match any sessions in CDL. Also, the N4 Association update with the Route Deletion request should not have any effect on the UPFs as they are not using this chunk or route.

Configuration to Enable or Disable Reconciliation of IP Chunks

Use following configuration to enable or disable the feature Reconciliation of IP Chunks between SMF and UPF:

```
config
   ipam
      instance gr_instance_id
         audit chunk [ local | none ]
           end
```

NOTES:

- **audit chunk** *[local | none]* —Configures audit activity on IPAM. **audit chunk** has two possible values:
  - *local* —Enables the feature.
  - *none* —Disables the feature.

  Default value is *none*.

Configuration Example

The following is an example configuration:

```
[smf] smf(config)# ipam instance 1 audit chunk
Possible completions:
  local   Enable local audit
  none    Disable audit
[smf] smf(config)# ipam instance 1 audit chunk local
```

OAM Support

This feature supports following metrics and statistics:

Bulk Statistics

Following label is added in the reasons in the existing bulk statistics **smf_disconnect_stats**:

- **dp_chunk_audit_local**—Session disconnected due to IPAM local audit.

IP Chunk Throttling

Feature Description

The SMF supports the IP chunk throttling feature to optimize IP pool utilization and manage IP address chunk allocation across multiple UPFs. This feature helps balance the load by throttling new IP chunk allocations based on UPF capacity as advertised by the UPF, or local configuration on SMF. When throttling is triggered, no new chunks are allocated, but existing chunks continue to be used until exhausted.

To determine the UPF capacity, SMF evaluates the following configurations:

- The **max-upf-sessions** command configured at the network element (UPF) level.
- The **max-upf-sessions** command configured at the vDNN level (also applicable per UPF level).
- The **load-control capacity** command configured at the user plane service level in UPF.

If all three configurations are present, the SMF compares the values and selects the lowest one to control IP chunk allocation for the UPF. However, the SMF initiates throttling checks even when the maximum number of UPF sessions is not configured in the UPF, leading to unnecessary processing overhead.

To mitigate unintended throttling checks, SMF introduces a new configuration command, **chunk-throttling false**, at the gr-instance level to explicitly disable IP chunk throttling.

How It Works

The IP chunk throttling process involves the following steps:

1. SMF supports a new proprietary IE in PFCP association setup request coming from a UPF, which carries the maximum session capacity of a UPF.

   For more information on the support of this IE from the UPF side, see the *UCC 5G UPF Configuration and Administration Guide, Release2023.03*.
2. Configure the maximum session capacity per UPF on SMF. This configuration can be applied per UPF configuration or per UPF, per DNN.
3. As part of the PFCP association, the SMF allocates IP chunk to UPF per node manager.
4. When IP usage per UPF reaches 80% of the total IP allocated, SMF attempts to allocate additional chunks. Further allocation can also occur based on internal changes, such as pool configuration modifications or pool threshold hits.
5. SMF compares the IP usage of the UPF, which includes current IP usage by active sessions and IPs in quarantine, with the maximum session capacity of the UPF.
6. SMF throttles chunk allocation if the current usage exceeds the maximum session capacity.

Limitations

Following are the known limitations of this feature:

- Throttling is not applicable when the initial chunk is allocated to each node manager instance on a UPF association.
- The split-size configuration must be less than the session limits configured in SMF/UPF. Ideally, it must be less than half considering that initial chunks are allocated to both the native node manager instances and also to the remote nodemgr instance (for GR deployment).
- In cases where the session limits are configured with lower values, the actual minimum value applicable will be in relation to the chunk size (cache-split & dp-split) configuration.

Configuring Maximum Supported Session for UPF on SMF

Following CLI configures the maximum session supported per UPF:

```
config
  profile network-element upf upf_profile_name
    max-upf-sessions max_upf_sessions_count
    n4-peer-address {  [ ipv4-address  ipv4_address ] [ ipv6-address
ipv6_address ] }
    n4-peer-port  port_number
    dnn-list dnn_list_value
    capacity lb_capacity
    priority lb_priority
    end
```

NOTES:

- **max-upf-sessions** *max_upf_sessions_count*—Maximum sessions supported for a particular UPF.

Configuration Example

Following is the sample configuration for defining the maximum supported sessions for UPF:

```
profile network-element upf upf1
 max-upf-sessions 2000
 n4-peer-address ipv4 10.1.8.48
 n4-peer-port 8805
 dnn-list     [ intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 intershat_hrt intershatipex spectrum ]
 capacity     65535
 priority     65535
exit
```

Configuring Maximum Sessions Supported Per vDNN Per UPF

SMF supports the configuration of maximum sessions supported per vDNN per UPF. Initial DNN profile selection happens based on UE DNN. SMF selects the vDNN based on the DNN RMGR configuration under the initial DNN profile. Additional DNN profiles can be configured for this vDNN and the CLI **max-upf-sessions** can be configured under this vDNN based DNN profile.

Note

- The **max-upf-sessions** can be configured under the initial DNN profile also based on the use case.
- The DNN RMGR must be configured as a DNN profile where the **max-upf-sessions** can be configured.

```
config
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | sepp | udm } profile_name
 | ipv6 ipv6_address }
    dnn  ims network-function-list [ chf | pcf | udm | upf ]
    timeout  up-idle up_idle_duration cp-idle cp_idle_duration
    charging-profile  charging_profile_name
    pcscf-profile  profile_name
    ppd-profile  profile_name
    ssc-mode  [ 1 | 2 | 3 ] allowed [ 1 | 2 | 3 ]
    session type  default_session_type
    max-upf-sessions max_upf_sessions_count
    end
```

Configuration Example

Following is the sample configuration for defining the maximum supported sessions per vDNN per UPF on SMF:

```
profile dnn dnnprof-ims
 dns primary ipv4 10.177.0.34
 dns primary ipv6 fd00:976a::9
 dns secondary ipv4 10.177.0.210
 dns secondary ipv6 fd00:976a::10
 dnn rmgr ims-pool-ipv6
 wps-profile dynamic-wps
 upf apn ims
exit

profile dnn dnnprof-ims.epdg.prod
 dns primary ipv4 10.177.0.35
 dns primary ipv6 fd00:976a::8
 dns secondary ipv4 10.177.0.211
 dns secondary ipv6 fd00:976a::11
 dnn rmgr ims-pool-ipv6
 upf apn ims.epdg.prod
exit

profile dnn ims-pool-ipv6
 network-element-profiles chf nfprf-chf1
 network-element-profiles amf nfprf-amf1
 network-element-profiles pcf nfprf-pcf1
 network-element-profiles udm nfprf-udm1
 dnn ims network-function-list [ chf pcf udm upf ]
 timeout up-idle 3600 cp-idle 7320
 charging-profile           chgprof-1
 pcscf-profile              pcscf1
 ppd-profile                ppd-prof1
 ssc-mode 1 allowed [ 2 ]
 session type IPV6
 max-upf-sessions 10000
exit
```

OAM Support

This section covers the metrics supported in this feature.

Metrics

Following new metric was introduced to capture the event when new chunk allocation is throttled:

Metric Name: IPAM_DP_chunk_allocation_throttled

Description: This metric captures the event when a new chunk allocation request is throttled for a UPF for a specific address-type and DNN. The new chunk allocation request is normally triggered on every address allocation request after hitting the upper threshold (80%) for the specific address-type and DNN.

Following labels are added in this metric:

- **grInstId:** GR Instance ID
- **upf:** UPF Key
- **addressType:** Address Type (IPv4/IPv6-PD/IPv6
- **dnn:** DNN Tag name
- **chunkAllocTrigger:** Trigger for new chunk allocation
  - **Threshold_Hit_Addr_Alloc**: Threshold hit after new address allocation.
  - **Threshold_Hit_DP_Monitoring**: Threshold hit after pool monitoring for that UPF.
  - **Insufficient_Addr_Space**: If sufficient addresses are not available during IP allocation.

Route Aggregation to Handle Switch Limit

Feature Description

For every IP chunk that SMF allocates to a UPF, the UPF publishes a route record to upstream routers for advertising the IP address subnets toward the data network. However, some of the routers have limitation with the number route records that it can allow.

It limits the number of IP chunks that SMF can allocate to a UPF and is forced to use bigger chunks (32K / 16K). But, using bigger IP chunks causes under-utilization of the allocated IP chunks, therefore, those chunks cannot be used by native instances.

SMF allows defining smaller chunk sizes and hence, limiting the number of route records that are published using some route record optimizations.

How It Works

Chunk size defining and route aggregation is done by allocating continuous IP chunks to a UPF and publishing a single or aggregated route records as per the subnet of the continuous chunk. This functionality works in the following process:

- Smaller chunk sizes, such as 4K, in consecutive fashion are defined.
- During allocation, IPAM allocates a complete group to a UPF and single route record, as per chunk group range, is sent to UPF.
- The chunk groups have 2, 4, or 8 chunks within it. This way, one group consists of 8K, 16K, or 32K size, and accordingly the route record of that size is sent to the UPF.
- Node manager instances work on the smaller IP chunks only.
- Upon an initial UPF registration, chunks for the remote node manager are also allocated from the same group.
- When the chunks start getting freed up, they return to the free pool only when all the chunks within the group are freed.
- To further optimize the routes sent to the UPF, **reserve-contiguous-groups** option can also be enabled. With this SMF upfront reserves multiple continuous chunks-groups (as per the **max-session-size** configured for the UPF/vDNN) for the UPF and push only one route record toward the UPF. The option **reserve-contiguous-groups** configuration must be enabled along with the complete address pool configuration. When enabled, the option to disable it, is not supported. If the user wishes to change the pool behavior, they must clear the subscribers associated with the pool, delete the address pool configuration, and re-configure it without the option.
- The cache-split and dp-split values must be the same when the chunk-groups are to be enabled for the address-pool. In case the dp-split and cache-split values are different then the node manager pulls more chunks.

Migration of Old Pools Without Chunk-Group into Pools with Chunk-Group

Migration of IP pools is carried-out in the following process:

1. Add new pools with chunkGroupSize configuration for the same vDNN (with IP ranges unique across the pools within the system and also the subnets for the address-ranges of the new pool must be as per standard IP-subnet). Here, **reserve-contiguous-groups** can be enabled or disabled based on the usage or planning.
2. Check if the new pools are showing from **show ipam pool** output.

   Sample config:

```
[smf-m6-cndp-rack2/data] smf# show ipam pool Mon Jul 24 08:34:36.617 UTC+00:00
================================================================================================
PoolName Ipv4Utilization Ipv6AddrUtilization Ipv6PrefixUtilization
================================================================================================
data-ipv6-pool2 92.23% 0.00% 97.66%
data-ipv6-pool1 59.42% 0.00% 34.40%
data-ipv6-pool4 0.00% 0.00% 0.00%
data-ipv6-pool3 1.70% 0.00% 1.10%
================================================================================================
[smf-m6-cndp-rack2/data] smf#
```

3. When the newly added pool is visible from **show ipam pool** output, check if the new pool is active with chunk-group-wise allocation as per chunks-per-group configuration. It can be done using the command **show ipam pool <newly added pool> ipv4-addr/ ipv6-prefix**.

   Sample config:

```
show ipam pool data-ipv6-pool4 ipv4-addr/ ipv6-prefix
```

4. Mark the old pools without chunk-group as offline. Expectation is New IPs must not be allocated from the old pool further.
5. For the ongoing traffic, chunks from the new pool will be allocated as per chunk-group configuration. It can be checked using the same CLI.

   show ipam dp <DP association> show ipam pool <new pool> ipv4-addr/ ipv6-prefix
6. As sessions associated with IPs from the old pools are terminated, they release the IPs from the old pools, and further release their chunks.
7. Wait until all the chunks from the old pools are released.

Note If there are further IPs still stuck/stale with old pools, then the subscribers can be cleared with admin-clear CLIs. For example, **show subscriber count nf-service smf dnn <dnn> show subscriber count nf-service smf ipv4-pool/ ipv6-pool <old pool>**, and **clear subscriber nf-service smf ipv4-pool/ ipv6-pool <old pool>**. Wait for all the subscribers to get cleared from the old pools with this CLI and the corresponding old routes toward the UPF must also get deleted.

8. Check if all the subscribers are moved back in the new pool with chunk-group.

   show subscriber count nf-service smf ipv4-pool/ ipv6-pool <new pool>
9. When all the subscriber move back in the new pool, delete the configuration for the old pool from IPAM.

```
[smf-m6-cndp-rack2/data] smf(config)# ipam instance 1
Mon Jul 24 08:43:19.875 UTC+00:00
[smf-m6-cndp-rack2/data] smf(config-instance-1)# no address-pool data-ipv6-pool2
```

Note It is recommended to carry-out the migration of old pools without chunk-group into pools with chunk-group in low-traffic hours/maintenance window.

Limitations

Following are the known limitations of this feature:

- Chunk Groups must be used for managing larger address pools and not for smaller address pools.
- The chunk-size (dp-split) must be 2K, 4K, 8K, and so on. It is not suitable in cases where the dp-split is less than 256.
- The values of cache-split and dp-split must be the same when chunk-groups are to be enabled for the address-pool.

Configuring IPv4 Address Range to Define Chunk Group Size

To define the small chunk-group size for IPv4 address range use the following configuration:

```
config
  ipam
    instance gr_instance_id
      address-pool pool_name
```

```
ipv4
address-range start_ipv4_address end_ipv4_address
   chunk-group chunks-per-group { 2 | 4| 8 }
   exit
```

NOTES:

- **address-range** *start_ipv4_address end_ipv4_address*—This CLI specifies the range of IPv4 address range consisting of start address and end addresses. The address range in dotted-decimal notation.

  When **chunk-group** is enabled, the number of IPs in the address range should be a power of 2, i.e., the number of IPs should be even. If the address range has odd number of IPs, it displays following error message:

  "address range from " + startAddr +" to "+ endAddr + " is odd"

Note This check is applicable only when the **chunk-group** is enabled and ony applicable for IPv4 addresses.

- **chunk-group**—This CLI configures chunk-groups for a pool.
- **chunks-per-group** *{ 2 | 4| 8 }*— This CLI defines the number of chunks in a chunk group. The values can be either 2, 4, or 8. Therefore, the chunk-group can be calculated as:

  Chunk Group= Chunk Size * 2K or 4K or 8K

Note This feature does not support or recommend the configuration of odd-numbered chunks-per-group.

Configuration Example

Following is the sample configuration for defining the chunk group size for the IPv4 address range:

```
config
ipam
 instance 1
  address-pool poolv4
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 256
     per-dp    256
    exit
    chunk-group
     chunks-per-group 4
    exit
    address-range 10.0.0.1 10.0.10.254
   exit
  exit
 exit
exit
```

Configuration Verification

Following is the output of the configuration of IPv4 address range to define chunk group size:

```
[smf] smf# show ipam pool poolv4 ipv4-addr

================================================================================================
Flag Indication: S(Static) O(Offline)
================================================================================================
StartAddress          EndAddress         AllocContext                    Flag  GroupId
================================================================================================
10.0.0.1              10.0.0.255         Free:CP                               1
10.0.1.0              10.0.1.255         Free:CP                               1
10.0.2.0              10.0.2.255         Free:CP                               1
10.0.3.0              10.0.3.255         Free:CP                               1
10.0.4.0              10.0.4.255         10.1.13.52:10.1.8.184                 2
10.0.5.0              10.0.5.255         10.1.13.52:10.1.8.184                 2
10.0.6.0              10.0.6.255         Free:CP                               2
10.0.7.0              10.0.7.255         Free:CP                               2
10.0.8.0              10.0.8.255         Free:CP                               3
10.0.9.0              10.0.9.255         Free:CP                               3
10.0.10.0             10.0.10.254        Free:CP                               3
```

Note The CLI **show ipam pool <pool-name> <ipv4-addr|ipv6-prefix|ipv6-addr>** output is updated to have an additional column *GroupId* to show the chunk Group ID. Chunks that belong to the same group reflect in the same chunk Group ID.

Configuring IPv6 Prefix Range to Define Chunk Group

Use the following configuration to define the small chunk-group size for the IPv6 address range:

```
config
   ipam
      instance instance_id
         address-pool pool_name
            ipv6
               prefix-ranges
                  prefix-range Prefix-range
                  chunk-group chunks-per-group { 2 | 4| 8 }
                  exit
```

Configuration Example

Following is the sample configuration for defining chunk group size for the IPv6 prefix range:

```
ipam
 instance 1
  address-pool poolv6
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv6
    prefix-ranges
     split-size
```

```
      per-cache 8192
      per-dp    1024
     exit
     chunk-group
      chunks-per-group 4
     exit
     prefix-range 2001:db0:: length 48
    exit
   exit
  exit
 exit
exit
```

Configuring IPv6 Address Range to Define Chunk Group

Use the following configuration to define the small chunk-group size for the IPv6 address range:

```
config
   ipam
      instance gr_instance_id
         address-pool pool_name
            vrf-name vrf_name
            ipv6
               address-range start_ipv6_address end_ipv6_address
               chunk-group chunks-per-group { 2 | 4| 8 }
               exit
```

Configuration Example

Following is the sample configuration for defining chunk group size for the IPv6 address range:

```
ipam
 instance 1
  address-pool poolv6DNN2
   vrf-name ISP
   tags
    dnn intershat1
   exit
   ipv6
    address-ranges
     split-size
      per-cache 1024
      per-dp    1024
     exit
     chunk-group
      chunks-per-group 4
     exit
     address-range 64:ff9b:: 64:ff9b::ffff:ffff
    exit
   exit
  exit
 exit
exit
```

Configuration Verification for IPv6 Prefix Range and Address Range

The configuration for IPv6 prefix range and address range can be verified using the following show command:

```
[smf-m6-cndp-rack2/data] smf# show ipam dp 100.105.64.10:10.210.184.49 ipv6-p
Tue Jul  11 12:08:36.232 UTC+00:00

=============================================================================================================
Flag  Indication: S(Static) O(Offline) R(For Remote Instance) RF(Route Sync Failed)
G:N/P Indication: G(Cluster InstId) N(Native NM InstId) P(Peer NM InstId)
=============================================================================================================
StartAddress                  EndAddress                Route                      G:N/P
Utilization   Flag      AllocContext
=============================================================================================================
2607:fb90:8700::              2607:fb90:8700:fff::      2607:fb90:8700::/52        1:0/1
100.00%                 data-ipv6-pool1(ISP)
2607:fb90:8700:1000::         2607:fb90:8700:1fff::     2607:fb90:8700:1000::/52 1:1/0
100.00%                 data-ipv6-pool1(ISP)
=============================================================================================================
```

The allocated context per chunk-group for IPv6 can be verified using the following command:

show ipam pool data-ipv6-pool2 ipv6-prefix | include (DP-Name)

A sample output/format is given here:

```
[smf-m6-cndp-rack2/data] smf# show ipam pool data-ipv6-pool2 ipv6-prefix | include
100.105.64.80:10.210.184.49
Mon Jul 17 07:43:20.510 UTC+00:00
2607:fb90:8732:400::/64 2607:fb90:8732:7ff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:800::/64 2607:fb90:8732:bff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:1000::/64 2607:fb90:8732:13ff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:1800::/64 2607:fb90:8732:1bff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:2000::/64 2607:fb90:8732:23ff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:2800::/64 2607:fb90:8732:2bff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:3000::/64 2607:fb90:8732:33ff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:3800::/64 2607:fb90:8732:3bff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:4000::/64 2607:fb90:8732:43ff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:4800::/64 2607:fb90:8732:4bff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:5000::/64 2607:fb90:8732:53ff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:5800::/64 2607:fb90:8732:5bff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:6000::/64 2607:fb90:8732:63ff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:6800::/64 2607:fb90:8732:6bff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:7000::/64 2607:fb90:8732:73ff::/64 100.105.64.80:10.210.184.49 40
2607:fb90:8732:7800::/64 2607:fb90:8732:7bff::/64 100.105.64.80:10.210.184.49 40
2607:fb90:8732::/64 2607:fb90:8732:3ff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:c00::/64 2607:fb90:8732:fff::/64 100.105.64.80:10.210.184.49 33
2607:fb90:8732:1400::/64 2607:fb90:8732:17ff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:1c00::/64 2607:fb90:8732:1fff::/64 100.105.64.80:10.210.184.49 34
2607:fb90:8732:2400::/64 2607:fb90:8732:27ff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:2c00::/64 2607:fb90:8732:2fff::/64 100.105.64.80:10.210.184.49 35
2607:fb90:8732:3400::/64 2607:fb90:8732:37ff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:3c00::/64 2607:fb90:8732:3fff::/64 100.105.64.80:10.210.184.49 36
2607:fb90:8732:4400::/64 2607:fb90:8732:47ff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:4c00::/64 2607:fb90:8732:4fff::/64 100.105.64.80:10.210.184.49 37
2607:fb90:8732:5400::/64 2607:fb90:8732:57ff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:5c00::/64 2607:fb90:8732:5fff::/64 100.105.64.80:10.210.184.49 38
2607:fb90:8732:6400::/64 2607:fb90:8732:67ff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:6c00::/64 2607:fb90:8732:6fff::/64 100.105.64.80:10.210.184.49 39
2607:fb90:8732:7400::/64 2607:fb90:8732:77ff::/64 100.105.64.80:10.210.184.49 40
```

Pre-Allocation of IP Chunks Based on Maximum Session Size

Use the following configuration to define the small chunk-group size for IPv6 address range:

```
config
  ipam
```

```
instance instance_id
   address-pool pool_name
      ipv4
         chunk-group chunks-per-group { 2 | 4| 8 }
         reserve-contiguous-groups
            exit
```

NOTES:

- **reserve-contiguous-groups**—If **reserve-contiguous-groups** is enabled and **max-upf-sessions** is configured, then IPAM will reserve the chunk-group and chunks in the power of 2 to cover the value of **max-upf-sessions**.

  For example, if the **max-upf-sessions** is 60000 and **reserve-contiguous-groups** is enabled with DP-size 8192 and **chunks-per-group** is 4, then IPAM reserves two chunk-groups in this case with 65536 (2 to the power of 16) IPs and single-route is published for this toward the UPF.

Configuration Example

Following is the sample configuration for pre-allocating multiple continuous chunks as per the max-session-size configured for the UPF/vDNN:

```
[smf] smf# show running-config ipam instance 1 address-pool poolv4
Sun Jun  18 20:00:19.226 UTC+00:00
ipam
 instance 1
  address-pool poolv4
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 256
     per-dp    256
    exit
    chunk-group
     chunks-per-group          4
     reserve-contiguous-groups
    exit
    address-range 10.0.0.1 10.0.10.254
   exit
  exit
 exit
exit
```

OAM Support

This section covers the metrics details supported in this feature.

Metrics

This feature adds a new label **groupID** in the following two metrics:

1. **IPAM_chunk_events_total**
2. **IPAM_chunk_allocations_current**

groupID: This label captures the additional information about the chunk-group ID from which the chunk is allocated/released for an UPF. Following configuration helps cature this lable:

```
config
   infra metrics verbose application metrics IPAM_chunk_allocations_current level production
 granular-labels [ groupID ]
   infra metrics verbose application metrics IPAM_chunk_events_total level production
granular-labels [ groupID ]
```

Note **groupID** is a granular label and is not enabled by default due to high cardinality for this label's value.

NAT Support

Table 305: Feature History

Feature Name	Release Information	Description
Network Address Translation Binding Updates	2023.04	SMF supports NAT Binding Record functionality where, N4 Session Report Request Message is used for providing NAT Binding Record Information from UPF to SMF. After SMF receives NAT Binding Record Information from UPF, it sends the corresponding NAT Binding Updates to the AAA Server over the RADIUS interface. **Default Setting**: Disabled – Configuration required to enable

Feature Description

Network Address Translation (NAT) is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network. This helps to save IP addresses and improve security.

When NAT is enabled on the UPF, external platforms require the real-time NAT binding updates. This allows the mapping of private IP address to public IP address used on the Gi interface to be provided to external platforms.

SMF supports NAT Binding Record functionality where, N4 Session Report Request Message is used for providing NAT Binding Record Information from UPF to SMF. After SMF receives NAT Binding Record Information from UPF, it sends the corresponding NAT Binding Updates to the AAA Server over the RADIUS interface.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > IP Address Management chapter.

How it Works

This section describes the call flows and procedures pertaining to the Network Address Translation binding updates in the SMF.

Network Address Translation Binding Updates feature supports the following functionalities:

- NAT Binding updates of Port Chunk Allocation and Release
- Session deletion with Valid NAT IP
- NAT Binding Record handling at SMF

Call Flows

The following call flow depicts sending NAT Binding Updates in the SMF.

Port Chunk Allocation

NAT Binding Updates for Port Chunk Allocation occurs when subscribers share Network Address Translation IP addresses. This is performed either at a call setup or during data flow based on the allocation mode. NBUs supports both one-to-one and many-to-one Network Address Translation IP Modes.

This section describes the call flows pertaining to the Network Address Translation binding updates for Port chunk allocation in the SMF.

Figure 173: Call Flow for Port Chunk Allocation

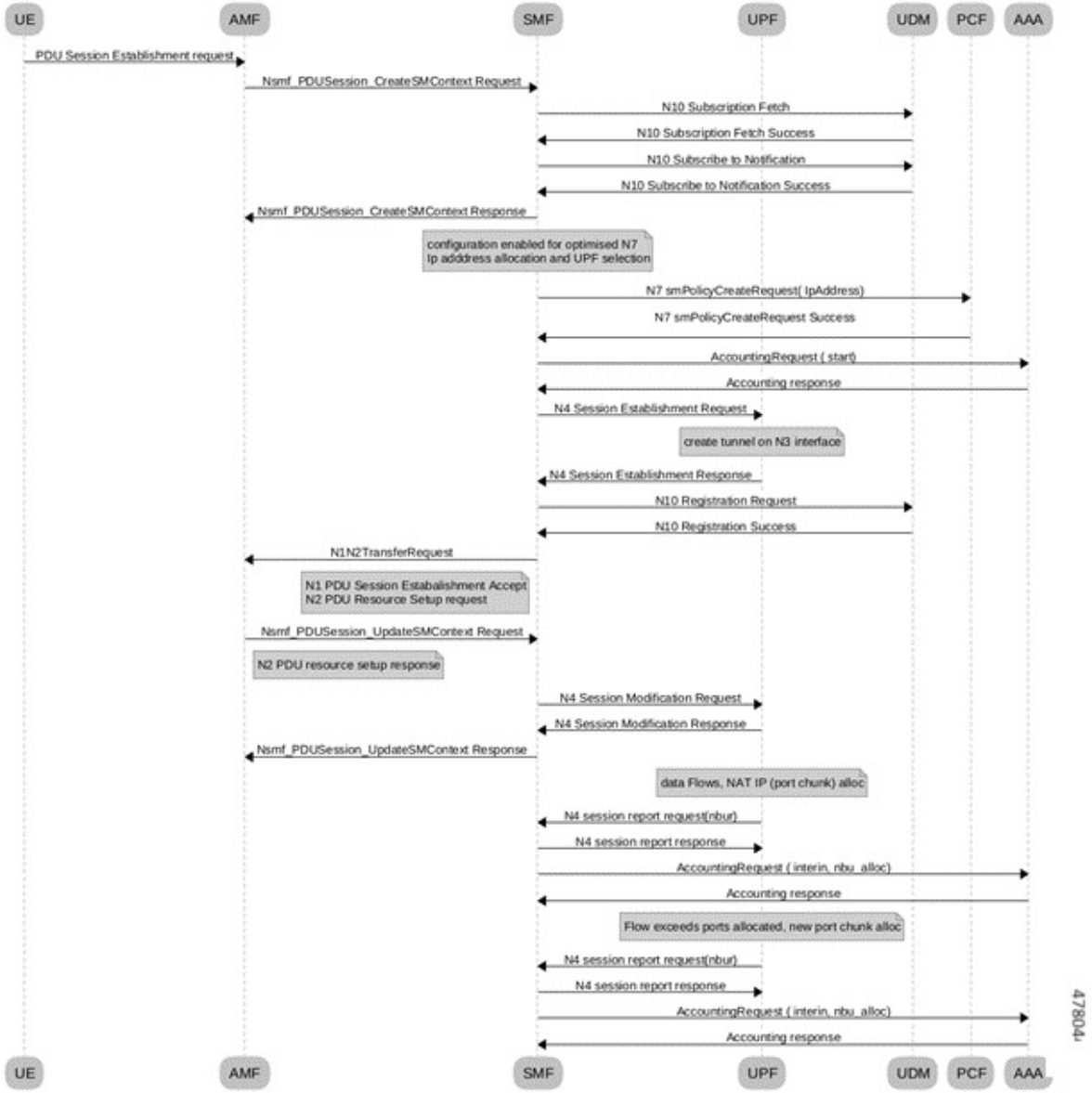


Table 306: Port Chunk Allocation Call Flow Description

Step	Description
1	During 5G session creation, RADIUS Accounting Request Start message is sent to the AAA server. .
2	When data flow happens for the subscriber, NAT IP and Port chunk gets allocated. Then UPF sends new N4 Session Report Request with NBR Information to the SMF.

Step	Description
3	SMF sends NAT Binding Update as RADIUS Accounting Request interim update to the AAA along with NAT related AVPs.
4	When number of flows crosses the already allocated ports, UPF allocates a new port chunk. Every time when Port chunk gets allocated, UPF sends a new N4 Session Report Request to the SMF and SMF in turn sends NAT Binding Update to the AAA server as RADIUS Accounting Interim update.

Port Chunk Release Procedure

This section describes the call flows pertaining to the Network Address Translation binding updates for Port chunk release in the SMF.

Figure 174: Call Flow for Port Chunk Release

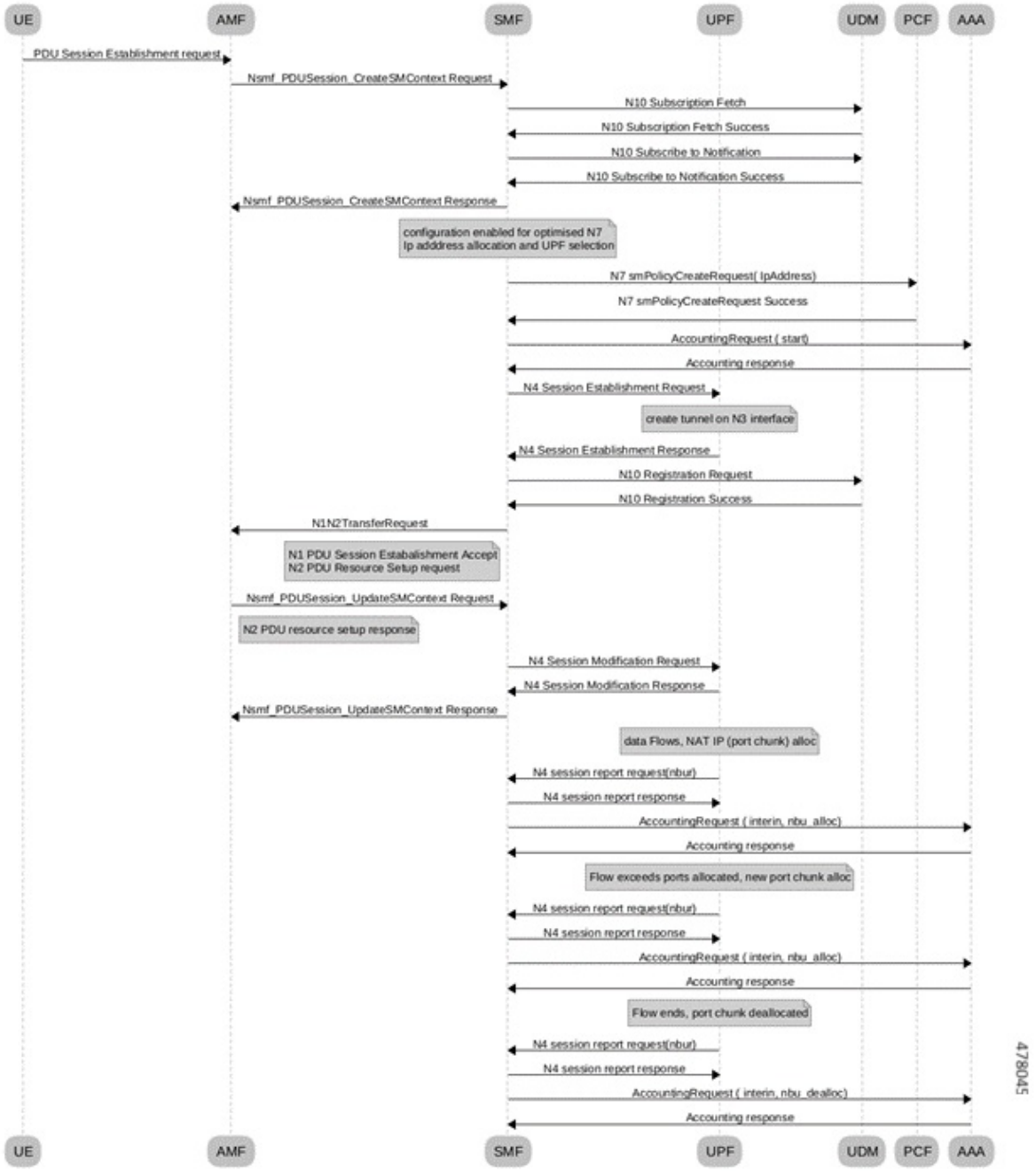


Table 307: Port Chunk Release Call Flow Description

Step	Description
1	During 5G session creation, RADIUS Accounting Request Start message is sent to the AAA server. .

Step	Description
2	When data flow happens for the subscriber, NAT IP and Port chunk gets allocated. Then UPF sends new N4 Session Report Request with NBR Information to the SMF.
3	SMF sends the NAT Binding Update as RADIUS Accounting Request interim update to the AAA server with NAT related AVPs.
4	When number of flows crosses the already allocated ports, UPF allocates a new port chunk. Every time when Port chunk gets allocated, UPF sends new N4 Session Report Request to the SMF and SMF in turn sends NAT Binding Update to the AAA server as RADIUS Accounting Interim update.
5	UPF releases the port chunk henever port chunk is not used. For each Port Chunk Release N4 Session Report Request is sent to the SMF. SMF in turn sends NAT Binding Update to the AAA server as RADIUS Accounting Interim update.
Note	Every time Port chunk gets allocated or released, NAT Binding Update is sent to the AAA server as RADIUS Accounting Interim update for Port Chunk Allocation or Port Chunk Release.

Session Deletion with Valid NAT IP

The following call flow depicts the session deletion with Valid NAT IP in the SMF.

Figure 175: Call Flow for Session Deletion

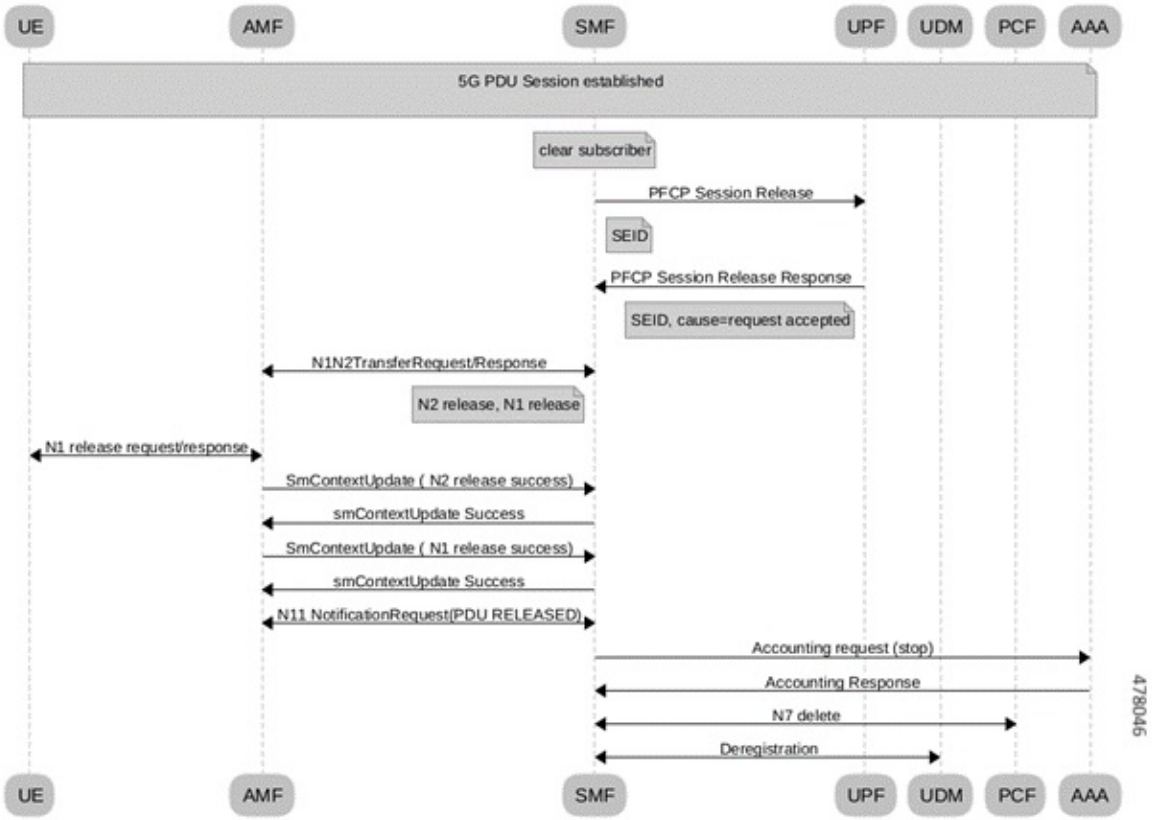


Table 308: Session Deletion Call Flow Description

Step	Description
1	During 5G session creation, RADIUS Accounting Request Start message is sent to the AAA server.
2	When data flow happens for the subscriber, NAT IP and Port chunk gets allocated. Then UPF sends new N4 Session Report Request with NBR Information to the SMF.
3	SMF sends the NAT Binding Update as RADIUS Accounting Request interim update to the AAA server.

There is no explicit messages sent to indicate Port Chunk Release, during Session Deletion Procedure. As part of Normal Session Deletion procedure, SMF sends Radius Accounting STOP message to the AAA Server. and this Radius STOP message should clear the previously sent NAT Binding Updates for Port Chunk Allocation for the Subscriber.

PFCP IEs for NAT Binding Procedure

The following tables shows IEs in PFCP Session Report Message that carries NAT Binding Information.

Table 309: Session Report Request for Nat Bind Update

InformationElements	Priority	Condition / Comment	IE Type
Report Type	M	This IE shall indicate the type of the report that is NBUR	Report Type
NBR Info	M	NBR Info IE shall carry Information for NAT Bind Updates	NBR Info

The following table describes the encoding of the Report Type IE. It indicates the type of the report the UPF function sends SMF. To send the NBR Information, the report type is set to NBUR.

Figure 176: Report Type

Octets	Bits 8	7	6	5	4	3	2	1
1–2	Type = 39 (decimal)							
3–4	Length = n							
5	Spare	UISR	SESR	TMIR	UPIR	ERIR	USAR	DLDR
6	Spare	Spare	Sparte	Spare	Spare	NBUR	SPTER	MSUR

478608

The following table describes the NBR Information grouped IE.

Figure 177: NBR Information

Octet 1 and	NBR Info IE Type = 247 (decimal)						
Octets 3 and 4	Length = n						
Information elements	**P**	**Condition / Comment**	**Appl.**				**IE Type**
			Sxa	**Sxb**	**Sxc**	**N4**	
NAT IP	M	This IE shall identify NAT IP allocated or released	-	X	-	X	NAT IP
Port Chunk Info	M	Port Chunk Info IE carries Port Chunk that is allocated or released. Several IEs within the same IE type may be present to represent a list of Port Chunks.	-	X	-	X	Port Chunk Info
Allocation Flag	M	Allocation Flag shall indicate that NBR Info is for Allocation or for Release	-	X	-	X	Allocation Flag
NAPT Number of Users Per IP	M	This IE carries Number of Users allowed to share the same NAT IP	-	X	-	X	NAPT Number of Users Per IP
Release Timer	M	Release Timer is the Release Timer configure for the realm from which NAT IP was allocated or released	-	X	-	X	Release Timer

The following table describes the encoding of the NAT IP IE.

Figure 178: NAT IP

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1–2	Type = 248 (decimal)							
3–4	Length = 4							
5–8	IPv4 IP Address Value							

The following table describes the encoding of the Port Chunk Information IE.

Figure 179: Port Chunk Information

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1–2	Type = 249 (decimal)							
3–4	Length = 4							
5–6	Start Port Value							
7–8	End Port Value							

The following table describes the encoding of the Allocation Flag IE.

Figure 180: Allocation Flag

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1–2	Type = 250 (decimal)							
3–4	Length = 1							
5	Flag							

Flag value 1 indicates the Allocation and Flag Value 0 indicates the Release.

The following table describes the encoding of the NAPT number of users per IP IE.

Figure 181: NAPT Number of Users Per IP

Octets	Bits 8	7	6	5	4	3	2	1
1–2	Type = 251 (decimal)							
3–4	Length = 2							
5–6	Number of Users Per IP values							

The following table describes the encoding of the Release Timer IE.

Figure 182: Release Timer

Octets	Bits 8	7	6	5	4	3	2	1
1–2	Type = 252 (decimal)							
3–4	Length = 2							
5–6	Release Timer Value							

The value of the release timer is in seconds.

Handling Network Address Translation Binding Record at SMF

SMF handles a Session report in a Non-State Handler process. A response is sent back immediately and an internal event is posted to handle the request.

Typically, NAT Binding Reports are considered as high priority and adding them to the Usage report procedure results in delay. This is because the Usage report procedure has lower priority compared to other procedures such as handover, modify, idle mode procedures.

To handle with appropriate priortiy, SMF handles the NIntSelfTxnN4SessRptReq for NBU as part of non-state handler. This allows messages to get handled even when other procedures are ongoing. This ensures that NAT Binding Update handling need not wait until the completion of the current procedure.

There are no changes on the Handling of regular Session Reports (non-NBU).

Note During Create and Release procedures, NAT Binding Report is not handled fully. Only the N4 Success Response is sent and the message gets ignored.

Radius AVPs for NAT Binding Procedure

NBUs are sent as part of RADIUS Accounting Interim update messages. Following new RADIUS attributes (AVPs) are sent as part of NBU messages, in addition to standard RADIUS Accounting Attributes.

- NAT-IP-Address: Network Address Translation IP Address is allocated or released to the Subscriber flow.
- NAT-Port-Block-Start: Starting Port of Port chunk that is allocated or released.
- NAT-Port-Block-End: Ending Port of the Port Chunk that is allocated or released.
- Alloc-Flag: Flag indicates that NBU is for Allocation or Release. 1 is for allocation and 0 for release.

- Loading-Factor: Number of users per IP
- Binding-Timer: Network Address Translation Binding Release Timer

Limitations

Following are the limitations:

- When a call gets cleared due to ungraceful termination, for example, battery that is drained before the IP release, Network Address Translation bind update is not performed.
- When the Network Address Translation binding updates feature is enabled, minimal performance impact to SMF might occur because of additional signaling between UPF to SMF and SMF to the AAA Server.
- As there is an extra hop (UPF to SMF update) for sending an NBU to the AAA server, some delay can occur before the NBU is sent. Hence, it is not guaranteed to achieve real-time delivery of those updates.

Configuring NAT Binding Update

Following CLI configures NAT binding updates in SMF:

```
config
  profile dnn intershat dnn_intershat
    supported-features   [ inter-plmn-ho nat-binding-update  ]
  exit
```

NOTES

- **supported-features** —List of supported features which can be enabled/disabled in SMF at DNN level. *This flag enables inter plmn roaming handover*
- **inter-plmn-ho** —Enables inter plmn roaming handover.
- **nat-binding-update** —Enables support for NAT Binding Update procedure

.

OAM Support

Bulk Statistics

The following metrics details are modified in support of NAT Binding Updates (NBU) feature.

- smf_sess_report_stats - This existing metrics includes a label sess_report_type for which a new label value sess_report_type_nbur is added. Use the metrics in handling PFCP Session Report with NBU.

  Sample Metrics:

  ```
  smf_sess_report_stats{app_name="SMF",cluster="SMF",data_center="DC",gr_instance_id="1",
  instance_id="0",rat_type="NR",reason="success",
  service_name="smf-service",sess_report_type="sess_report_type_nbur"} 3
  ```

- radius_accounting_message_stats - This existing metrics includes a new label trigger_reason and new label value nat_binding_update. Use the metrics in handling PFCP Session Report with NBU.

  Sample Metrics:

```
Attempt:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="attempted",
trigger_reason="nat_binding_update"} 3

Successful Response:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="success",
trigger_reason="nat_binding_update"} 2

Failure Response:
radius_accounting_message_stats{app_name="SMF",cluster="SMF",data_center="DC",
dnn="",gr_instance_id="1",instance_id="0",procedure_type="radius_update",
rat_type="NR",reason="",service_name="smf-service",status="failures",
trigger_reason="nat_binding_update"} 1
```

Troubleshooting Information

This section provides information on using the command line interface (CLI) commands, alerts, logs, and metrics for troubleshooting issues that may arise during system operation.

Range of IPv6 Allocated to UPF

The **show ipam dp** *dp_name* **ipv6-prefix** CLI command displays the IP pool chunks allocated to UPF. This pool chunk includes the VRF tag information and details, such as whether the pool defined is a static or dynamic pool.

[unknown] smf# show ipam dp 198.18.1.3 ipv6-prefix

```
================================================================================
Flag Indication: S(Static) O(Offline)
N/P  Indication: N(Native InstId) P(Peer InstId)
================================================================================
StartAddress          EndAddress             AllocContext       Route
N/P    Utilization   Flag
================================================================================
3001:db0::            3001:db0:0:3fff::      v6pool4(vrf4@ISP)  3001:db0::/50            -
                    S
3001:db0::            3001:db0:0:3fff::      v6pool3(vrf3@ISP)  3001:db0::/50            -
                    S
3001:db0:0:4000::     3001:db0:0:7fff::      v6pool4(vrf4@ISP)  3001:db0:0:4000::/50     -
                    S
3001:db0:0:4000::     3001:db0:0:7fff::      v6pool3(vrf3@ISP)  3001:db0:0:4000::/50     -
                    S
================================================================================
[unknown] smf#
```

Range of IPv4 Allocated to UPF

The **show ipam dp** *dp_name* **ipv4-addr** CLI command displays the IP pool chunks allocated to UPF. This pool chunk includes the VRF tag information and details, such as whether the pool defined is a static or dynamic pool.

```
[unknown] smf# show ipam dp 209.165.201.3 ipv4-addr

=============================================================================================
Flag Indication: S(Static) O(Offline)
N/P  Indication: N(Native InstId) P(Peer InstId)
=============================================================================================
StartAddress     EndAddress         AllocContext       Route              N/P   Utilization
   Flag
=============================================================================================
209.165.200.129  209.165.202.131    v4pool3(vrf3@ISP)209.165.200.129/27      -
      -S
209.165.200.129  209.165.202.131    v4pool4(vrf4@ISP)209.165.200.129/27      -
      -S
209.165.200.253  209.165.202.153    v4pool3(vrf3@ISP)209.165.200.253/27      -
      -S
209.165.200.253  209.165.202.153    v4pool4(vrf4@ISP)209.165.200.253/27      -
      -S
209.165.202.154  209.165.202.155    v4pool3(vrf3@ISP)209.165.202.154/27      -
      -S
209.165.202.154  209.165.202.155    v4pool4(vrf4@ISP)209.165.202.154/27      -
      -S
209.165.202.156  209.165.202.156    v4pool3(vrf3@ISP)209.165.202.156/27      -
      -S
209.165.202.156  209.165.202.156    v4pool4(vrf4@ISP)209.165.202.156/27      -
      -S
209.165.202.128  209.165.202.158    v4pool4(vrf4@ISP)209.165.202.128/27      -
      -S
209.165.202.129  209.165.202.158    v4pool4(vrf4@ISP)209.165.202.129/27      -
      -S
209.165.200.225  209.165.200.253    v4pool4(vrf4@ISP)209.165.200.225/27      -
      -S
209.165.201.134  209.165.201.30     v4pool4(vrf4@ISP)209.165.201.134/27      -
      -S
=============================================================================================
```

IP Pool Mapping Error Logs

The following is a sample error log for incorrect static IP to pool mapping or if static IP received from RADIUS is not found with any UPF.

```
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [DEBUG] [rmgrutil.go:501]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
response received for message NmgrRersourceMgmtResponse
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [INFO] [upmgrCacheApi.go:450]
[misc-lib.upmgrcache.gen] Cache doesnot have entry for UpfEpKey:
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [ERROR] [rmgrutil.go:73]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Both
 the associated nodemgr instances for upfEpKey:  is down
[smf-service-n0-0] *errors.errorString Both the associated nodemgr instances for upfEpKey:
  is down
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd8b29e)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/rmgrutil.go:73 (0x14dbd61)
```

Releasing N4 Resources or Association

Table 310: Feature History

Feature Name	Release Information	Description
N4 Resource or Association Release	2023.04	SMF supports clearing resources with respect to a particular UPF from the SMF using a CLI **release-resource**.

Feature Description

Whenever the network is in an erroneous state with respect to the state of IP pools, such as pool mismatch between SMF and UPF, there may be a need to clear resources like subscriber sessions or IP pools/chunks with respect to a particular UPF from the SMF.

This feature introduces a CLI that triggers and automates the resource releasing process from SMF. When the resource releasing process is triggered, SMF does the following two things:

1. It clears all the IP pools associated to the peer. This in turn clears the calls using the pool and also deletes the routes.

Note Static IP chunks will not be cleared as part of the release resource operation.

2. A new call disconnect reason is added to the SMF Disconnect Statistics. Also, the routes are re-registered with UPF post a quarantine time of 2 minutes.

Caution This feature to be executed only when the SMF is in an unhealthy state. If executed on a healthy SMF, it will impact the active subscribers as it involves clearing the calls. Please exercise with caution.

How It Works

The N4 resource or association releasing process follows the given steps:

1. Set the priority of the UPF to 0. This prevents new calls from picking up this UPF.
2. Execute the command for the N4 interface to clean up the resources.
3. Ensure to check if the calls are cleared.
4. Set the priority of UPF back.

Configuration for Releasing N4 Resources or Associations

The following configuration is used to release N4 resources or associations between SMF and UPF:

```
mode debug exec  action release-resource attributes { interface n4 peer {
 ip upf_ip } } condition { dnn matches dnn-name }
```

NOTES:

- **debug**—This keyword indicates that this is a debug mode operational CLI.
- **exec**—This command executes the command to trigger N4 release per UPF from SMF.
- **action** —This command indicates the action to perform.
- **release-resource**—Upon executing **release-resource**, the SMF triggers clean-up of subscriber/pool resources to the peer provided.
- **attributes**—This command defines the attributes to perform an action.
- **peer**—The UPF peer can be defined using the UPF IP address.
- **interface** —This command specifies the interface name to trigger the operation for.
- **condition**—This CLI specifies the additional condition to filter the data for the selected operation. This is an optional filter.
- **dnn**—Pools associated to this dnn-name will be cleared based on the given operator. The DNN name for which the IP pools are assigned, has to be used here.
- **matches**—This command verifies the DNN that matches the output modifiers.

Configuration Example

Following is the sample configuration for releasing the N4 resources or associations:

```
mode debug exec action release-resource attributes { interface n4 peer { ip <upf_ip> } }
condition { dnn matches dnn1 }
```

Configuration Verification

Following command verifies the configuration for releasing the N4 resources and associations per UPF and SMF:

```
[smf] smf# show ipam pool poolv4 ipv4-addr
Wed Aug  23 07:04:48.511 UTC+00:00

================================================================================
Flag Indication: S(Static) O(Offline)
================================================================================
StartAddress          EndAddress         AllocContext                  Flag  GroupId
================================================================================
209.165.200.225       209.165.200.231    QT:NM1
209.165.200.232       209.165.200.239    Free:CP
209.165.200.240       209.165.200.247    Free:CP
209.165.200.248       209.165.200.254    Free:NM1
================================================================================
```

OAM Support

This section details the metrics supported in this feature.

Metrics

Following reason is added in the **smf_disconnect_stats** counter:

disc_rel_upf_admin_clear: The session terminates as the IP chunk is cleared for a particular UPF triggered by the admin.

Identification of Corrupted IP Chunks

Feature Description

SMF allows identifying the missing or corrupted IP chunks by auditing the configured IP pools and their data in cache-pod and IPAM internal states.

Note Please contact your Cisco Account or support representative for any questions about configuring SMF to identify the missing or corrpupted IP chunks.

How It Works

SMF can capture the debug information that can check for any corruption in IPAM data due to following scenario:

- The chunk entry is missing from the IPAM cache-pod data.
- The chunk entry is present, but has some missing essential non-unique-keys, such as pool-name, address-type, gr-instance-id, and so on.
- The chunk is showing as allocated (locked) in the cache-pod, but it is not allocated by the node manager to any UPF.
- The chunk is showing as free in the cache-pod, but the node manager has allocated the IP chunk to a UPF (DP).

OAM Support

This section discusses the metrics and statistics supported in this feature.

Bulk Statistics

Following metric is supported under the new category **SMF IPAM Pool Total Chunks Counter Category**:

IPAM_pool_total_chunks: It captures the total number of chunks for the pool.

- **Metrics-Type**: Gauge

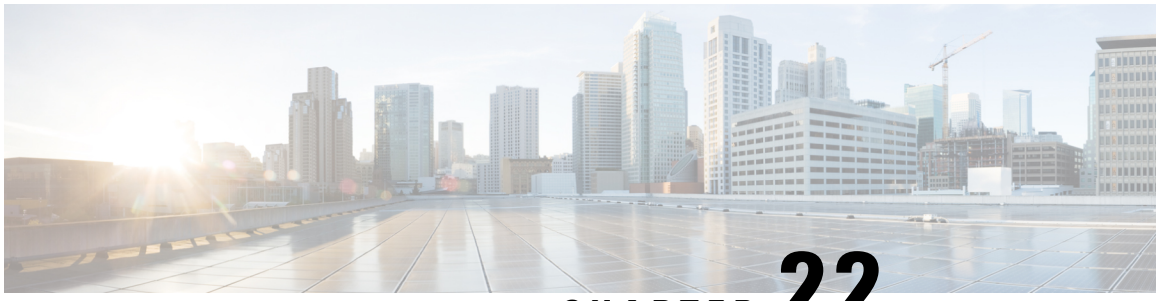
Following labels are supported as part of this metric:

- **grInstId**: GR Instance ID
- **pool**: Address pool name
- **addressType**: Address-Type (ipv4/ipv6)
- **IPAM_Chunk_Alloc_Type**: Chunk allocation status

  It has the following possible values:

  - **FreeCP**: Chunks free in cache-pod
  - **FreeNM**: Chunks free with node manager instance
  - **AllocatedUPF**: Chunk allocated to UPF

Note The parameter FreeCP label captures the total number of free chunks available in the cache-pod. As this value is common to the node manager instances, it is captured only by one of the node manager instances (leader). This way the Grafana sum query shows the correct total chunk count.



CHAPTER 22

IPv6 PDU Sessions

- Feature Summary and Revision History, on page 815
- Feature Description, on page 816
- Configuring Router Solicit and Router Advertisement, on page 817

Feature Summary and Revision History

Summary Data

Table 311: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 312: Revision History

Revision Details	Release
Added permissible range values for the following commands in ICMPv6 Profile configuration options. • **mtu** • **reachable-time** • **retrans-timer**	2021.02.1
First introduced.	Pre-2020.02.0

Feature Description

SMF supports ICMPv6 Router Solicit and Advertisement to comply to IPv6 Stateless Auto-configuration.

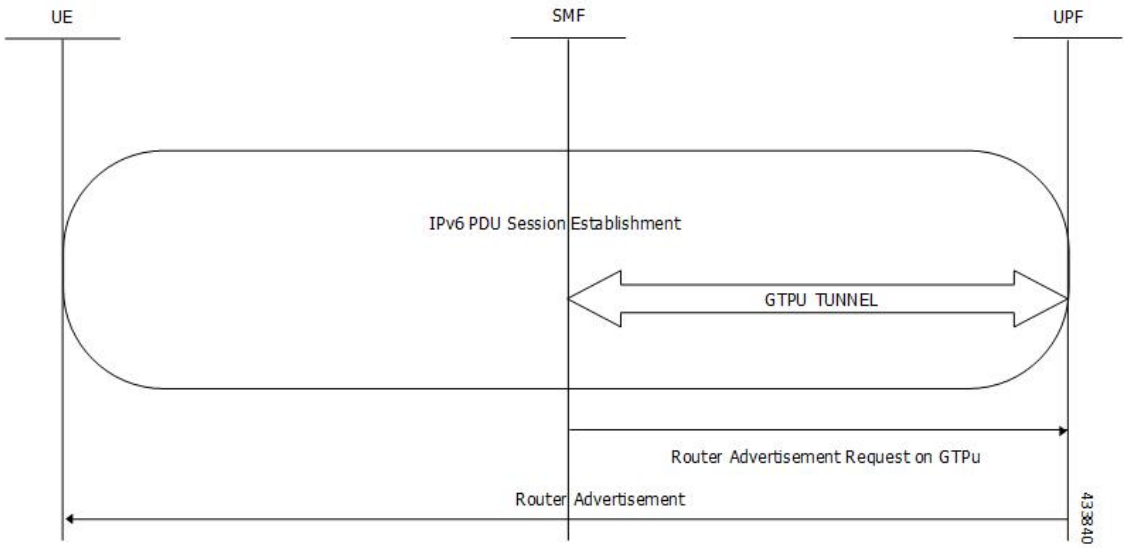
Router Advertisement supports the following ICMPv6 options:

- Prefix Information—Sends the allocated UE IPv6 prefix.
- MTU—Takes the MTU size from the configuration. Default is 1500.
- Source Link Layer Address—Takes the value from the configured local virtual MAC.

Unsolicited Router Advertisement

The SMF sends unsolicited router advertisement on successful PDU Session Establishment to share the allocated IPv6 prefix to UE. RA message is sent over the GTPU tunnel, which is created between SMF and UPF during the session establishment procedure. SMF also installs PDRs and FARs on the UPF to enable routing for RS and RA messages.

Figure 183: Router Advertisement Message Processing Call Flow

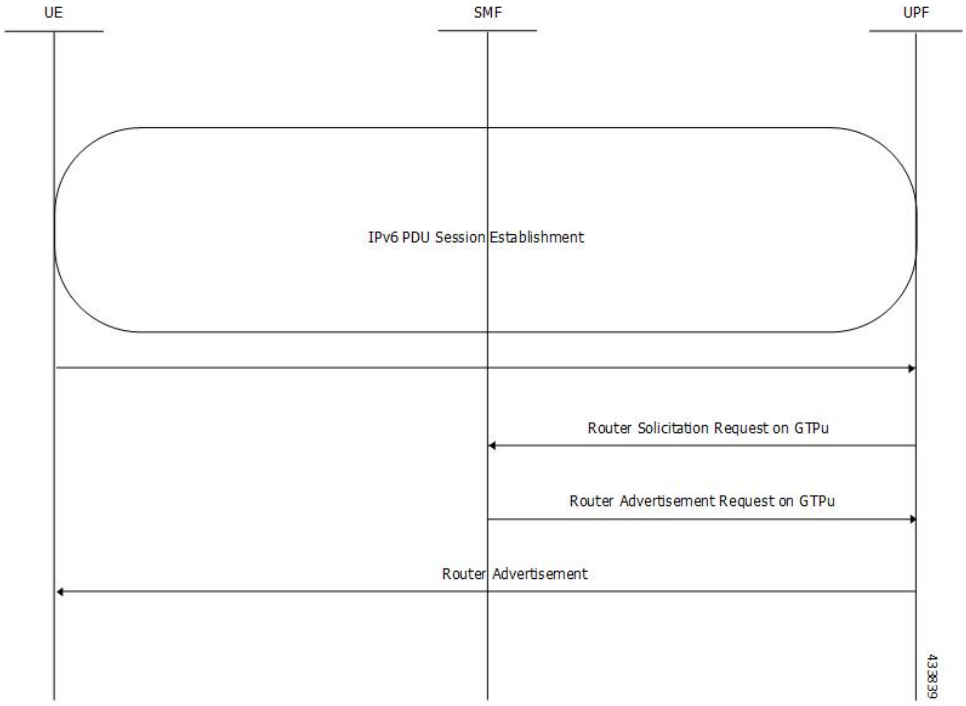


Note The UPF cannot generate or send the unsolicited router advertisement to the UE as the IPv6 prefix allocation is performed by SMF.

Solicited Router Advertisement

To get the allocated IPv6 prefix, UE sends a router solicit message. Upon receiving the router solicit message, SMF sends the router advertisement message containing the allocated UE IPv6 prefix towards UE.

Figure 184: Router Solicitation and Advertisement Message Processing Call Flow



Configuring Router Solicit and Router Advertisement

This section describes how to configure the Router Solicit and Router Advertisement feature.

Configuring the Router Solicit and Router Advertisement feature involves the following:

- Configuring Router Advertisement Parameters, on page 817
- Configuring Virtual MAC Address, on page 818
- Associating the ICMPv6 Profile with SMF Service Profile, on page 819

Configuring Router Advertisement Parameters

To configure the Router Advertisement parameters, use the following sample configuration:

```
config
  profile icmpv6 icmpv6profile_name
    options { hop-limit hop_limit | mtu mtu_size | reachable-time reachable_time
 | retrans-timer retrans_timer | router-lifetime router_lifetime | virtual-mac
 virtual_mac }
    ra trigger handover { false | true }
    end
```

NOTES:

- **profile icmpv6** *icmpv6profile_name*: Specify the ICMPv6 profile name. *icmpv6profile_name* must be an alphanumeric string.
- **options { hop-limit** *hop_limit* **| mtu** *mtu_size* **| reachable-time** *reachable_time* **| retrans-timer** *retrans_timer* **| router-lifetime** *router_lifetime* **| virtual-mac** *virtual_mac* **}**: Configure the ICMPv6 options.
  - **hop-limit** *hop_limit*: Configure the hop limit. *hop_limit* must be an integer in the range of 0–255. Default: 255.
  - **mtu** *mtu_size*: Configure the MTU size. Default: 1500.

    mtu_size must be an integer in the range of 1280-1500.
  - **reachable-time** *reachable_time*: Configure the reachable time in milliseconds. Default: 0.

    reachable_time must be an integer in the range of 0-3600.
  - **retrans-timer** *retrans_timer*: Configure the retransmission timer in milliseconds. Default: 0.

    retrans_timer must be an integer in the range of 0-4294968.
  - **router-lifetime** *router_lifetime*: Configure the router lifetime in seconds. *router_lifetime* must be an integer in the range of 0–65535. Default: 65535.
  - **virtual-mac** *virtual_mac*: Configure the local virtual MAC address.
- **ra trigger handover { false | true }**: Configure the trigger to send router advertisements for Wi-Fi handovers.

Verifying the Configuration

Use the **show running-config profile icmpv6** command to verify the Router Advertisement configuration.

The following configuration is an example output of the command:

```
[unknown] smf(config)# show running-config profile icmpv6
profile icmpv6 icmpprf1
 options hop-limit 255
 options mtu   1500
 options reachable-time 0
 options retrans-timer 0
 options router-lifetime 65535
 options virtual-mac b6:6d:57:45:45:45
 ra trigger handover true
exit
```

Configuring Virtual MAC Address

To configure the remote virtual MAC address in the DNN profile, use the following sample configuration:

```
config
  profile dnn dnnprofile_name
    virtual-mac mac_address
    exit
```

NOTES:

- **profile dnn** *dnnprofile_name*: Specify the DNN profile name. *dnnprofile_name* must be an alphanumeric string.
- **virtual-mac** *mac_address*: Specify the remote virtual MAC address used to generate interface ID for UE. *mac_address* must be a string in the MAC address pattern.

In release 2021.01 and later, the SMF generates unique 64-bit interface ID which is non-EUI-64 format by using SBI VIP address and CommonId of the subscriber.

That is, IPv6 interface ID = VIP-IP (4 bytes) + CommonId (4 bytes)

By default, **virtual-mac** CLI command is now disabled under DNN configuration.

Table 313: Interface ID for Different Messages

Call Model	PDU Session Establishment Accept	Create Session Response
5G	N11-SBI-VIP+CommonID	—
4G	—	GTP-VIP+CommonID
WiFi	—	GTP-VIP+CommonID
5G->4G	—	—(N26 HO - there are NAS contents during handover)
4G->5G	— (N26 HO - there are NAS contents during handover)	—
4G->WiFi	—	GTP-VIP+CommonID (Same as 4G)
WiFi->4G	—	GTP-VIP+CommonID (Same as 4G)
5G->WiFi	—	N11-SBI-VIP+CommonID (Same as 5G)
WiFi->5G	GTP-VIP+CommonID (Same as WiFi)	—

Associating the ICMPv6 Profile with SMF Service Profile

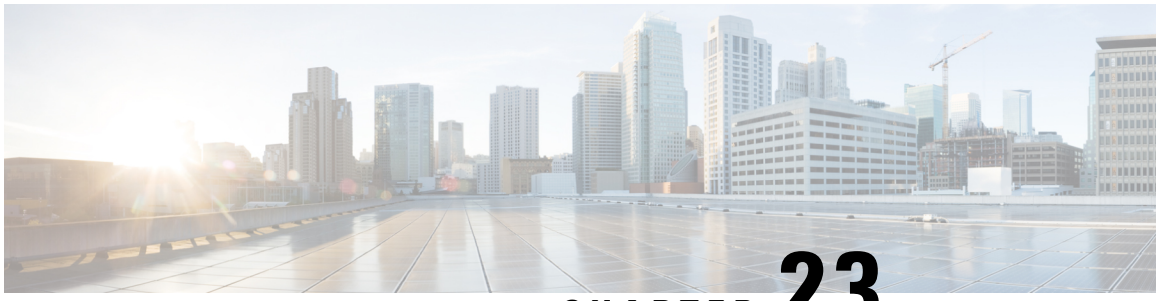
To associate the ICMPv6 profile with the SMF service profile, use the following sample configuration:

```
config
  profile smf smfprofile_name
    service name svc_name
      icmpv6-profile icmpv6profile_name
      exit
```

NOTES:

- **profile smf** *smfprofile_name*: Specify the SMF service profile name. *smfprofile_name* must be an alphanumeric string.

- **service name** *svc_name*: Specify the name of the SMF network function service. *svc_name* must be an alphanumeric string.
- **icmpv6-profile** *icmpv6profile_name*: Specify the load profile name to associate with the SMF service profile. *icmpv6profile_name* must be an alphanumeric string.



CHAPTER 23

MBR Short Circuit Optimization

- Feature Summary and Revision History, on page 821
- Feature Description, on page 821
- How it Works, on page 822
- Limitations, on page 822
- MBR Short Circuit Optimization Support, on page 823

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 314: Revision History

Revision Details	Release
First introduced.	2021.02.x

Feature Description

Generating the Modify Bearer Response message at gtpc-ep pod is called MBR short circuit. SMF now generates Modify Bearer Response messages at gtpc-ep pod to limit the impact of processing Modify Bearer

Request sending Modify Bearer Response message (Modify Bearer Response) with success cause at the smf-service pods. The Modify Bearer Response messages are generated at gtpc-ep pod.

How it Works

Important The CEPS optimization with GTPv2 CEPs works only with System mode shutdown and restart. It is not recommended to use this with Rolling Software Update as it may lead to system inconsistency.

Cache

At the udp-proxy pod, a cache is maintained. This cache contains entries corresponding to sessions that require GTP protocol for interaction with other nodes in network. Each cache entry is mapped to TEID assigned to the corresponding session by SMF. The cache entry contains details remote session TEID, EBI, TEID allocated by SMF and last sequence number.

There is a limit on the number of cache entries that can be added in the cache. The limit is around a million cache entries. Stale(cache entries that are not used for an hour) cache entries are periodically removed from the cache.

Short Circuit

On receiving an incoming UDP packet, SMF identifies if the message is a request message. It lookups the cache to see if there is corresponding cache entry present.

If the cache entry is present and the request is MBR and if it short circuited, then MBR response is generated without full processing.

The conditions for short circuiting MBR are as follows:

- MBR comprising of only Serving Network IE
- MBR comprising of Serving Network IE and Bearer Context with EBI only
- MBR comprising of Serving Network IE and Indication IE with other than HO (Handover) bit set

Limitations

MBR Short Circuit feature has the following limitations:

- For WiFi Session, SMF doesn’t create cache entry.
- For 4G to 5G HO, SMF is unable to clean up the Cache-Entry and leave a stale entry, then the entry is deleted automatically after cache-entry timeout.
- SMF supports maximum of one million entries and maximum of 60 min cache-entry timeout. Cache entry is removed if there are no access to it.

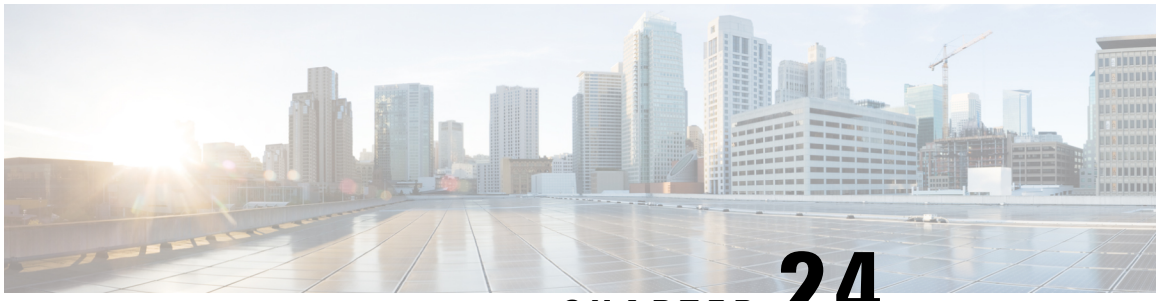
MBR Short Circuit Optimization Support

This section describes the operations, administration, and maintenance information for this feature.

Statistics

Following statistics support MBR Short Circuit feature:

- gtpc_msg_short_circuit_stats - Captures number of messages short circuited. Displays if the message is skipped or short circuited along with the condition that message was short circuited.
- gtpc_short_circuit_map_count – Captures number of entries added/deleted/updated in the cache. Displays addition entries from the deleted entries and the update entries separately.
- smf_service_gtpc_cache_stats – Captures number of cache-entries sent from Smf-Service with operations added/deleted. Displays each cache-entry with procedure-type, message-type, operation (added/deleted).



CHAPTER 24

Mesh Connectivity to All UPFs

- Feature Summary and Revision History, on page 825
- Feature Description, on page 825

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 315: Revision History

Revision Details	Release
First introduced.	2021.02.1

Feature Description

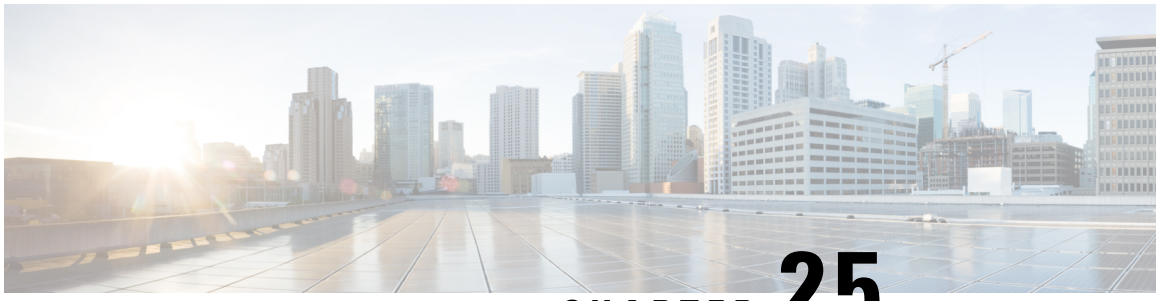
With release 2021.02.01, SMF Mesh connectivity to all UPFs in a region is introduced.

Mesh connectivity enables UPF to connect to all SMFs in particular region. Subscriber however will be hosted on only one UPF. All UPFs in the region should be connected to all the SMF in the region.

Ideally SMF can be connected to maximum of 1024 UPFs. UPF can support up to maximum of four Peers(SMF/SGWC/CN-SGW).

Important Mesh connectivity support is prerequisite for Geographic redundancy support feature on the SMF.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Mesh Connectivity to All UPFs chapter.



CHAPTER 25

MTU Support in PCO

- Feature Summary and Revision History, on page 827
- Feature Description, on page 827
- Configuring IPv4 Link MTU, on page 828

Feature Summary and Revision History

Summary Data

Table 316: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 317: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

This feature allows sending a Maximum Transmission Unit (MTU) value to a subscriber device for modification in settings and performing tasks, such as avoiding fragmentation and blocked traffic. If UE requests, configuration links MTU in Protocol Configuration Options (PCO) IE. When CSR comes with PCO requesting

IPv4 link MTU, SMF sends create session response with PCO containing link MTU configured under network-capability policy. When N1 PDU session establishment request includes PCO requesting IPv4 link MTU, SMF sends N1 PDU session establishment response with PCO containing link MTU configured under network-capability policy.

If CSR comes with PCO, EPCO, or APCO requesting MTU, SMF sends the configured IPv4 MTU in CSR response, if the network-capability policy is associated to the operator policy.

If 5G PDU session establishment request is received with PCO requesting MTU, SMF sends the configured IPv4 MTU in PDU session establishment accept, if network-capability policy is associated to the operator policy.

If the PGW-C decides to return Extended Protocol Configuration Options (ePCO) to the UE during an Initial Attach, UE-requested PDN Connectivity procedure initiates. If the PGW-C supports the ePCO and the EPCOSI flag is set to 1 in the Create Session Request message, the PGW-C sends ePCO to the S-GW. If the S-GW receives the ePCO IE, the S-GW forwards it to the MME.

In roaming scenarios, the vSMF decodes the input N1 message, fills and encodes the n1SmInfoFromUE IE with the N1 message in a PDU session create or update request. Similarly, if the hSMF receives the ePCO with a request for MTU and the policy network-capability is configured with a link MTU value, it sends the link MTU value in the n1SmInfoToUE IE. Otherwise, the hSMF sends the default MTU value, which is 1500.

If it's a network-initiated session modification and the session was established with an ePCO, the hSMF includes the ePCO in the session update request.

Configuring IPv4 Link MTU

This section describes how to configure the MTU to be included in PCO IE sent to the UE.

To configure the IPv4 MTU, use the following sample configuration:

```
config
   policy network-capability network_capability_name
      link-mtu link_mtu_range
      end
```

NOTES:

- **link-mtu** *link_mtu_range* : Configure network capability policy to include link MTU in PCO IE, if it is requested by UE.

  link_mtu_range must be an integer in the range of 1280-2000. The default value is 1500 bytes.

Configuration Verification

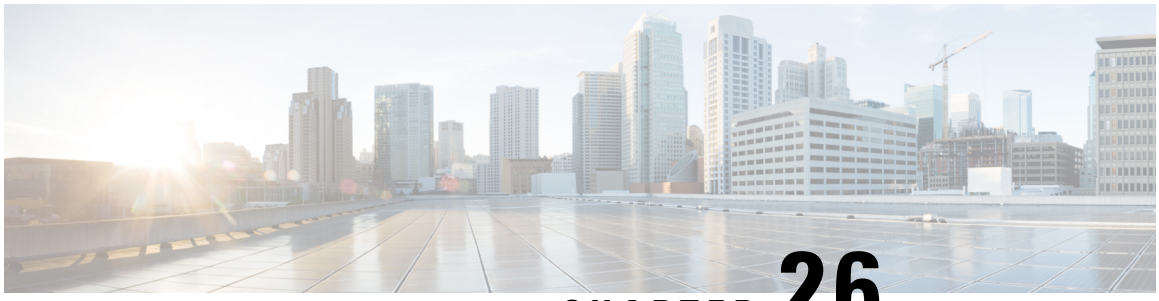
To verify the configuration, use the following show command:

```
show running-config policy network-capability
```

If the IPv4 MTU is configured, then the value appears as part of the **link-mtu** configuration in the following output.

```
[unknown] smf# show running-config policy network-capability
policy network-capability nc1
 link-mtu 1500
 max-supported-pkt-filter 20
```

```
 nw-support-local-address-tft true
exit
```



CHAPTER 26

DNN Support

- Feature Summary and Revision History, on page 831
- Feature Description, on page 832
- How It Works, on page 833
- Configuring Virtual DNN, on page 834
- Network Function Selection based on SMF Instances, on page 839
- Switching DNN Profile to Offline Mode During Dynamic Config Update, on page 841
- DNN Inheritance, on page 844
- IP Pool Allocation per DNN, on page 849
- IP Pool Allocation per Slice and DNN, on page 851

Feature Summary and Revision History

Summary Data

Table 318: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 319: Revision History

Revision Details	Release
Added dynamic configuration change support for DNN profile.	2023.03.0

Revision Details	Release
Added override keyword in the CLI to support virtual DNN from RADIUS server.	2023.02.0
Added support for IP pool allocation per slice and DNN.	2022.04.0
Added support for: • Charging Characteristics lookup parameter in the subscriber policy configuration. • Extension in Charging Characteristics ID range values.	2021.02.3.t3
Added support for IPv6 interface ID generation based on SBI VIP address and CommonId of the subscriber.	2021.01.1
SMF supports the maximum limit of 2048 for the following configurations: • Precedence • Operator policy • DNN policy • DNN profile	2021.01.0
SMF supports case insensitive DNN configuration.	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The multi-DNN support enables the SMF to have multiple PDN connections for end users to provide different services including Internet and VoNR services.

The SMF fetches the locally configured profile-based Data Network Name (DNN) in PDU Session Establishment Request from the AMF. Then, the SMF maintains the PDN connections based on using SUPI and PDU Session ID. The SMF includes the received DNN in all SBI interfaces to authorize the end user to fetch subscription information, policy, and charging related information. The SMF provisions the forward path information to the UPF. The SMF integrates the multi-DNN support with the IP Address Management (IPAM) module to allocate address to the end user based on received DNN. The SMF maps the DNN profile that is derived from subscriber policies. The SMF also fetches DNN and IPv4 and IPv6 path information based on IPAM pool configuration and updates the UPF as part of node association interactions.

Note Multiple DNN is supported only for 5GS procedures and is not qualified for EPS Session using SBI interfaces.

The SMF supports virtual DNN (vDNN) mapping based on a subscriber profile. It supports mapping of a UE-requested DNN to a configured DNN and sends the selected DNN profile towards the configured network interfaces.

For 5G subscribers, SMF allows a higher number of vDNNs with slice-based vDNN selection. However, when 5G subscribers connect from 4G access network, the slice information is unavailable until SMF fetches the UE subscription data from UDM. In such scenarios, SMF performs initial vDNN selection based on the CC lookup parameter. After the subscription data is fetched, the SMF reselects the vDNN based on the slice ID information and uses the new vDNN profile. This approach remains the same for the Wi-Fi calls as well.

SMF provides the flexibility of vDNN selection based on using either Charging Characteristics or slice through the CLI configuration. For more information on the configuration part, see the Configuring Subscriber Policy, on page 834 section.

Note As the DNN profile is under the operator policy, the reselection of the vDNN profile implies the reselection of the operator policy as well. SMF supports the configuration so that the reselection doesn't impact the existing features that are associated to other parameters in the operator policy.

How It Works

The DNN profile lookup is based on subscriber policy or DNN policy. You can associate these policies in the SMF profile configuration. The subscriber policy has a higher precedence over the DNN policy when both the configurations are available.

The subscriber policy consists of a list of precedence values. The selection of precedence is based on various values. For example, the subscriber SUPI, GPSI, Serving PLMN, NSSAI, Charging Characteristics, and IMSI. Each precedence has an associated operator policy and the DNN policy is chosen from the selected operator policy.

The DNN policy can have a DNN profile configuration for each UE-requested DNN. The DNN profile has a Virtual or Mapped DNN with its list of interfaces.

The order of selection for a Virtual DNN is as follows:

- Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.
- Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.

PCF, CHF, UDM, UPF, and Resource Manager (RMGR) are the supported interfaces for Virtual DNN mapping.

If the Virtual DNN mapping is not configured, the UE-requested DNN is used across all the interfaces.

Limitations

This feature has the following limitation:

- The SMF includes first-configured DNN profile in "dnnSmfInfoList" of NFProfile during registration with NRF.

Configuring Virtual DNN

This section describes how to configure the Virtual DNN feature.

Configuring the Virtual DNN feature involves the following steps:

1. Configuring Subscriber Policy, on page 834
2. Configuring Operator Policy and Associating a DNN Policy, on page 836
3. Configuring a DNN Policy, on page 837
4. Configuring a Virtual DNN under a DNN Profile, on page 837
5. Associating Subscriber Policy under the SMF Service, on page 838

Configuring Subscriber Policy

To configure the subscriber policy, use the following sample configuration:

```
config
   policy subscriber subscriber_policy_name
      precedence precedence_value
         cc-start-range cc_start_range_value
         cc-stop-range cc_stop_range_value
         gpsi-start-range gpsi_start_range_value
         gpsi-stop-range gpsi_stop_range_value
         imsi { mcc mcc_value | mnc mnc_value | msin  msin_value }
         imsi-start-range imsi_start_value
         imsi-stop-range imsi_stop_value
         operator-policy operator_policy_name
         pei-start-range pei_start_range_value
         pei-stop-range pei_stop_range_value
         sdt sdt_value
         serving-plmn { mcc mcc_value | mnc mnc_value | mnc-list  mnc_list_value
 }
         serving-plmn  serving_plmn_value
         sst sst_value
         supi-start-range supi_start_range_value
         supi-stop-range supi_stop_range_value
         instance-start-range start_range_value
         instance-stop-range stop_range_value
         end
```

NOTES:

- **precedence** *precedence_value*: Specify the precedence value associated with the subscriber policy.

  The maximum limit for precedence is 2048.

- **cc-start-range** *cc_start_range_value*: Specify the charging characteristics start range value associated with the subscriber policy. *cc_start_range_value* must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 0001.

- **cc-stop-range** *cc_stop_range_value*: Specify the charging characteristics end range value associated with the subscriber policy. *cc_stop_range_value* must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 12AB.

- **gpsi-start-range** *gpsi_start_range_value*: Specify the GPSI start range value to be associated with the subscriber policy. *gpsi_start_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **gpsi-stop-range** *gpsi_stop_range_value*: Specify the GPSI stop range value to be associated with the subscriber policy. *gpsi_stop_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **imsi { mcc** *mcc_value* **| mnc** *mnc_value* **| msin** *msin_value***}**: Specify the IMSI value by providing the MCC, MNC, or MSIN value that is to be associated with the subscriber policy.

- **imsi-start-range** *imsi_start_value*: Specify the IMSI start range value. *imsi_start_value* must be an integer in the range from 1000000000 through 999999999999999.

- **imsi-stop-range** *imsi_stop_value*: Specify the IMSI stop range value. *imsi_stop_value* must be an integer in the range from 1000000000 through 999999999999999.

- **operator-policy** *operator_policy_name*: Specify the operator policy to be associated with the subscriber policy.

  The maximum limit for operator policy is 2048.

- **pei-start-range** *pei_start_range_value*: Specify the PEI start range value. *pei_start_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **pei-stop-range** *pei_stop_range_value*: Specify the PEI stop range value. *pei_stop_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **sdt** *sdt_value*: Specify the SDT value be associated with the subscriber policy. *sdt_value* must be a 6-digit octet string in the [0-9a-fA-F]{6} - 000000 - ffffff format. For example, 1A2B3c.

- **serving-plmn { mcc** *mcc_value* **mnc** *mnc_value* **mnc-list** *mnc_list_values***}** : Specify the 3-digit Mobile Country Code (MCC), 2- or 3-digit Mobile Network Code (MNC), or the list of MNC values of the serving PLMN. *mcc_value* and *mnc_value* must be a string. *mnc_list_values* must be a string, such as [580 660].

- **sst** *sst_value*: Specify the Slice/Service Type (SST) value. *sst_value* must be a 2-digit octet string in the [0-9a-fA-F]{2} - 00 to FF format. For example, A8.

- **supi-start-range** *supi_start_range_value*: Specify the SUPI start range value. *supi_start_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **supi-stop-range** *supi_stop_range_value*: Specify the SUPI stop range value. *supi_stop_range_value* must be an integer in the range from 1000000000 through 999999999999999.

- **instance-start-range** *start_range_value*: Specify the SMF instance start range value. *start_range_value* must be an integer in the range from 1 to 8.
- **instance-stop-range** *stop_range_value*: Specify the SMF instance stop range value. *stop_range_value* must be an integer in the range from 1 to 8.

Configuration Verification

To verify the policy-related configuration details, use one of the following commands:

show subscriber policy *policy_name* or **show full** in the policy configuration mode.

The following is an example output of the show command:

If the subscriber policy configuration includes the charging characteristics parameter, then the value appears as part of **cc-start-range** and **cc-stop-range** in the following output.

```
smf(config-subscriber-polSub)# show full
policy smf polSmf
precedence 1
  sst              22
  sdt              232322
  serving-plmn mcc 210
  serving-plmn mnc 90
  supi-start-range 100000000000001
  supi-stop-range  100000000000010
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  cc-start-range 0001
  cc-stop-range 0005
  operator-policy  opPol1
!
!
```

Configuring Operator Policy and Associating a DNN Policy

To configure the operator policy, use the following sample configuration:

```
config
   policy operator operator_policy_name
      policy dnn dnn_policy_name [ [ secondary secondary_dnn_policy_name ] [
network-capability network_capability ] ]
      end
```

NOTES:

- **policy dnn** *dnn_policy_name* **[[secondary** *secondary_dnn_policy_name* **] [network-capability** *network_capability***]]** : Specify the parameters of primary DNN policy to be associated with the operator policy. *dnn_policy_name* must be a string.
  - **secondary** *secondary_dnn_policy_name*: If the parameters of DNN policy to be associated with the operator policy don't match with the primary policy, specify the secondary DNN policy for fallback. *secondary_dnn_policy_name* must be a string.
  - **network-capability** *network_capability*: Specify the network capability configuration details for the respective operator policy that you have selected. The *network_capability* value must be a string.

Configuring a DNN Policy

To configure the DNN policy, use the following configuration:

```
config
   policy dnn dnn_policy_name
      dnn dnn_name profile dnn_profile_name dnn-list dnn_list
   exit
exit
```

NOTES:

- **policy dnn** *dnn_policy_name*: Specify the DNN policy. *dnn_policy_name* must be an alphanumeric string.

  The maximum limit for DNN policy is 2048.

- **dnn** *dnn_name*: Specify the virtual DNN profile to map with the specified network DNN profile. *dnn_name* must be an alphanumeric string.

  The DNN configuration accepts an alphanumeric string from 1 through 62 alphanumeric characters, that is case insensitive. It can also contain dots (.) and/or dashes (-).

- **profile** *dnn_profile_name*: Specify the network DNN profile. *dnn_profile_name* must be an alphanumeric string.

  The maximum limit for DNN profile is increased from 512 to 2048.

- **dnn-list** *dnn_list*: Specify the list of DNNs supported by the UPF node.

Configuring a Virtual DNN under a DNN Profile

The SMF provides flexibility to send Virtual-DNN value on all northbound interfaces. Virtual DNN to be send on each interface can be configured as follows. The Resource Manager (RMGR) virtual DNN is used to map IP pool to DNN.

To configure a virtual DNN under a DNN profile, use the following sample configuration:

```
config
   profile dnn profile_name
      dnn dnn_name network-function-list [ chf | ocs | pcf | pcrf | radius
 | upf | cgf ]
   profile profile_name
   end
```

NOTES:

- **dnn** *dnn_name*: Specify the DNN name. *dnn_name* must be an alphanumeric string.
- **network-function-list**: Specify the network functions. The DNN profile goes to these network functions. Supported values are **CHF, OCS, PCF, PCRF, RADIUS, UPF, and CGF.**

Configuring Override Command

In addition to the preceding CLI, SMF has the capability to override the access DNN with the vDNN received from the RADIUS server.

RADIUS-ep is upgraded to decode Starent VSA attribute “SN-Virtual-APN-Name (Type: 94) “ and application is enhanced to support this attribute.

RADIUS Server sends vDNN to SMF in access accept and SMF includes this DNN in N4 messages to UPF. A new configuration is added on the SMF to decide whether to override the DNN sent on specific interfaces with the value received from RADIUS server.

Override keyword is added to support virtual DNN from the Radius Server.

```
config
   profile dnn profile_name
      dnn override network-function-list [ chf | ocs | pcf | pcrf | radius
 | upf | cgf ]
       dnn override rmgr
       end
```

Details of attribute used for receiving virtual DNN on RADIUS interface is as follows:

- **SN**: Virtual-APN-Name
- **Syntax**: Opaque Value
- **Length**: 1-64
- **Type**: 26
- **Vendor ID**: 8164
- **VSA Type**: 94
- Override keyword takes priority over the locally configured value.
- Override keyword is present but RADIUS isn’t providing any vDNN then SMF uses the locally configured value (if present) or gnDNN.
- If for an interface, there’s no configuration (either override or local-dnn-name), it takes the gnDNN.

  Override vDNN isn’t applicable for UDM network-function.
- The framed-ip received from the RADIUS server must be a part of the IP pool associated to the vDNN received from the RADIUS server. If there’s mismatch, session creation fails.
- Different RMGR vDNN can be assigned to the same UE for same DNN for dynamic and static ip allocation case and hence IP can be assigned from dynamic or static pool.

Associating Subscriber Policy under the SMF Service

To associate a subscriber policy under SMF service, use the following sample configuration:

```
config
  profile smf smf_profile_name
     service name service_name
        subscriber-policy subscriber_policy_name
        end
```

NOTES:

- **subscriber-policy** *subscriber_policy_name*: Specify the subscriber policy name. *subscriber_policy_name* must be an alphanumeric string.

Network Function Selection based on SMF Instances

Table 320: Feature History

Feature Name	Release Information	Description
UPF Selection based on SMF Instances	2024.01.2	This feature allows you to customize SMF instances in the Subscriber Policy Configuration and to bind SMF instances to the colocated UPFs in the inter-site GR deployment model. When the user selects operator policies, the SMF instances act as a filter and allow the SMF to select a specific DNN profile. The DNN selection helps in finding the closest and active Network functions (for example, UPFs) and ensures routing the user traffic only to the colocated UPFs. This implementation reduces the latency and improves user experience. To implement this feature, the following keywords are added under the policy subscriber command: • **instance-start-range** • **instance-stop-range** **Default Setting**: Disabled – Configuration required to enable

Instance-based Network Function Selection

Feature Description

During the subscriber session creation, SMF selects operator policy based on the SMF instance IDs configured in the Subscriber Policy Configuration mode. For each subscriber, SMF associates the selected operator policies with different DNN profiles, virtual DNNs, IP pools, and UPF profiles.

SMF provides the flexibility to choose appropriate DNN profiles corresponding to the SMF instances.

For example, in an active-standby Geo Redundancy (GR) deployment scenario, assume that there are two racks (Rack 1 and Rack 2) with each rack comprising two regions (Region 1 and Region 2), two active and

standby SMF instances (SMF instance 1 and SMF instance 2), IP pools (Pool 1 and Pool 2), virtual DNNs (vdnn 1 and vdnn 2), and two UPF sets (UPF Set 1 (UPF 1 and UPF 3) and UPF Set 2 (UPF 2 and UPF 4)).

SMF is configured in such a way that vdnn 1 is associated to SMF Instance 1, Pool 1, and UPF Set 1, and vdnn 2 is associated to SMF Instance 2, Pool 2, and UPF Set 2. When the subscriber attempts to establish PDU connection, SMF instance is selected based on the Virtual IP (VIP) of the session it lands. If SMF instance 1 in one region is active and selected, SMF chooses vdnn1, Pool 1, and UPF Set 1 even though the SMF instances have the same DNN in both the regions.

SMF subsequently distributes the IP pools from Pool 1 only to the UPFs in UPF Set 1. If the SMF instance IDs are not configured, SMF allocates the available IP addresses to the UPFs associated to both the SMF instances.

Configuring SMF Instances

To configure the SMF instances, use the following sample configuration:

Note It is recommended to add this configuration at runtime. A new operator policy selection post configuration change uses new configuration.

```
config
   policy subscriber subscriber_policy_name
      precedence precedence_value
          instance-start-range start_range_value
          instance-stop-range stop_range_value
          operator-policy operator_policy_name
          end
```

NOTES:

- **precedence** *precedence_value*: Specify the precedence value associated with the subscriber policy.

  The maximum limit for precedence is 2048.

- **instance-start-range** *start_range_value*: Specify the SMF instance start range value. *start_range_value* must be an integer in the range from 1 to 8.

- **instance-stop-range** *stop_range_value*: Specify the SMF instance stop range value. *stop_range_value* must be an integer in the range from 1 to 8.

Configuration Example

The following is an example of a configuration **show running-config policy subscriber** command that describes SMF instances for DNN profile selection.

```
 [smf] smf# show running-config policy subscriber
Wed Mar  6  05:09:45.143 UTC+00:00
policy subscriber polSub
 precedence 1
  sst                  02
  sdt                  Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range     100000000000001
```

```
  supi-stop-range       999999999999999
  gpsi-start-range      100000000000001
  gpsi-stop-range       999999999999999
  instance-start-range 1
  instance-stop-range  1
  operator-policy       opPolHomer
exit
```

Switching DNN Profile to Offline Mode During Dynamic Config Update

Feature Description

This feature enables SMF to switch the DNN to offline mode to support dynamic configuration update. SMF allows dynamic configuration update of some DNN profile parameters only when the DNN profile is changed to offline mode.

When the DNN is in offline mode, new sessions or subsequent messages of existing sessions, will use the updated configuration values.

Important You must clear the subscriber sessions before switching DNN to offline mode while changing the configuration for which dynamic change is not allowed. New session requests are rejected until the DNN is changed back to online mode.

How it Works

This section describes how this feature works for the supported SMF configurations.

DNN Policy

DNN Policy configuration defines the DNN Profile mapping with the DNN. After the DNN to profile mapping is changed, new subscriber for the same DNN uses the updated DNN Profile. So, there is no impact on existing subscribers.

DNN Profile

DNN profile defines various parameters for a particular DNN.

The following table describes if the dynamic configuration change is allowed or if the DNN must be set to an offline mode.

Table 321: DNN Profile Configuration and its Impact During Dynamic Update

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnsServers	Allowed	No impact
DnnInfo	Allowed	New values are used after database reload of the session

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
NetworkElementProfile	Not recommended (See NOTES)	
Timeout	Allowed	No impact
ChargingProfile	Not recommended (See NOTES)	
RemoteVmac	Allowed	No impact
PcscfProfile	Allowed	No impact
PpdProfile	Allowed	Immediate (new values are used)
DefaultSscMode	Allowed	No impact
DefaultPduSession	Allowed	No impact
AllowedPduSession	Allowed	No impact
QosProfile	Allowed	Immediate (new values are used)
UpfApn	Allowed	No impact
SecondaryAuthen	Allowed	No impact
LocalAuthorization	Allowed	No impact
NetworkCapability	Allowed	No impact
PolicyProfile	Allowed	No impact

NOTES:

- It's recommended not to modify or delete the NetworkElementProfile and ChargingProfile configuration parameters. If the parameters are changed, then the behavior for:
  - NetworkElementProfile: Messages for the existing sessions may be sent on new servers.
  - ChargingProfile: There may be some inconsistencies related to Usage Reporting Rules (URRs) between SMF and UPF.
- For modifying the DNN profile mapping, the DNN profile must be in the offline mode.
- It's recommended to review the messages shown in the help string before executing the CLI commands.
- Switch the DNN profile to an offline mode when configuring the parameters dynamically. This step avoids the network impact, which is caused by the configuration changes.

Subscriber Policy

SMF uses subscriber policy to select the operator policy based on the following options:

- SUPI range
- SST (Slice/Service Type)
- IMSI range

- GPSI
- PEI
- SDT (Slice Differentiator Type)
- S-NSSAI
- PLMN ID
- CC (Charging Characteristics) range
- SMF instance range

A change in Subscriber Policy configuration can be applied dynamically as it has no impact on the existing sessions. SMF selects the operator policy for the new sessions based on the updated configurations.

Limitations

The following limitations apply when the DNN is in the offline mode:

- The subsequent 5G calls for the offline DNN are rejected with the HTTP Cause - HTTP_STATUS_CODE_503_SERVICE_UNAVILABLE, and 5GSMCause as “Service option temporarily out of order”.
- The subsequent 4G calls for the offline DNN are rejected with the GTP cause “No resources available".

Configuring the Offline DNN Profile

This section describes how to enable the offline mode for a DNN profile.

Switching the DNN Profile to Offline Mode

To change the DNN profile to offline mode, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    mode dnn_mode
    end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile.
- **mode** *dnn_mode*: Specify the DNN mode of operation. When the DNN mode is set to **offline**, the new sessions are rejected. The default value is **online**.

Verifying the DNN Profile Offline Mode Configuration

This section describes how to verify if the DNN profile is set to the offline mode.

The following is an example output of the **show running-config profile dnn** *profile_name* command.

```
show running-config profile dnn intershat
  profile dnn intershat
       mode offline
```

```
    network-element-profiles chf chf1
    network-element-profiles amf amf1
    network-element-profiles pcf pcf1
    network-element-profiles udm udm1
    charging-profile chgprf1
    virtual-mac b6:6d:47:47:47:47
    ssc-mode 2 allowed [ 3 ]
    session type IPV4 allowed [ IPV6 IPV4V6 ]
    upf apn intershat
    dcnr true
exit
```

OAM Support for DNN Profile Offline Mode Setting

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The following label is introduced as part of this feature:

- LABEL_DISC_PDUSETUP_DNN_OFFLINE: This label is defined to indicate that the call is rejected because the DNN is in the offline mode.

DNN Inheritance

Feature Description

Table 322: Feature History

Feature Name	Release Information	Description
DNN Inheritance for 4G Sessions on Legacy Interfaces	2024.02.0	SMF with legacy interfaces support the DNN inheritance feature.

SMF provides a way to configure common attributes in a parent DNN profile template and reuse it in other DNN profiles, for example, child DNN profiles as and when required. This feature optimizes the DNN profile configurations and improves the operational efficiency.

Note The DNN Inheritance feature is currently qualified only for SMF (including legacy interfaces) and not for cnSGW-C.

How it Works

This section provides details about how the network operators can perform the DNN profile configuration to inherit or reuse a parent DNN profile.

Table 323: Preparation to Configure the Parent DNN Profile

Step	Description
1	Configure parent DNN profile having common attributes.
2	Inherit the configured parent DNN profile in a child DNN profile. The following conditions apply: • If a child profile is trying to inherit a DNN profile that doesn't exists, then the SMF CLI displays an error while committing the changes. • If the parent DNN profile is deleted but found in a child profile, then SMF CLI displays an error while committing the changes. **Note** Delink the parent profile from the child DNN profile to delete the parent DNN profile. • If the attributes configured in a child DNN profile do not belong to any parent DNN profile, then the operator can modify those attributes in an individual child DNN profile.

Step	Description
3	

Step	Description

	SMF receives request for the child DNN profile. If the child DNN profile has an *inherit* attribute, then SMF resolves the inherited/parent profile based on the following conditions:
	• If the parent profile is found and the child profile doesn't override parent attributes, then SMF updates the child profile with inherited attributes.
	• If a parent profile is found and a child profile overrides some or all the parent attributes, then SMF prioritizes overridden attributes over a parent profile and updates the child profile by taking overridden attributes from a child profile and the rest of the attributes from a parent profile.
	• If a parent profile has attributes in the form of arrays or slices, and the child profile also has the same attributes configured, then the resultant DNN profile overrides that attribute completely from the child profile, which means the combined profile contains the value of the child attribute.
	Example for DNN profiles:
	`profile dnn intershat_Parent // parent dnn profile`
	`ims mark qci [ 83 128 ]`
	`network-element-profiles chf chf1`
	`network-element-profiles amf amf1`
	`network-element-profiles pcf pcf1`
	`network-element-profiles udm udm1`
	`charging-profile chgprfFBC`
	`override [ charging-profile charging-characteristics-id ]`
	`virtual-mac b6:6d:47:47:47:47`
	`session type IPV4 allowed [ IPV6 IPV4V6 ]`
	`dcnr true`
	`exit`
	`profile dnn intershatRoamer // child dnn profile`
	`inherit intershat_Parent`
	`override [ charging-characteristics-id charging-qbc-profile ]`
	`exit`
	Example for resultant profiles:
	`profile dnn intershatRoamer // Resultant dnn profile`
	`ims mark qci [ 83 128 ]`
	`network-element-profiles chf chf1`
	`network-element-profiles amf amf1`
	`network-element-profiles pcf pcf1`
	`network-element-profiles udm udm1`
	`charging-profile chgprfFBC`
	`override [charging-characteristics-id charging-qbc-profile ]`
	`virtual-mac b6:6d:47:47:47:47`
	`session type IPV4 allowed [ IPV6 IPV4V6 ]`
	`dcnr true`
	`exit`
	• If a parent profile has attributes in the form of structures and the child profile also has the same attributes configured, then the resultant DNN profile overrides that attribute completely from child, which means the combined profile contains the value of a child attribute.
	Example for DNN profiles:
	`profile dnn intershat_Parent // parent dnn profile`
	`charging-profile chgprfFBC`
	`virtual-mac b6:6d:47:47:47:47`

Step	Description
	dcnr true network-element-profiles chf chf1 network-element-profiles amf amf1 network-element-profiles udm udm1 exit profile dnn intershatRoamer // child dnn profile inherit intershat_Parent network-element-profiles pcf pcf1 exit **Example for resultant profiles**: profile dnn intershatRoamer // Resultant dnn profile charging-profile chgprfFBC virtual-mac b6:6d:47:47:47:47 dcnr true network-element-profiles pcf pcf1 exit **Note** When the SMF receives a request for the child DNN profile and the child DNN profile doesn't have an inherit attribute, then the SMF returns all attributes from the child DNN profile.
4	Update the parent and child DNN profile at runtime. After the changes are committed, SMF picks the latest attributes from the child and parent profiles.

Configuring DNN Inheritance

You can define all the common attributes in a separate DNN profile and then use this parent profile in other DNN profiles by using the CLI configuration.

To inherit the parent DNN profile with common attributes, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      inherit dnn_template_name
       dnn rmgr  ims_pool_ipv6
      end
```

NOTES:

- **inherit** *dnn_template_name*: Specify the name of parent DNN profile to inherit to child profile(s).

Configuration Example

The following is an example configuration to inherit the attributes from a parent DNN profile and use them in a child profile.

```
// Parent DNN profile
profile dnn dnnprof-ims.epdg.prod
  dns primary ipv4 10.177.0.34
  dns primary ipv6 fd00:976a::9
  dns secondary ipv4 10.177.0.210
  dns secondary ipv6 fd00:976a::10
  network-element-profiles chf nfprf-chf1
```

```
  network-element-profiles amf nfprf-amf1
  network-element-profiles pcf nfprf-pcf1
  network-element-profiles udm nfprf-udm1
  dnn ims.epdg.prod network-function-list [ chf pcf udm upf ]
  timeout up-idle 3600 cp-idle 7320
  charging-profile           chgprof-1
  pcscf-profile              pcscf1
  ppd-profile                ppd-prof1
  ssc-mode 1 allowed [ 2 ]
  session type IPV6
  session skip-ind false
  upf apn ims.epdg.prod
  qos-profile                5qi-to-dscp-mapping-table-IMS
  always-on                  true
  dcnr                       true
  userplane-inactivity-timer 3600
  only-nr-capable-ue         false
exit

// Child DNN profile
profile dnn dnnprof-ims.prod
  inherit dnnprof-ims.epdg.prod
  dnn rmgr ims-pool-ipv6
exit
```

IP Pool Allocation per DNN

Feature Description

The IP Pool Allocation feature supports mapping of a UE-requested DNN to a configured DNN for IP Pool selection. This feature is supported for the SMF and PGW-C in 5G and 4G.

SMF supports the following functionalities:

- Supports configuration under the DNN profile to enable mapping of the UE-requested DNN to a DNN that is associated with an IP pool.
- Sends the mapped DNN over Remote Procedure Call (gRPC) to the Resource Manager functionality under Node Manager service for IP allocation.
- Supports configuration for IP pool DNN over the virtual DNN with Redundancy Manager, if available.
- Sends the UE-requested DNN when both the configuration for IP pool and the virtual DNN are unavailable.

How it Works

This section provides a brief of how the IP Pool Allocation feature works.

- The DNN profile lookup is based on the subscriber policy or DNN policy. The DNN profiles are associated in the SMF profile configuration. The subscriber policy takes precedence over the DNN policy when both the configurations are present.
- The subscriber policy contains a list of precedence values. The selection of the precedence is based on the SUPI, GPSI, serving PLMN, and NSSAI value of the subscriber.

- Each precedence has an associated operator policy. The DNN policy is picked from the selected operator policy.
- The DNN policy can have a DNN profile configuration for each of the UE-requested DNNs.
- The DNN profile contains the virtual or mapped DNN with its list of interfaces. This is an existing configuration and Redundancy Manager is also in the list of interfaces. For more information, see the Configuring a Virtual DNN under a DNN Profile, on page 837 section.
- The configuration under the DNN profile contains the mapping of the UE-requested DNN to IP pool DNN.
- The DNN profile selection occurs in the following order:
  - Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.
  - Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested Dnn) > Virtual DNN mapping.

Note
- IP pool DNN mapping takes precedence over the existing virtual DNN configuration if the Redundancy Manager configuration exists.
- If both the configurations for the Redundancy Manager are not present, the UE-requested DNN is used to select the IP pool.
- If the mapped DNN does not have the IP pool configured, then IP allocation fails, and the call is deleted.
- Both the EPS and 5G calls follow the same principles for IP allocation for a DNN.

Configuring IP Pool Allocation

This section describes how to configure the IP Pool Allocation feature.

Configuring the IP Pool Allocation involves either one of the following steps:

1. Configuring virtual DNN under DNN profile. For more information, see the Configuring a Virtual DNN under a DNN Profile, on page 837 section.

Note This is a generic configuration along with other interfaces as an option.

2. Allocating the IP pool per DNN

Note This configuration is only for IP allocation.

Allocating the IP Pool per DNN

To allocate the IP pool per DNN, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    dnn rmgr rmgr_name
    end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Map the Virtual DNN profile with the specified network DNN profile. *dnn_profile_name* must be an alphanumeric string.
- **dnn rmgr** *rmgr_name*: Specifiy the Redundancy Manager to which the DNN profile will be sent. *rmgr_name* must be an alphanumeric string.

Verifying IP Pool Allocation Configuration

This section describes how to verify the IP pool allocation configuration.

Use the **show full** CLI command in the DNN Profile Configuration mode to verify the configuration associated with IP pool allocation per DNN.

The following is an example output of this show command.

```
[unknown] smf(config-dnn-cisco123)# show full
profile dnn intershat
dns primary ipv4 209.165.200.231
dns primary ipv6 2001:DB8:1::1
dns secondary ipv4 209.165.200.232
dns secondary ipv6 2001:DB8:1::2
network-element-profile-list chf [ chgser1 ]
dnn starent.com network-function-list [ upf chf rmgr ]
dnn rmgr cisco.com
charging-profile chgprf1
virtual-mac      01-00-5E-90-10-00
pcscf-profile    pcscf1
ppd-profile      ppd1
ssc-mode 1
session type IPV4
.
.
.
```

IP Pool Allocation per Slice and DNN

Feature Description

SMF supports IP pool allocation per slice with the same DNN. A slice is a logical end-to-end network that is created dynamically. A user equipent (UE) can access multiple slices over one access network, such as over the same radio interface.

SMF performs the following tasks:

- Register, discover, subscribe, and send traffic to all the external NFs based on the slice ID.

- Provide slice-based procedure and session statistics.
- Provide slice information on an EDR.
- Provide slice information on logs.
- Limit the maximum number of supported slices on SMF to 512.

How it Works

SMF selects NFs, such as PCF, CHF, UDM, and AMF through the static configuration or NRF-based dynamic selection. In both these options, the messaging includes the slice information that is used in those interfaces.

SMF performs the following tasks:

- Register slice with NRF.
- Receive slice information on the N11 and N10 interfaces.
- Use slice for peer NF discovery and UPF selection.
- Send slice information on the N7 and N40 interfaces.

Limitations

The IP Pool Allocation per Slice and DNN feature has the following limitations:

- Only the procedure and session statistics have the slice information. Other statistics are on NF level.
- Enabling or disabling logging based on slice information is not supported.

Feature Configuration

This section describes how to configure the IP pool allocation per slice and DNN.

Configuring this feature involves the following steps:

1. Configure tags. For details, see Configuring SMF Tags, on page 749.
2. Perform the dynamic node selection with slice using the following tasks:
   - Register NRF. For details, see Discovering NRF.
   - Configure allowed NSSAI values. For details, see Configuring Allowed NSSAI Values.
   - Discover NRF. For details, see Discovering NRF.
3. Configure NSSAI labels of smf_service_stats metrics for slice information on procedure and session statistice. For details, see Configuring Metrics Collection, on page 1618.

Configuring Allowed NSSAI Values

To configure the allowed NSSAI values for slicing, use the following sample configuration:

```
config
```

```
profile smf smf_profile_name
   instances instance_id
      allowed-nssai allowed_nssai_values
      end
```

NOTES:

- **allowed-nssai** *allowed_nssai_values* : Specify one or multiple values for the allowed NSSAI for slicing.

Configuring Slice-based IP Pool Allocation

To configure the slice-based pool allocation, use the following sample configuration.

```
config
nssai name nssai_name
   sst sst_value
   sdt sdt_value
   dnn dnn_name_value
   pool-selection pool_selection_value
   end
```

NOTES:

- **pool-selection** *pool_selection_value* : Configure the IP pool selection methods as DNN or NSSAI. The default pool selection method is DNN. If the pool selection method is slice or slice DNN only, then based on the slice and the DNN, the IP pools are selected.

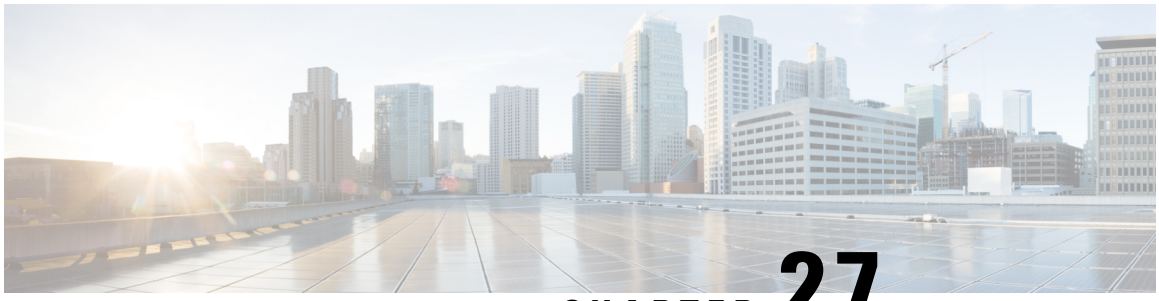
Note

- When you configure the pool selection method as NSSAI for a slice, then in IPAM configuration for all the DNN for that UPF, you must configure "slice1" and "dnn" as values.
- In IPAM, tag "nssai" is a string and must match with the SMF slice configuration name.

Configuration Example

The following is an example configuration of the slice-based pool allocation.

```
nssai name slice1
 sst 02
 sdt  Abf123
 pool-selection [ dnn nssai ]
exit
```



CHAPTER 27

Multiple PLMN Support

- Feature Summary and Revision History, on page 855
- Feature Description, on page 856
- How it Works, on page 856
- Configuring Multiple PLMNs, on page 856
- OAM Support for Multiple PLMNs, on page 859

Feature Summary and Revision History

Summary Data

Table 324: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 325: Revision History

Revision Details	Release
Added the non-standard PLMN list configuration.	2023.04.0
Removed the **visitor-hrt** CLI keyword from the configuration in Operator Policy.	2021.02.3
First introduced.	2021.01.0

Feature Description

The multi-PLMN feature supports multiple PLMNs for homer and roamer networks. A maximum number of 32 PLMNs can be configured.

SMF uses the primary PLMN configured under profile DNN for peer discovery. The feature supports homer and roamer networks with different session type configuration. Homer with IPv6 session type configuration and roamer with IPv4 or IPv6 session type is a typical configuration.

This feature supports emergency calls from 4G and 5G RATs from roamer UEs with SIM (unauthenticated IMSI) and without SIM. For emergency calls without IMSI, if primary PLMN is not configured (no PLMN ID and no primary PLMN under profile DNN), then one of the PLMNs in the PLMN list is used as primary PLMN for external messaging.

SMF validates UE PLMN on receiving SmContextCreate or CreateSessionRequest message and populates the PLMN in external messaging.

For more details on the roaming functionality, see the Roaming Support, on page 1281 chapter.

How it Works

The operator PLMNs configured under PLMN list includes all UE PLMNs and serving PLMNs.

On receiving the Create Request from 4G or 5G RAT (SmContextCreate or Create Session Request), the SMF extracts UE PLMN from SUPI. SMF compares the UE PLMN and serving PLMN with the configured PLMN list and populates the PLMN in external messaging. The SMF determines the roaming status of subscribers based on the HPLMN values.

If the UE PLMN and the serving PLMN both belong to the PLMN list that is configured in SMF, then it is a home subscriber. If the UE PLMN does not belong to the configured PLMN list and the serving PLMN belongs to the configured PLMN list, then it is a visitor. If the UE PLMN belongs to the configured PLMN list and the serving PLMN does not belong to the configured PLMN list, then it is a roamer.

Configuring Multiple PLMNs

This section describes how to configure the multi-PLMN feature.

Configuration-based Peer NF Selection

This section describes how to configure the use of NRF discovery or local configuration for selecting peer network function.

The configuration under profile network-element allows the user to have different selection logic linked to subscriber policy. For example, the user can configure peer NF selection logic for homers, roamers, or visitors.

To select the configuration for NF discovery, use the following sample configuration:

```
config
  profile network-element amf amf_profile_name
    discovery local
    end
```

NOTES:

- **discovery local**: Specify to use local configuration for NF discovery.

Configuring PLMN ID

This section describes how to configure the PLMN ID.

To configure one or multiple PLMN IDs, use the following sample configuration:

```
config
  profile smf smf_profile_name
    plmn-id mcc mcc_value mnc mnc_value
    plmn-list { mcc mcc_value mnc mnc_value | range mcc mcc_value mnc mnc_value
 }
    end
```

NOTES:

- **plmn-id mcc** *mcc_value* **mnc** *mnc_value*: Specify the 3-digit Mobile Country Code (MCC) and 2- or 3-digit Mobile Network Code (MNC) of the PLMN ID. *mcc_value* and *mnc_value* must be a string.
- **plmn-list { mcc** *mcc_value* **mnc** *mnc_value* **| range mcc** *mcc_value* **mnc** *mnc_value* **}**: Specify the list of 3-digit Mobile Country Code (MCC) and 2- or 3-digit Mobile Network Code (MNC) of multiple PLMNs. *mcc_value* and *mnc_value* must be a string.

Note

- A maximum number of 32 PLMNs can be configured.
- All operator PLMNs are configured under PLMN list including all UE-PLMNs and serving PLMNs.

Configuring Non-standard PLMN List

This section describes how to configure the non-standard PLMN list.

To configure one or multiple non-standard PLMN lists, use the following sample configuration:

```
config
  profile smf smf_profile_name
    non-standard-plmn-list mcc mcc_value mnc mnc_value
    end
```

NOTES:

- **non-standard-plmn-list mcc** *mcc_value* **mnc** *mnc_value* : Specify the list of supported non-standard PLMN to derive UE PLMN ID. *mcc_value* and *mnc_value* must be an integer.

Verifying Non-standard PLMN List

This section describes how to verify the non-standard PLMN list feature configuration.

Use the following show command to view the list of non-standard PLMN configured.

show running-config profile smf plmn-list

The following is an example output of this show command.

```
[smf] smf# show running-config profile smf smf1 non-standard-plmn-list
   profile smf smf1
       non-standard-plmn-list mcc 200 mnc 111
       exit
       non-standard-plmn-list mcc 100 mnc 100
       exit
exit
```

Configuring Primary PLMN

This section describes how to configure the primary PLMN under DNN profile.

To configure the primary PLMN for peer discovery, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    primary-plmn mcc mcc_value mnc mnc_value
    exit
```

NOTES:

- **primary-plmn mcc** *mcc_value* **mnc** *mnc_value*: Specify the 3-digit Mobile Country Code (MCC) and 2- or 3-digit Mobile Network Code (MNC) of the primary PLMN. *mcc_value* and *mnc_value* must be a string.

Configuring PLMN in NRF Discovery

This section describes how to configure the PLMN for NRF Discovery.

To configure the PLMN query parameters, use the following sample configuration:

```
config
  profile network-element pcf pcf_profile_name
    query-target-plmn { primary | serving | ue }
    exit
```

NOTES:

- **query-target-plmn { primary | serving | ue }**: Specify the query parameter target-plmn to be used in NRF discovery. It can be one of the following:
  - **primary**: Configure the primary PLMN which is sent in the target PLMN.
  - **serving**: Configure the serving PLMN which is sent in the target PLMN.
  - **ue**: Configure the UE PLMN which is sent in the target PLMN.

Configuring Serving PLMN MNC list

This section describes how to configure the MNC list for serving PLMN.

To configure the serving PLMN information, use the following configuration:

```
config
  policy subscriber policy_name
    precedence precedence_value
    serving-plmn { mcc mcc_value | mnc mnc_value | mnc-list mnc_list_values }
    exit
```

NOTES:

- **serving-plmn { mcc** *mcc_value* **| mnc** *mnc_value* **| mnc-list** *mnc_list_values* **}**: Specify the 3-digit Mobile Country Code (MCC), 2- or 3-digit Mobile Network Code (MNC), or the list of MNC values of the serving PLMN. *mcc_value* and *mnc_value* must be a string.

  mnc_list_values must be a string. For example: [580 660]

- This configuration is backward compatible. If both **mnc** and **mnc-list** are configured, both are considered while selecting the operator policy.

Configuring Roamer in Operator Policy

This section describes how to configure the roamer network in operator policy.

To configure the operator policy-specific roaming configuration, use the following sample configuration:

```
config
  policy operator operator_policy_name
    roaming-status { roamer | visitor-lbo }
    exit
```

NOTES:

- **roaming-status { roamer | visitor-lbo }**: Specify the roaming status. It can be one of the following:
  - **roamer**: Specify the status of roamer in homer network.
  - **visitor-lbo**: Specify the status of roamer in local breakout session.
- In the absence of roaming status configuration, the SMF uses the values of PLMN and SUPI to determine the roaming status of subscribers.

OAM Support for Multiple PLMNs

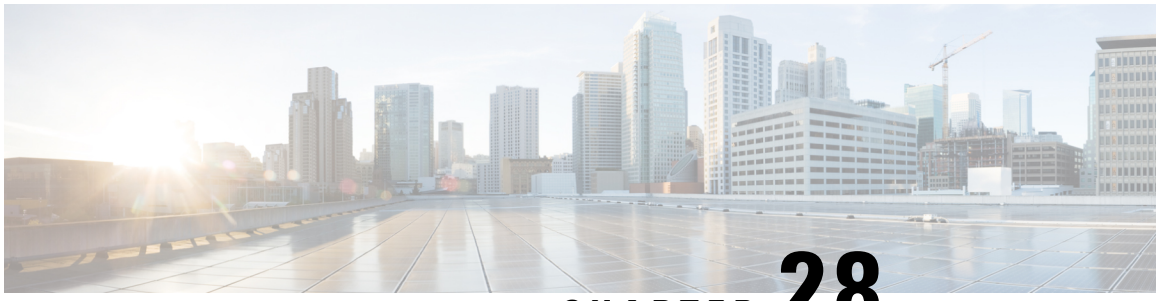
This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics are updated to support the multiple PLMN feature.

- smf_service_stats: This statistics includes roaming_status label to indicate the roaming status of the subscriber session.
- smf_service_counters: This statistics includes roaming_status label to indicate the roaming status of the subscriber session.

- smf_session_counters: This statistics includes roaming_status label to indicate the roaming status of the subscriber session.
- smf_session_stats: This statistics includes roaming_status label to indicate the roaming status of the subscriber session.



CHAPTER 28

N3IWF for Non-3GPP Access

Table 326: Feature History

Feature Name	Release Information	Description
N3IWF for Untrusted Non-3GPP Access Network	2024.01	SMF supports the N3IWF interface for interworking between 5G core and untrusted non-3GPP networks. N3IWF facilitates seamless handover and uninterrupted connectivity for users when they transition between different network types. **Default Setting**: Disabled – Configuration Required

- Feature Description, on page 861
- How it Works, on page 862
- Standard Compliance, on page 863
- OAM Support, on page 864

Feature Description

The Non-3GPP Interworking Function (N3IWF) in the 5G SBA (Service Based Architecture) is responsible for interworking between untrusted non-3GPP networks and the 5G core. As such, the N3IWF supports both N2 and N3 based connectivity to the core, whilst supporting IPSec connectivity towards the device. The N3IWF provides the access and authentication protocols from the non-3GPP Wi-Fi network to seamlessly interface with the 5G Core Network by enabling the N2 and N3 interfaces.

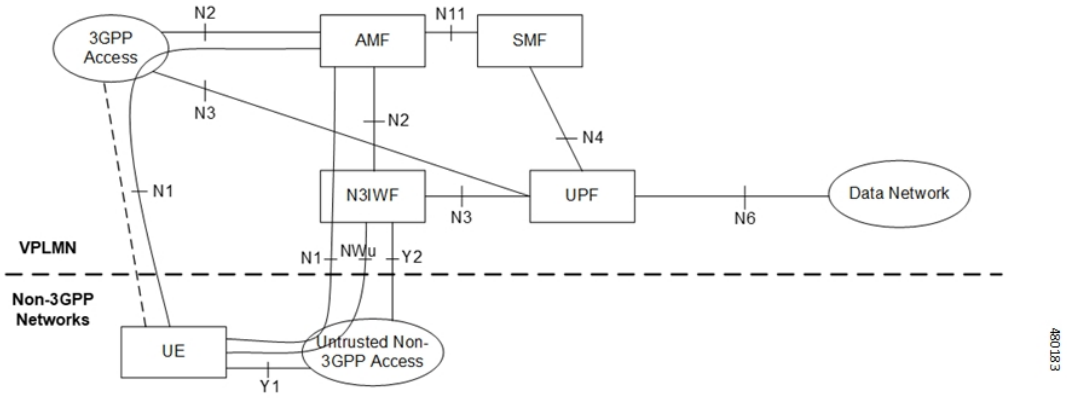
This interface establishes an end-to-end security association between the User Equipment (UE) and N3IWF, irrespective of the security measures implemented at the layer 2 access level (WPA2).

SMF supports only the following procedures:

- PDU session establishment over N3IWF
- PDU session release over N3IWF

Architecture

The following figure represents the non-roaming architecture of 5G core network with untrusted non-3GPP access network.



How it Works

N3IWF is deployed as a network function within the service provider's infrastructure. It interacts with various components of the 5G network architecture, such as the Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF).

Call Flows

This section describes the call flows related to the N3IWF.

PDU Session Establishment Over N3IWF

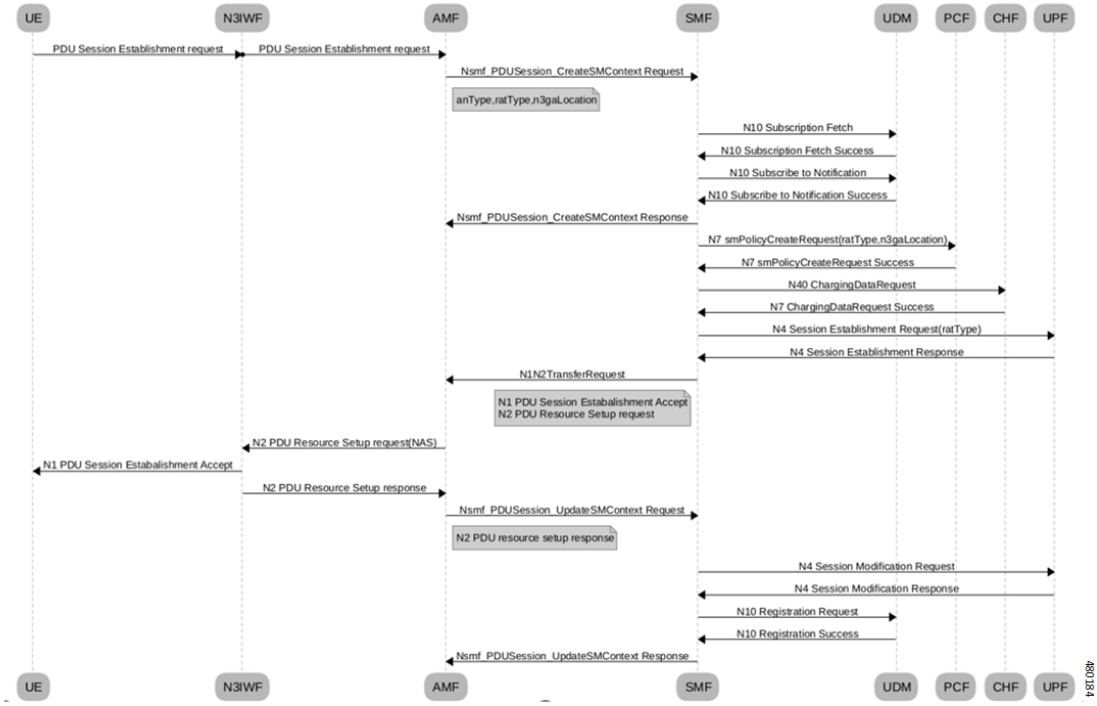
UE performs initial registration and authentication with 5G core network using N3IWF. The 5G PDU session create over N3IWF remains the same as that of 5G NR PDU create except that the 5G PDU Create Request message includes these additional attributes:

- ratType
- anType
- n3gaLocation

Note

- 5G PDU session create over N3IWF does not require EBI assignment to be performed.
- The n3gaLocation attribute carrying N3GPP TAI information is included in 3GPP-User-Location-Info AVP and sent to RADIUS server if the anType attribute is Non-3GPP Access.
- N3GaLocation information is shared only with PCF and CHF.

The following call flow describes the initiation of PDU establishment over N3IWF:



PDU Session Release over N3IWF

The PDU session release procedure over N3IWF remains the same as with the following 5G NR PDU session release procedures.

- Access triggered release
- Network triggered release
  - PCF initiated
  - Admin initiated
  - CHF triggered
  - IDLE timeout-based
  - Release due to N4 path failure

Standard Compliance

The N3IWF feature complies with the following standards:

- 3GPP 23.501 release 15 version

OAM Support

Bulk Statistics Support

This feature supports a new label "anType" as part of the smf service stats. This label defines the access network type as 3GPP access or non-3GPP access.

For more information on bulk statistics support, see the *UCC 5G SMF Metrics Reference* document applicable for this release.

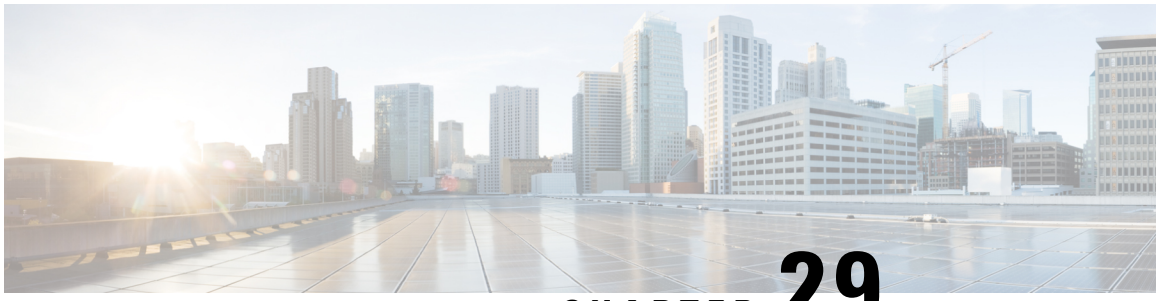
Monitoring Support

The existing show subscriber and clear subscriber commands include a new filter option "an-type" to indicate the access type of subscribers. The show subscriber command output also displays information on N3Ga location.

If the UE connects to the Wi-Fi access point and attempts to attach through ePDG, the access type is categorized as non-3GPP access. In the case of N3IWF sessions attaching through AMF, the access type is 3GPP access and the an-type is non-3gpp access.

Logging Support

This feature provides support for access network type information in the procedure failure logs.



CHAPTER 29

Network-initiated Session Modification Procedures

- Feature Summary and Revision History, on page 865
- Feature Description, on page 866
- How it Works, on page 866
- OAM Support, on page 870

Feature Summary and Revision History

Summary Data

Table 327: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 328: Revision History

Revision Details	Release
Added VoNR related hardening fix.	2022.04.0
First introduced.	Pre-2020.02.0

Feature Description

The purpose of PDU session modification procedure is to create dedicated QoS flows for a UE. There are two ways to create dedicated QoS flows with different QoS characteristics to the default QoS flow for the UE such as the:

- UE-initiated PDU session modification
- Network-initiated PDU session modification

Note The PDU modify procedure is triggered if the Policy Update Response includes the policy parameters.

The network can be AN, AMF, or PCF.

The SMF receives a UE-initiated session modification request or network-initiated session modification request to augment the PDU session of UE to either modify an existing or creating a new QoS flow suitable for the user traffic.

Note If there is a failure during a PCF-initiated flow deletion procedure, the SMF deletes the PCC rules and communicates the details on the deleted PCC rules to UPF and PCF.

How it Works

This section describes how this feature works.

Call Flows

This section describes the following call flows:

- Network-initiated Modification Call Flow for Active User Plane and UE in CM-Connected State, on page 866
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State, on page 868
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State, on page 868

Network-initiated Modification Call Flow for Active User Plane and UE in CM-Connected State

This section describes how the N4 session modification works after network initiation when the UE is in CM-Connected state and the User Plane is activated. The network can be PCF, UDM, or SMF.

The following figure depicts the network-initiated modification call flow when the UE is in CM-Connected state and the User Plane is activated.

Figure 185: Network-initiated Modification Call Flow for UE in CM-Connected State and Activated User Plane

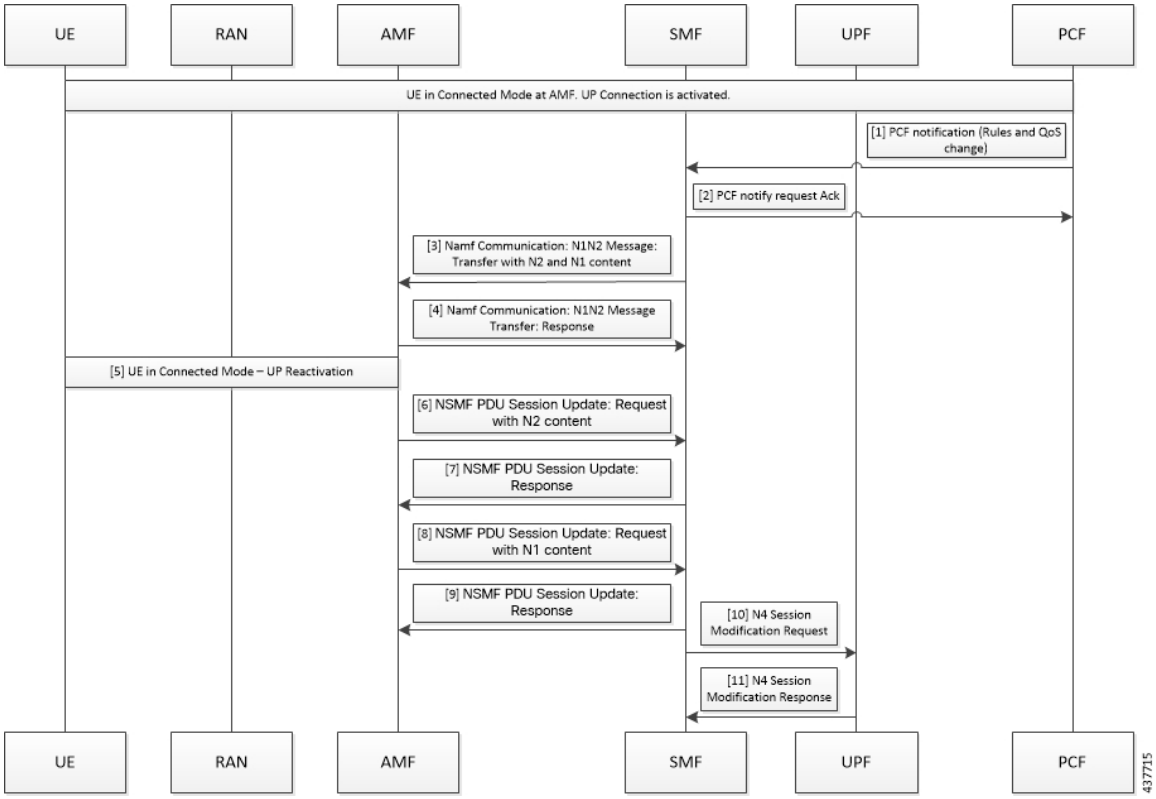


Table 329: Network-initiated Modification Call Flow Description for UE in CM-Connected State and Activated User Plane

Step	Description
1	The PCF sends the notification towards SMF with policy decision to apply.
2	The SMF sends an acknowledgment for the policy notification to the PCF.
3	The SMF identifies the changes in QoS model that occur due to policy decision and triggers the NAMF Communication N1 and N2 message transfer toward AMF. This message transfer includes the following details: • PDU Session ID • N2 SM information • N1 SM information • N1 and N2 transfer failure notification target address N2 includes the PDU session resource modify request transfer IE and N1 includes the PDU session modification request.
4	As UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and “N1_N2_TRANSFER_INITIATED” cause.
5	The user plane modification procedures begin both towards RAN and UE.

Step	Description
6	After receiving a response from RAN, the AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface.
7	The SMF responds to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request.
8	After receiving a response from the UE, the AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N1 interface.
9	The SMF responds to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request.
10	Based on the new QoS information, the SMF initiates the N4 Modification procedure towards the UPF to modify the session.
11	The UPF modifies the session and sends the acknowledgment of modification to the SMF.

Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State

This section describes the network-initiated modification procedure when the UE is in CM-Connected state and the User Plane (UP) context is deactivated.

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “N1N2_TRANSFER_INITIATED” cause.
5. The SMF waits for the Nsmf_PDUSession_UpdateSMContext message from the AMF.
6. After receiving the response from UE, the SMF updates the subscriber session in the UPF with the modified parameter values and the UP context state remains as Deactivated.
7. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
8. The UPF sends the N4 Session Modification response for the PDU session.
9. The SMF activates the UP connection as a result of the trigger to send downlink or uplink data.

Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State

This section describes the network-initiated modification procedure when the UE is in CM-Idle state and the User Plane (UP) context is deactivated.

The SMF supports the following use cases during the network-initiated PDU session modification procedure:

- When the UE turns active with the service request for PDN activation
- When the UE turns active with the control service request

Use case 1: When the UE turns active with the service request for PDN activation

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING_TO_REACH_UE” cause.
5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.

Note The N1 PDU Modification Command retransmission timer is configurable. Use the **n1 t3591-pdu-mod-cmd timeout** *timeout* **max-retry** *retry_count* command in Access Profile Configuration mode to configure the timeout value and maximum attempts for the retransmission of N1 PDU Modification Command. The default timeout value is 2 seconds and the default retry count is 2.

6. The UE receives the paging request from the AMF and initiates the requested service to activate the PDU session. The UE includes the PDU Session ID in PDU Session-to-Activate list only if the UP context needs to be activated.

   The SMF initiates the Idle-to-Active PDU Session transition procedure and suspends the current modification procedure.
7. After the Idle-to-Active procedure is complete, the SMF restarts the modification procedure and sends both the N1 and N2 content in N1 N2 transfer message and waits for both N1 and N2 response from the UE and gNB respectively.
8. The SMF receives the N2 response from gNB, and the N1 response from the UE respectively.
9. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
10. The UPF sends the N4 Session Modification response for the PDU session.

Use case 2: When the UE turns active with the control service request.

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING_TO_REACH_UE” cause.

5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.
6. The AMF initiates the paging procedure towards the UE and the UE turns active with the Service Request for control message.
7. The SMF receives the N1 response from the UE.
8. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details. Then, the SMF sets the Forwarding Action Rule (FAR) action for the new rules as ‘drop’.
9. The UPF sends the N4 Session Modification response for the PDU session.

Standards Compliance

The network-initiated messages support for UE in CM-Idle or CM-Connected state feature complies with the *3GPP TS 23.502, V15.6.0 (2019-10)*.

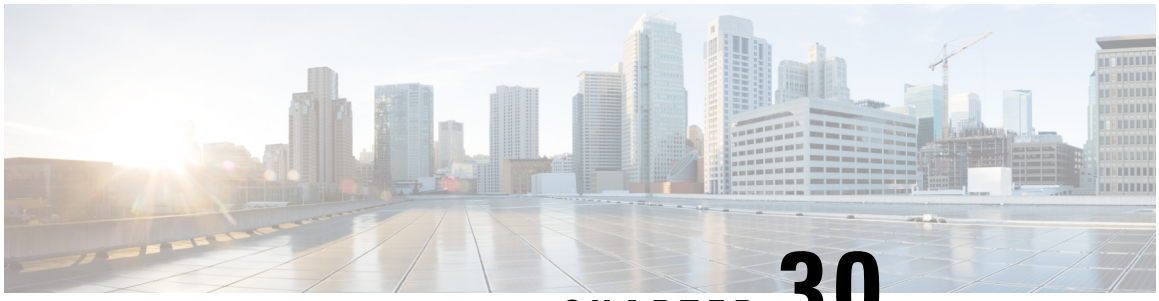
OAM Support

This section describes the operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The SMF maintains the following statistics triggered during the network-initiated modification procedure.

- Total number of attempted network-initiated modifications triggered when the UP context is deactivated.
- Total number of succeeded network-initiated modifications triggered when the UP context is deactivated.
- Total number of failed network-initiated modifications triggered when the UP context is deactivated.
- Total number of "ATTEMPTING_TO_REACH_UE" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.
- Total number of "N1N2_TRANSFER_INITIATED" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.



CHAPTER 30

New Radio Dual Connectivity

- Feature Summary and Revision History, on page 871
- Feature Description, on page 871

Feature Summary and Revision History

Summary Data

Table 330: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 331: Revision History

Revision Details	Release
First introduced.	2021.02.0

Feature Description

New Radio Dual Connectivity (NR-DC) is a dual connectivity configuration using the 5G standalone core. In this configuration, both the primary and secondary RAN nodes are 5G gNBs. SMF supports 5G aggregation along with NR-DC to achieve higher 5G data rates.

This feature has the following key points:

- Use NR-DC only for data traffic
- Use only default flow for data traffic
- One tunnel is sufficient
- SMF requires no configuration

The NR-DC feaure is applicable to both roaming and non-roaming scenarios.

How it Works

The RAN-initiated QoS flow is offloaded from Primary Node (PN) to Secondary Node (SN). After the flow is created, PN may switch the traffic to SN. SN allocates new DL TEID and sends it to PN. Then, PN initiates the PDU Session resource modify request with that DL TEID. SMF updates only the DL FAR to switch the traffic to SN. The switch from SN to PN can happen. However, SMF has no behavioral change.

Call Flows

This section describes the call flow of RAN-initiated Qos flow offloading from PN to SN.

RAN-Initiated QoS Flow Offloading Call Flow

This section describes the call flow of RAN-initiated QoS flow offloading from PN to SN.

Figure 186: RAN-Initiated QoS Flow Offloading Call Flow

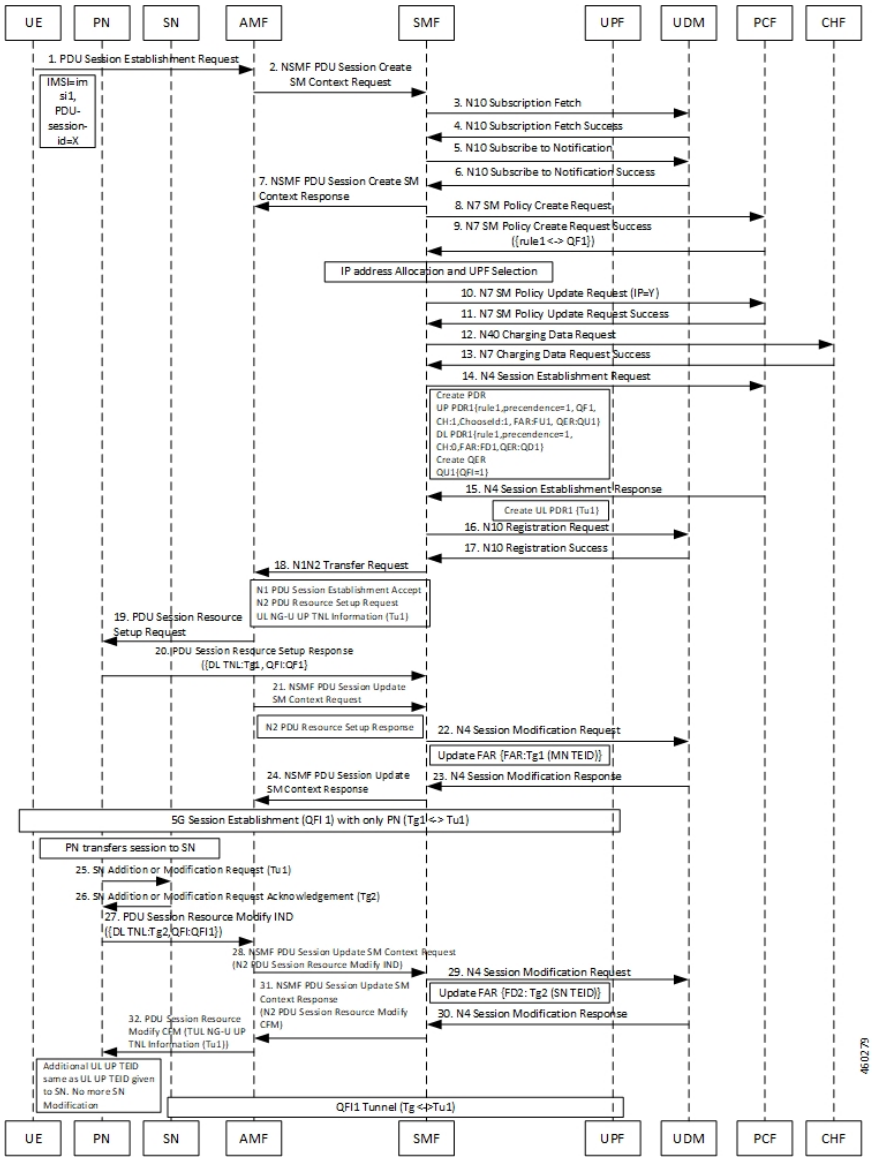
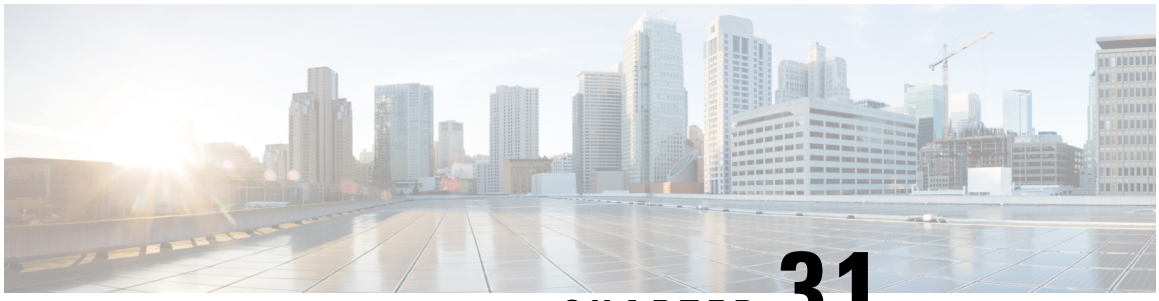


Table 332: RAN-Initiated QoS Flow Offloading Call Flow Description

Step	Description
1	UE sends the PDU Session Establishment Request to AMF.
2	AMF sends the NSMF PDU Session Create SM Context Request to SMF.
3	SMF sends the N10 Registration Request to UDM.
4	UDM sends the N10 Registration successful notification to SMF.
5	SMF sends the N10 subscription fetch message to UDM.

Step	Description
6	UDM sends the N10 subscription fetch successful acknowledgment to SMF.
7	SMF sends the N10 Subscribe to Notification message to UDM.
8	UDM sends the N10 Subscribe to Notification successful notification to SMF.
9	SMF sends the NSMF PDU Session Create SM Context Response to AMF.
10	SMF sends the N7 SM Policy Create Request to PCF.
11	PCF sends the N7 SM Policy Create Request Success notification to SMF.
12	Based on the IP address allocation and UPF selection, SMF sends the N7 SM Policy Update Request to PCF.
13	PCF sends the N7 SM Policy Update Request successful notification to SMF.
14	SMF sends N40 Charging Data Request to CHF.
15	CHF sends the N7 Charging Data Request Success notification to SMF.
16	SMF sends the N4 Session Establishment Request to UPF.
17	UPF sends the N4 Session Establishment Response to SMF.
18	SMF sends the N1N2 Transfer Request to AMF.
19	AMF sends the PDU Session Resource Setup Request to PN.
20	PN sends the PDU Session Resource Setup Response notification with DL tunnel and QFI information to SMF.
21	AMF sends the NSMF PDU Session Update SM Context Request to SMF.
22	SMF sends the N4 Session Modification Request to UPF.
23	UPF sends the N4 Session Modification Response message to SMF.
24	SMF sends the NSMF PDU Session Update SM Context Response to AMF.
25	After the 5G session is established with only PN, PN transfers the session to SN. Then, PN sends the Addition or Modification Request to SN.
26	SN sends the Addition or Modification Request acknowledgment to PN.
27	PN sends the PDU Session Resource Modify Indication message to AMF.
28	AMF sends the NSMF PDU Session Update SM Context Request to SMF.
29	SMF sends the N4 Session Modification Request to UPF.
30	UPF sends the N4 Session Modification Response message to SMF.
31	SMF sends the NSMF PDU Session Update SM Context Response to AMF.

Step	Description
32	AMF sends the PDU Session Resource Modify CFM request to PN. Another UL UP TEID remains same as UL UP TEID that is provided to SN and requires no further modification to SN. QFI1 Tunnel is available from SN to UPF.



CHAPTER 31

NF Discovery and Management

- Feature Summary and Revision History, on page 877
- Feature Description, on page 878
- NF Management, on page 878
- NF Discovery, on page 896
- Static Configuration for Peer NF Management, on page 915
- NRF Failure Handling, on page 920

Feature Summary and Revision History

Summary Data

Table 333: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 334: Revision History

Revision Details	Release
As part of associating NRF management and SMF locality to NRF endpoint, added the message handling profile for NRF.	2023.03.0

Revision Details	Release
As part of the IP pool allocation per slice and DNN feature, added configuration procedures for NRF registration and discovery.	2022.04.0
Added support for the following functionality: • Configurable retry actions for specific error codes. • Flexible options for the retry action associated with an error code. • Httpv2 status code range in the failure handling templates of NFs.	2021.02.0
Introduced support for individual NF Profile member changes through NRF notification. Included the following new parameters as part of the NRF discovery query: • limit • max-payload-size • requester-snssais	2020.03.0
First introduced.	Pre-2020.02.0

Feature Description

The Network Function (NF) Repository Function (NRF) supports the following functionality:

- Maintains the NF profile of available NF instances and their supported services;
- Allows other NF instances to subscribe to, and get notified about, the registration in NRF of new NF instances of a given type;
- Supports service discovery function. It receives NF Discovery Requests from NF instances, and provides the information of the available NF instances fulfilling certain criteria (for example, supporting a given service).

NF Management

Feature Description

This section describes the NF management procedures and their configurations that SMF supports. These procedures are NF registration, NF deregistration, NF heartbeat, and NF Update. The NF registration, update,

and heartbeat are sent from only one of the rest-ep pods, which is the elected primary node. After this nodes is elected, the instance remains as primary node for the NF management activities till the pod crashes or is removed.

NF management supports dynamic configuration change. With this feature, if the configurations were modified in the middle of the transaction or procedure, the ongoing transactions are not impacted.

The dynamic configuration change feature supports the following:

- NRF transaction or procedure picks a configuration version (v1) and uses the same version until the NRF transaction or procedure completes.
- If you change the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is applied in the new transaction.

The dynamic configuration changes apply to the following data structures:

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

Registration

SMF registers with NRF. During registration with NRF, SMF includes at least one of the addressing parameters, such as FQDN, IPv4 or IPv6 address in the NF profile. Including at least one of the addressing parameters in the NF profile registration is mandatory. If SMF supports "https" uri scheme, then SMF provides FQDN in the NFProfile or NFService.

Configuring NRF Endpoints Profile Parameters for NF Management

The SMF provides CLI for configuring NRF endpoints for **nnrf-nfm** (NF Management).

Note For NF management, you can configure only the **nnrf-nfm** service.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. Primary, secondary, and tertiary hosts [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 addresses can be specified. If both are specified, then the IPv4 address is preferred.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

Note In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See the *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

" apiRoot " is a concatenation of the following parts: scheme ("http" or "https")

- fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NRF endpoints for different services supported by NRF, use the following sample configuration.

```
config
  group nrf mgmt mgmt_name
    service type nrf nnrf-nfm
      endpoint-profile epprofile_name
        priority priority_value
        capacity capacity
        api-root api_string
        api-uri-prefix uri_prefix_string
        uri-scheme { http | https }
        endpoint-name ep_name { capacity capacity | primary ip-address
        { ipv4 ipv4_address | ipv6 ipv6_address | port port_num}
        | secondary ip-address { ipv4 ipv4_address | ipv6 ipv6_address
        | port port_num } | tertiary ip-address { ipv4 ipv4_address
        | ipv6ipv6_address | port port_num } }
        version [ uri-version version_num full version version_num ]
        end
```

NOTES:

- **group nrf mgmt** *mgmt_name* : Show the NRF self-management group configurations.
- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specify the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
- **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
- The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
- **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.

- **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
- **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.
- **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.
- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the api/version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the NF Endpoint Profile Parameters for NF Management

Use the **show running-config group nrf** command to verify the NF endpoint profile parameters for NF management.

```
show running-config group nrf
group nrf mgmt mgmt_group
 service type nrf nnrf-nfm
  endpoint-profile epprof
  uri-scheme http
   endpoint-name EP1
   priority       2
   primary ip-address ipv4 209.165.200.231
   primary ip-address port 8082
   secondary ip-address ipv4 209.165.200.232
   secondary ip-address port 8082
 exit
   endpoint-name EP2
      priority 10
       primary ip-address ipv4 209.165.200.231
       primary ip-address port 8082
       secondary ip-address ipv4 209.165.200.232
       secondary ip-address port 8082
     exit
   exit
 exit
exit
```

SMF Deregistration with NRF

Feature Description

The SMF supports the deregistration of Network Function (NF) Repository Function (NRF), wherein the NF deregister service operation of the SMF removes the profile of a network function that is registered in the NRF.

The SMF starts the NF deregister service operation in the following scenarios:

- When the Service Based Interface (SBI) endpoint is not configured and all the rest endpoints stop functioning.
- When all the configured SBI endpoints VIP IP and N11 VIP IPs are offline.

Note SMF can't perform NRF deregistration when all the REST endpoints abruptly stop functioning. Only the REST endpoints can perform registration or deregistration of NRF.

How it Works

The NF deregister service operation deletes the specific resource based on its NF instance ID. The NF deregistration starts when the Uniform Resource Identifier (URI) receives a request to delete a specific NF instance.

The recommended SMF shutdown process involves the following steps:

1. All N11 and SBI VIP IPs are marked as offline. After these endpoints appear offline, the NF deregistration request is sent to the NRF. The NRF notifies the peer NFs, such as AMF, about the SMF shutdown and its unavailability for traffic.
2. Wait for a grace period to allow convergence and perform a "system mode shutdown" to stop all the pods.

When the endpoint SBI is not configured, the system deletes the rest-ep pod immediately and avoids proper convergence. Implementing the system mode shutdown without taking the SBI and N11 VIP IPs offline also avoids convergence.

Call Flows

This section describes the following call flows:

- NRF deregistration call flow
- NRF deregistration trigger events call flow

NF Deregistration Call Flow

This section describes the NF deregistration call flow.

Figure 187: NRF Deregistration Call Flow

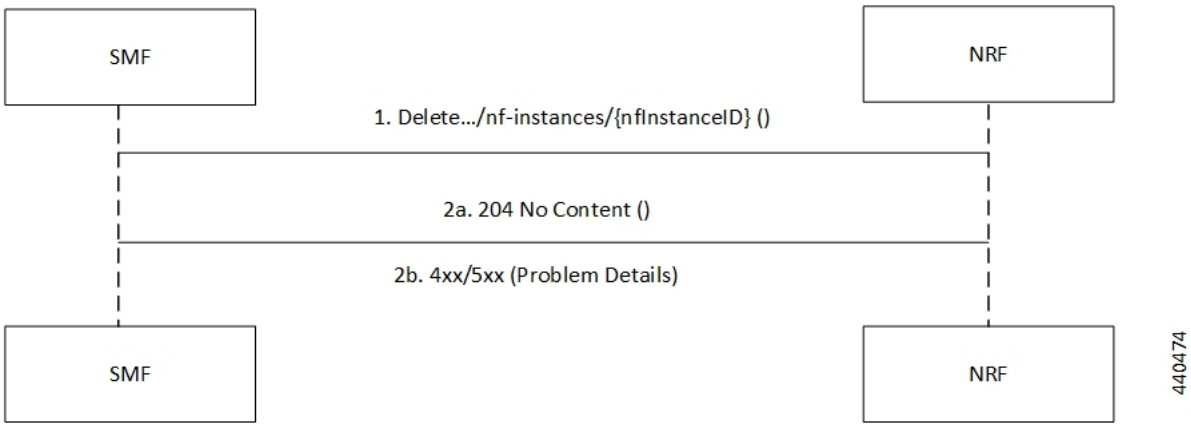


Table 335: NRF Deregistration Call Flow Description

Step	Description
1	The SMF sends a Delete request to the resource URI that indicates the NF instance. The request body is empty.
2a	If the deletion of the specified resource is successful, the "204 No Content" message appears. The response body remains empty.
2b	If the NF instance, which is identified with the NF instance ID, does not exist in the list of registered NF instances in the NRF database, the NRF sends the "404 Not Found" status code with the problem details.

NF Deregistration Trigger Events Call Flow

This section describes the NF deregistration trigger events call flow.

Figure 188: NF Deregistration Trigger Events Call Flow

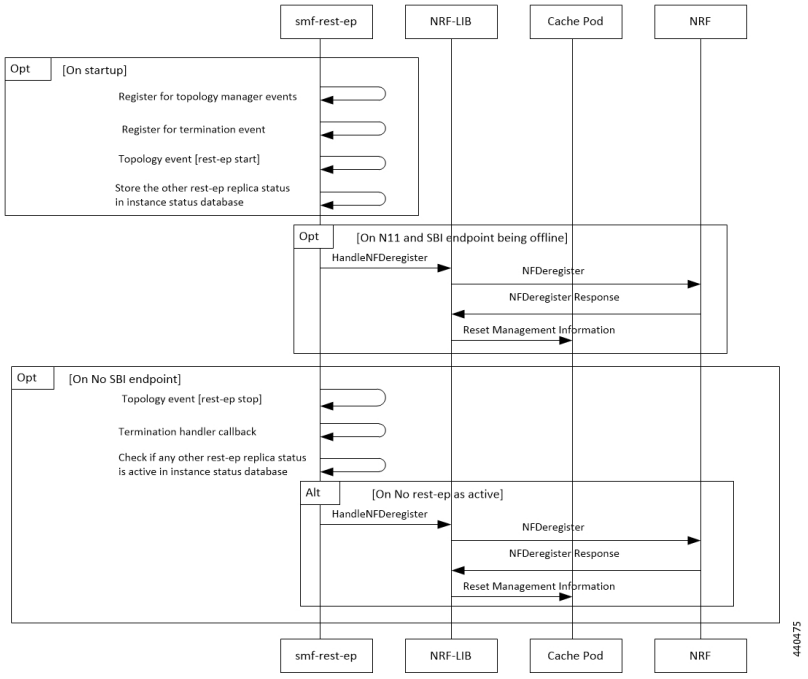


Table 336: NF Deregistration Trigger Events Call Flow Description

Step	Description
On startup	
1	The SMF rest-ep registers for topology manager events to identify the state of other rest-ep instances and keeps a track of these instances in an instance state database.
2	The SMF rest-ep registers for the termination handler with the application infrastructure for receiving notification when the application infrastructure stops functioning. As part of the termination handler, the SMF rest-ep monitors the instance state database for any other working rest-ep.
3	The SMF rest-ep starts the topology event.

Step	Description
4	The SMF rest-ep saves the status of other rest-ep replicas in the instance state database.
When the N11 and SBI endpoints are offline	
5	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
6	When all the SBI and N11 VIP IP endpoints are offline, the SMF rest-ep sends the deregistration request to the NRF.
7	The NRF sends the NF deregister response to the NRF-Lib.
8	The NRF-Lib resets all the management information that is configured in the cache pod.
When no SBI endpoint exists	
9	The SMF rest-ep starts the topology event to stop the other rest-ep.
10	The SMF rest-ep starts the termination handler callback.
11	The SMF rest-ep checks the instance status database for any other working rest-ep.
When no rest-ep is functional	
12	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
13	The SMF rest-ep sends the deregistration request to the NRF.
14	The NRF sends the NF deregistration response to the NRF-Lib.
15	The NRF-Lib resets all the management information that is configured in the cache pod.

Standards Compliance

The SMF deregistration with NRF feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 — 5G System; Network function repository services; Stage 3*

Limitations

The SMF deregistration with NRF feature has the following limitation:

- When N11 and SBI VIP IPs are not marked offline, the NF deregistration is not sent for the system mode shutdown because no specific order for pod deletion exists. In addition, no monitoring procedure exists to check if the rest-ep pods are working.

NF Heartbeat

Feature Description

The NF Heartbeat feature enables the NFs to notify the NRF that the NF is operational. Each NF registered with the NRF contacts the NRF periodically by invoking the NF Update service operation. The time interval at which the NRF is contacted is deployment-specific and is returned by the NRF to the SMF as a result of a successful registration.

SMF sends the NF status and load parameter as part of NF heartbeat to NRF. SMF provides a CLI to configure the interval between periodic NF heartbeat. If the heartbeat value is configured in the NF registration response, the same value is used instead of another configured value.

NF Heartbeat Interval

The SMF NF Heartbeat feature notifies the NRF that the SMF is operational. The default heartbeat interval is once in 10 seconds. With the **heartbeat interval** CLI command, you can configure the interval (in seconds) between the heartbeats. If NRF returns a different heartbeat time value as part of NF registration response or heartbeat response, then the same interval is used for subsequent heartbeats. As part of the heartbeat, NRF sends the HTTP PATCH Request to the resource URI representing the NF instance. The payload body of the PATCH Request contains a "replace" operation on the "nfStatus" attribute of the NF profile of the NF instance, and configures it to the "REGISTERED" value. This release does not support parameters, such as load and capacity.

Note SMF uses the configured heartbeat. If the heartbeat is not configured, SMF uses the locally configured heartbeat.

How it Works

Call Flows

NF Heartbeat Call Flow

The following figure illustrates the NF heartbeat call flow.

Figure 189: NF Heartbeat Call Flow

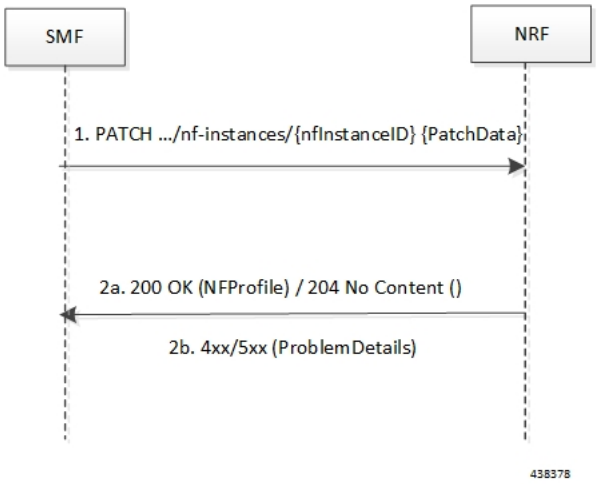


Table 337: NF Heartbeat Call Flow Description

Step	Description
1	The NF Service Consumer sends a PATCH request to the resource URI representing the NF instance. The payload body of the PATCH request contains a replace operation on the nfStatus attribute of the NF Profile of the NF instance, and set it to the value REGISTERED.

Step	Description
2	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body; otherwise, "204 No Content" is returned.
3	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF's database, the NRF returns "404 Not Found" status code with the ProblemDetails IE providing details of the error. Example: **PATCH .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64** **Content-Type: application/json-patch+json** **[** **{"op": "replace", "path": "/nfStatus", "value": "REGISTERED"}** **]** **HTTP/2 204 No Content** **Content-Location:** **.../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64**

Standards Compliance

The NF Heartbeat feature complies with the following standards:

- *3GPP TS 29.510, version 15.4.0 (2019-07) — 5G System; Network function repository services; Stage 3*

Configuring NRF Heartbeat Interval

This section describes how to configure the NRF heartbeat interval.

```
config
  group nf-mgmt nf_mgt_name
    hearbeat interval  hearbeat_interval
  end
```

NOTES:

- **group nf-mgmt** *nf_mgt_name*: Specify the group name of NF management.
- **hearbeat interval** *hearbeat_interval*: Specify the interval of hearbeat between the heartbeats. The value of heartbeat interval is in seconds.

Note If NRF returns a different heartbeat interval value as part of NF registration response or heartbeat response, the same value is used for subsequent heartbeats.

NRF Support for SMF Subscription and Notification

Feature Description

The SMF uses the NRF-provided Subscription service to subscribe to NF status changes that the NF receives as a discovery response. This feature helps in updating the cached NF discovery responses.

The SMF honors only the notification changes in load, capacity, status at the NF level, and at the service level. It ignores all other parameter changes in the notification.

After the successful subscription for notification service, the SMF receives notifications of registration and deregistration of NF Instances, or notifications of NF profile changes for a given NF Instance.

The SMF supports the "NFProfile" field and "ChangeItem" field in the "NotificationData". If the notification event type is set to "NF_PROFILE_CHANGED", the SMF receives notification about the profile-level changes or a list of individual change items for the NFProfile parameters along with nfInstanceUri.

The "ChangeItem" field includes the following parameters:

- op—Indicates the type of change that happens to the resource.
- path—Contains the JSON pointer value which indicates the target location within the resource.
- from—Indicates the path of the JSON element that is moved or copied to the location indicated by the "path" attribute. It is present if the "op" attribute is of value "MOVE".
- origValue—Indicates the original value at the target location within the resource specified in the "path" attribute.
- newValue—Indicates a new value at the target location within the resource specified in the "path" attribute.

Note The SMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter.

The following is an example of the notification payload sent from the NRF when an NF instance has changed its profile by updating the IP address value and the TCP port for the first endpoint of the first NF service.

Example 1:

```
{
  "event": "NF_PROFILE_CHANGED",
  "nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
  "profileChanges": [
    {
      "op": "REPLACE",
     "path": "/nfServices/0/ipEndPoints/0/ipAddress", ===> Change ipAddress to ipv4Address

      "newValue": "209.165.201.10"
    },
    {
      "op": "REPLACE",
      "path": "/nfServices/0/ipEndPoints/0/port",
      "newValue": 8080
    }
  ]
```

Example 2:

```
{
"event": "NF_PROFILE_CHANGED",
"nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
"nfProfile": <Newly updated complete profile>
}
```

How it Works

This feature uses the NF Subscribe service to subscribe to changes on the status of NF instances that the NF receives as discovery responses. The SMF sends a subscription for the response validity period for each of the NF profiles that it receives in the discovery response. The SMF checks if an existing NF instance subscription time needs an extension or not depending on the current response time validity. If a subscription needs an extension, a subscription PATCH is sent with the extended validity time.

During subscription, the NRF may respond with a modified validity time. This validity time might differ from the SMF validity time request. In such a scenario, the SMF tracks the required subscription time and the actual subscription time returned by the NRF.

The SMF periodically (every two minutes) checks in database if there is any subscription with the actual subscription time ending soon (as in next five minutes) but has required validity time more than the actual validity time. In this scenario, the SMF sends a PATCH subscription to extend the subscription validity time.

The SMF fills the Status Notification URI based on the interface NRF configuration that is specified in the configuration. The notification VIP IP and VIP port are used to frame the status notification URI.

```
http://{nrfinterface.vip-ip}:{ nrfinterface.vip-port}/{notifResourceURI}
```

On status notification, the SMF updates the local cache and the external cache (cache pod) with the changed attributes.

Call Flows

This section describes the call flows for the SMF Subscription and Notification feature.

Subscription (PATCH) Call Flow

The NRF updates the subscription to notifications on NF instances to refresh the validity time, when the specified time is due to expire. The SMF can request a new validity time to the NRF. If the operation is successful, the NRF can assign and provide a new validity time to the NF.

Updating the "subscriptionID" resource, initiates the Subscription (PATCH) operation. The operation starts on issuing an HTTP PATCH request on the URI representing the individual resource.

The following figure illustrates the call flow for subscription to NF instances in the same PLMN.

Figure 190: Subscription (PATCH) Call Flow

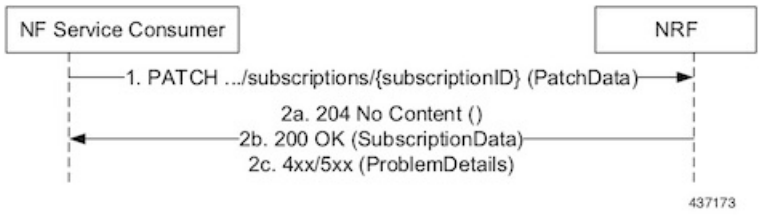


Table 338: Subscription (PATCH) Call Flow

Step	Description
1	The SMF sends a PATCH request to the resource URI identifying the individual subscription resource. The payload body of the PATCH request contains a "replace" operation on the "validityTime" attribute of the SubscriptionData structure. The request also contains a new suggested value for the "validityTime" attribute. This replace operation does not replace any other attribute of the resource.
2a	When a subscription is successful, the NRF sends a "204 No Content" response. This response indicates that the NRF accepts: • Extension of the subscription lifetime • Value of the "validityTime" attribute
2b	If the subscription fails due to errors in the JSON Patch object in the request body, the NRF returns a "400 Bad Request" status code with the problem details.

2c	If the subscription fails due to internal errors in the NRF, the NRF returns a "500 Internal Server Error" with the problem details.
	Example:
	`PATCH .../subscriptions/2a58bf47`
	`Content-Type: application/json-patch+json`
	`[`
	`{ "op": "replace", "path": "/validityTime", "value": "2018-12-30T23:20:50Z" },`
	`]`

Subscription (POST) Call Flow

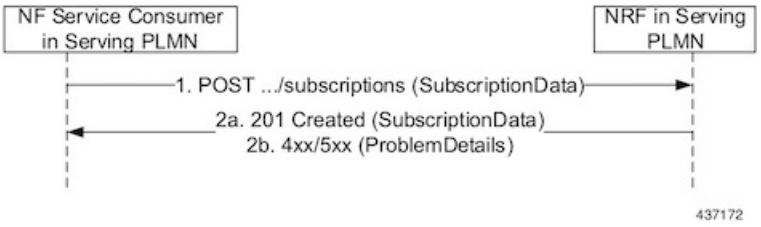
The Subscription service operation allows to:

- Create a subscription so that the SMF can request notification (depending on certain filters) in the following scenarios:
  - When there is a registration or deregistration in the NRF.
  - When there is a modification to a profile.
- Create a subscription to a specific NF instance such that the SMF can request notification in the following scenarios:
  - When there is a modification to an NF instance.
  - When there is a deregistration of an NF instance.

Important Currently, SMF only supports subscription of NF instances that the NF receives as its discovery response.

The following figure illustrates the call flow for subscription to NF instances in the same PLMN.

Figure 191: Subscription (POST) Call Flow



Implementing the subscription to notifications on NF instances creates a new individual resource under the collection resource "subscriptions." Issuing a POST request starts the operation on the Uniform Resource Identifier (URI) representing the "subscriptions" resource.

Table 339: Subscription (POST) Call Flow Description

Step	Description
1	The NF Service Consumer sends a POST request to the resource URI representing the "subscriptions" collection resource. The request body includes data that indicates the type of notifications that the SMF has subscribed to receive. It also contains a callback URI, where the SMF prepares to receive the actual notification from the NRF. The notification contains the SMF suggested validity time, which represents the time span during which the subscription remains active. The subscription request may also include more parameters indicating the list of attributes in the NF Profile to monitor (or to exclude from monitoring). This request determines if the NRF must send a notification, when there is a change in any of the profile attributes.
2a	When a subscription is successful, the NRF sends a "201 Created" response. This response contains newly created subscription data that includes the NRF-determined validity time beyond which, the subscription is invalid. When the subscription expires, the SMF creates a new subscription in the NRF to continue receiving status notifications.
2b	If the subscription fails due to errors in the subscription data, the NRF returns a "400 Bad Request" status code with the problem details. If the subscription fails due to internal errors in the NRF, the NRF returns a "500 Internal Server Error" with the problem details.

NFStatus Notify Call Flow

When a POST request is issued to each callback URI of the various subscribed NF instances, the SMF initiates the NFStatus Notify operator.

The following figure illustrates the NFStatus Notify call flow.

Figure 192: NFStatus Notify Call Flow

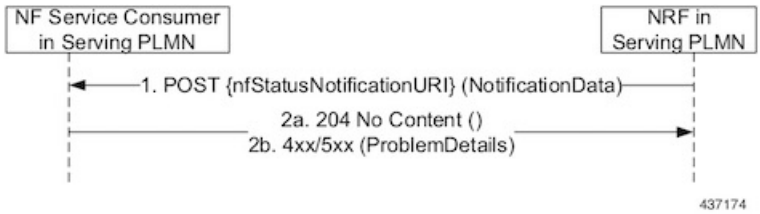


Table 340: NFStatus Notify Call Flow Description

Step	Description

1	The NRF sends a POST request to the callback URI.
	The request body for a profile change notification request includes the following:
	• **event**—This attribute indicates the notification type. It can be one of the following:
	  • NF_REGISTERED
	  • NF_DEREGISTERED
	  • NF_PROFILE_CHANGED
	• **nfInstanceUri**—Uniform Resource Identifier (URI) of the NF instance associated to the notification event.
	• **nfProfile**—Indicates the new or updated NF profile.
	• **profileChanges**—This attribute identifies changes on the profile of the NF instance associated to the notification event. This attribute is available when the event notification type is "NF_PROFILE_CHANGED".

2a	When the notification is successful, the NRF sends a "204 No content" response.
2b	If the SMF disregards "nfStatusNotificationURI" as a valid notification URI, the SMF returns a "404 Not Found" status code with the problem details. For example, if the URI does not belong to any of the existing subscriptions that the SMF has created in the NRF.

Limitations

This feature has the following limitations:

- NF status notification supports only NF profile load, NF profile capacity, NF profile status, service load, service capacity, and service status parameter changes.
- SMF supports only the NFPofiile field in the "NotificationData." It does not support the "Change item" field.
- The SMF supports notification of the following parameter changes:
  - nfProfile
    - nfStatus
    - ipv4Address

- ipv6Address
- priority
- capacity
- load

- nfService
  - version

Note Change to a new version is permitted but not the deletion and modification of the existing version.

  - scheme

Note Currently, http is only supported

  - nfServiceStatus
  - ipEndPoints
  - apiPrefix
  - capacity
  - load
  - priority

- The SMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter in the "ChangeItem" field.

Configuring NRF for Subscription and Notification

This section describes how to configure the NRF for subscription and notification.

Note For the subscription and notification to work, it is mandatory to configure the NRF interface within SBI interface.

When discovery is done with NRF, a subscription message for the discovered NF instances is sent. The SMF fills the Status Notification URL based on the NRF interface configuration that is specified in the configuration. The notification VIP IP and VIP port are used to frame the status notification URL. The SMF uses the URL that is included in the subscription request message for status notifications.

To configure the NRF interface, vip-ip, vip-port, and loopback port to open the server endpoints for the NF status notification, use the following sample configuration.

```
config
  instance instance-id gr_instance_id
    endpoint sbi
      replicas replica_num
        vip-ip ip_address
      interface nrf
        vip-ip ip_address
        vip-port port_number
        loopbackPort port_number
        end
```

NOTES:

- **interface nrf**: Specify the interface as NRF.
- **vip-ip** *ip_address*: Specify the virtual IP address of the virtual host. The SMF uses this as the listening IP address for the status notification.
- **vip-port** *port_number*: Specify the port number of the virtual host. The SMF uses this as the listening port for the status notification.
- **loopbackPort** *port_number*: Specify the internal port number of the loopback host. The SMF uses this port for the NF status notification.

NF Profile Update

Feature Description

The SMF invokes the NF Update service operation when there are changes to the NF registration parameters due to the SMF profile configuration change.

The NF Update service updates the NF profile that was previously registered in the NRF by providing the updated profile of the requesting NF to the NRF.

The update operation can be one of the following:

- A whole NF profile update (complete replacement of the existing profile with a new profile)
- An update to only a subset of the NF profile parameters (adding, deleting, or replacing services to the NF profile)

How it Works

This section describes the NF profile update procedure.

Call Flows

This section describes the following call flows:

- NF Profile Complete Replacement Call Flow, on page 894
- NF Registration and NF Update Call Flow, on page 894

NF Profile Complete Replacement Call Flow

The following figure illustrates a call flow representing the complete NF profile replacement.

Figure 193: NF Profile Complete Replacement

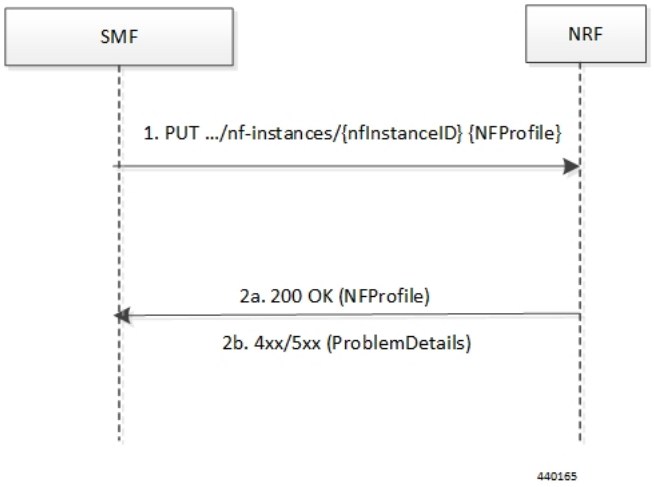


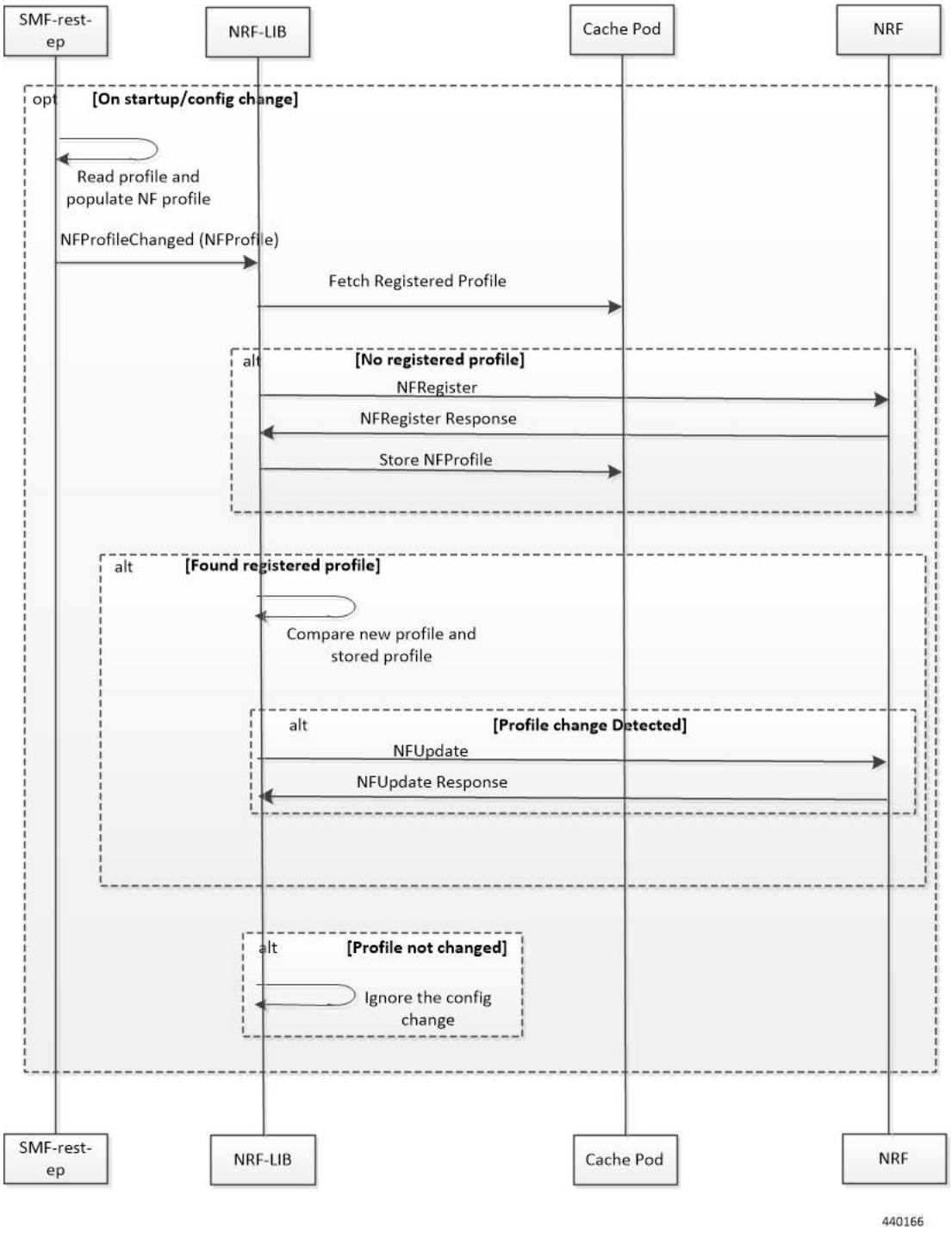
Table 341: NF Profile Complete Replacement Call Flow Description

Step	Description
1	The SMF sends a PUT request to the resource URI representing the NF instance. The payload body of the PUT request contains an update operation on the NF Profile of the NF instance.
2a	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body.
2b	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF database, the NRF returns 4xx or 5xx status code with the ProblemDetails IE providing details of the error.

NF Registration and NF Update Call Flow

The following figure illustrates the call flow representing the NF registration and NF update messaging from SMF on NF profile change trigger from REST-EP.

Figure 194: NF Registration and NF Update Call Flow



1. The SMF REST-EP, on start-up, reads the SMF profile configuration and accordingly populates the NF management profile. The REST-EP then triggers SMF to indicate the NF Profile change.
2. The SMF maintains the NF registration status and the registered profile in an external cache pod. The SMF detects whether the NF registration with NRF is completed. If the SMF detects that the registration

is not completed during NF profile change handling, perform Step 3. If the NF registration is complete, perform Step 4.

3. The SMF sends NF Register to NRF. It allows an NF instance to register its NF profile in the NRF. It includes the registration of the general parameters of the NF instance along with the list of services exposed by the NF instance.
4. The SMF fetches the registered NF profile and then compares it with the new profile.
5. The SMF sends NF update (PUT) request to the NRF when any of the parameters in the NF management profile changes due to SMF profile configuration change.

   Load parameter is not set as part of the PUT message. Heartbeat is set as the current active heartbeat interval.
6. The SMF ignores the trigger if there is no change detected.

Important The NF update is sent only from the elected SMF.

Standards Compliance

The NF Profile Update feature complies with the following standards:

- *3GPP TS 29.510, Version 15.4.0 (2019-07) – 5G System; Network function repository services; Stage 3*

Limitations

The NF Profile Update feature has the following limitation:

- Supports only the complete replacement of NF profile.
- Doesn't support capacity.

NF Discovery

Feature Description

The SMF uses the NRF-provided, NF discovery service to discover network functions (NFs), such as Access and Mobile Function (AMF), Unified Data Management (UDM), and Policy Control Function (PCF). The SMF configures the preferred locality as provided in the "profile nf-pair" configuration of Network Repository Function (NRF) in the discovery query.

For each NF, the query parameters, also known as filters, are configurable. Based on these parameters, NRF returns all the NFs matching the query criteria for the SMF to discover NF profiles.

Note The NF discovery and load-balancing capabilities are available only for UDM, PCF, CHF, and AMF.

NF discovery supports dynamic configuration change. With this feature, if the configurations were modified in the middle of the transaction or procedure, the ongoing transactions are not impacted.

The dynamic configuration change feature supports the following:

- NRF transaction or procedure picks a configuration version (v1) and uses the same version until the NRF transaction or procedure completes.
- If you change the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is applied in the new transaction.

The dynamic configuration changes apply to the following data structures:

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

How it Works

The service operation is executed by querying the "nf-instances" resource. The request is sent to an NRF in the same PLMN of the SMF.

Call Flows

This section describes the call flow associated with this feature.

Service Discovery Request Call Flow

This section describes the service discovery request call flow.

Figure 195: Service Discovery Request Call Flow

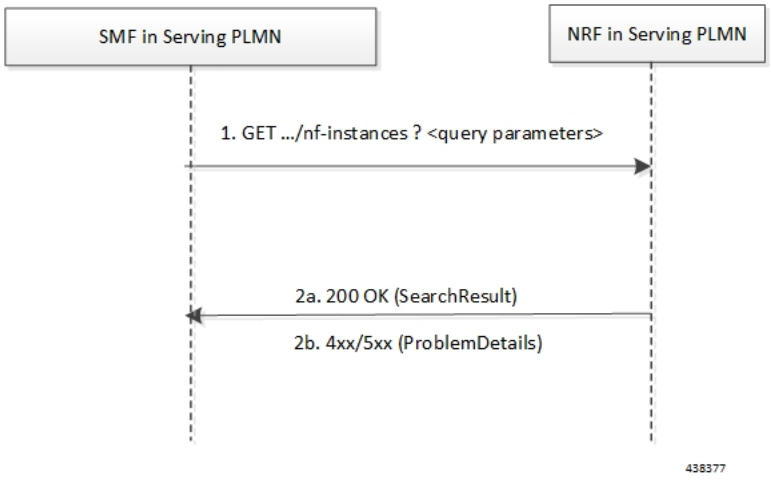


Table 342: Service Discovery Request Call Flow Description

Step	Description
1	The SMF sends an HTTP GET request to the resource URI "nf-instances" collection resource. The input filter criteria for the discovery request exists in query parameters.
2a	On success, "200 OK" is returned. The response body contains a validity period, during which the SMF caches the search result, and an array of NF profile object that satisfy the search filter criteria. For example, all NF instances displaying a certain NF Service name.
2b	If the SMF is not allowed to discover the NF services for the requested NF type provided in the query parameters, the NRF returns "403 Forbidden" response. If the discovery request fails at the NRF due to errors in the input data in the URI query parameters, the NRF returns "400 Bad Request" status code with the "ProblemDetails" IE providing details of the error. If the discovery request fails at the NRF due to NRF internal errors, the NRF returns "500 Internal Server Error" status code with the "ProblemDetails" IE providing details of the error.

The NF profile objects that are returned in a successful result contains generic data of each NF instance, applicable to any NF type. These objects can also contain NF-specific data, for those NF instances belonging to a specific type (for example, the attribute "udrInfo" exists in the NF profile when the type of the NF instance takes the "UDR" value). In addition, the attribute "customInfo" exists in the NF profile for NF instances with custom NF types. For NF instances, the NRF returns the "customInfo" attribute, if available, as part of the NF profiles returned in the discovery response.

The SMF service communicates with different NFs, such as UDM, AMF, PCF, and CHF, when the session is active. The NF discovery is based on set of filters, also called query parameters, which are associated with the session. The SMF service discovers the NFs, matching the filter criteria for the session, to send messages to NF.

The SMF supports the following filters:

- Dnn
- Tai
- TargetNfFqdn
- TargetPlmnList
- TargetNfInstanceId
- Snssais
- Preferred locality

The discovered NFs are cached with the filter as the key. The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters. The NF discovery response carries a validity time, which decides the cache validity period.

SMF sends the messages to a target based on the Location header URL in response to initial messages sent to NF.

SMF supports stickiness wherein the endpoint, service instance, and NF instance details of the selected endpoint for a message that is sent, will be provided to the application or REST-EP so that the same can be specified

in subsequent message (instead of discovery filter). This operation helps in maintaining stickiness for a session to the selected NF.

Standards Compliance

The NF Discovery feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 (2019-07) – 5G; 5G System; Network function repository services; Stage 3*

Limitations

The NRF Discovery feature has the following limitations:

- The cache maintained is local to the library. In case of deployment with multiple replicas of REST-EP, if two Discovery or Send messages with the same discovery filter land on different pods, then both the pods trigger NF discovery.
- This feature supports only the UDM, PCF, CHF, and AMF discovery, and load balancing. It does not support UPF discovery.

Configuring NRF for Discovery

This section provides the configurations that are required to perform the NF discovery.

Registering NRF

To register an NRF, use the following sample configuration.

```
config
nssai name nssai_name
    sst sst ssd ssd
    dnn dnn_name_value
    end
```

NOTES:

- **nssai name** *nssai_name*: Configure the NSSAI name value for the slice. The *nssai_name* value must be a string.

Note SMF supports a maximum of 512 slices to be sent toward NRF.

Configuration Example

The following is an example configuration of the NRF registration.

```
nssai name slice1
 sst 02
 sdt Abf123
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
intershat7 starosupf ]
exit
```

```
nssai name slice2
 sst 02
 sdt Abf124
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
intershat7 starosupf ]
exit
```

Discovering NRF

To configure the NRF discovery, use the following sample configuration:

```
config
  profile network-element [ amf amf_profile_name| chf chf_profile_name | pcf
pcf_profile_name | udm udm_profile_name | upf upf_profile_name ]
     query-params requester-snssais
     exit
```

NOTES:

- **query-params requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.

Configuration Example

The following is an example configuration.

```
config
   profile network-element udm udm1
      query-params requester-snssais
      exit
   profile network-element pcf pcf1
      query-params requester-snssais
      exit
   profile network-element chf chf1
      query-params requester-snssais
      exit
   profile network-element upf upf1
      query-params requester-snssais
      exit
   profile network-element amf amf1
      query-params requester-snssais
      exit
```

Configuring NF Client Profile

To configure the NF endpoints for AMF, CHF, PCF, and UDM, use the following sample configuration:

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
  end
```

NOTES:

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**: Specify the required NF client profiles and provide the local configuration for any of the following configured NFs:
  - **amf**: Enable the AMF local configuration
  - **chf**: Enable the CHF local configuration

- **pcf**: Enable the AMF local configuration
- **udm**: Enable the AMF local configuration

  For example, if you are configuring the **amf amf-profile** keyword, this command enables the AMF local configuration. The same approach applies for the other configured NFs.

  nf_profile_name must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable the configuration, use the **no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** command.

Configuration Example

The following is an example configuration.

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
  exit
exit
exit
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

Associating a Discovery Group with NF Type

To pair a discovery group with NF types, use the following sample configuration.

```
config
  profile nf-pair nf-type nf_type
    nrf-discovery-group nrfdisc_group_name
    end
```

NOTES:

- **nf-type** *nf_type*: Specify the NF client type value as SMF.
- **nrf-discovery-group** *nrfdisc_group_name*: Specify the NRF discovery group name. Discovery group is the logical link to the NRF endpoint groups (nrf-group). For each NF type, you can associate a discovery group and the locality information.

Configuring NF Endpoint Profile Parameters in NRF Discovery Group

The SMF provides CLI for configuring NF endpoints for **nnrf-nfd** (NF discovery).

Note For a discovery group, you can configure only the **nnrf-disc** service.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the SMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

Primary, secondary, and tertiary hosts [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 addresses can be specified. If both are specified, then the IPv4 address is preferred.

SMF provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, the structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot is a concatenation of the following parts:

- scheme ("http" or "https")

Note Both HTTP and HTTPS scheme URIs are allowed. See the *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

- fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NRF endpoints for different services supported by NRF, use the following sample configuration:

```
config
   group nrf discovery discovery_name
      service type nrf nnrf-disc
         endpoint-profile
            name  epprofile_name
            api-root api_string
            api-uri-prefix uri_prefix_string
            uri-scheme { http | https }
            endpoint-name ep_name { capacity capacity | primary ip-address {
ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | secondary ip-address {
 ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address
{ ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
            version [ uri-version version_num full version version_num ]
            end
```

NOTES:

- **group nrf discovery** *discovery_name* : Configure the NRF discovery group.
- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
  - The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.
  - **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.
- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the API URI version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the NRF Endpoints Profile Parameters for NF Discovery

This section describes how to verify the configuration of the NRF endpoints profile parameters.

```
show running-config group nrf
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity       10
   priority       1
   api-uri-prefix nudm-sdm
   api-root       root
   uri-scheme     http
   version
    uri-version v1
     full-version 209.165.200.225
    exit
   exit
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 3021
   exit
  exit
 exit
exit
```

Configuring Locality for NF Types

The SMF provides locality aware NF discovery.

A pair profile has the locality values configured with NF type as SMF. A locality has the following values:

- client—Specify the client locality information.
- geo-server—Specify the geo-service locality information.
- preferred-server—Specify the preferred server locality information.

For a profile selection, only the preferred-server and geo-server locality values are considered. Following are the scenarios of these locality values configuration:

- If both the preferred-server and geo-server locality values are configured, then the profiles, which exist in discovery response, matching these locality values are selected. In addition, the profiles with empty locality value are selected. Any other profile with locality other than preferred-server and geo-server locality values are not considered.
- If only the preferred-server locality value is configured, then the profiles, which exist in discovery response, matching this value is selected. In addition, the profiles with an empty locality value are selected. Any other profile with locality other than preferred-server locality value is not considered.
- If only geo-server locality value is configured then the profiles, which exist in discovery response, matching this geo-server locality value is selected. In addition, the profiles with empty locality value is selected. Any other profile with locality other than geo-server locality value is not considered.
- If both preferred-server and geo-server locality values are not configured then all the profiles, which exist in discovery response, are selected.

To configure the locality for NF types, use the following sample configuration.

```
config
  profile nf-pair nf-type nf_type
    locality { client client_name | geo-server geoserver_name | preferred-server
 prefserver_name }
     end
```

NOTES:

- **client** *client_name*: Specify the client locality information. Client locality is the SMF's locality and is a mandatory parameter.
- **preferred-server** *prefserver_name*: Specify the preferred server locality information. The preferred server locality is the locality that should be considered as the locality of preference during the corresponding NF discovery.
- **geo-server** *geoserver_name*: Specify the geo-server locality information. The geo-server locality is the geo redundant site for the preferred locality and is generally used as the next best server locality after preferred locality, during NF discovery.

Note **geo-server** *geoserver_name* is not fully qualified.

Verifying the Association of the Discovery Group and Locality Configuration

This section describes how to verify the discovery group association and locality configuration for NF.

```
show running-config profile nf-pair
profile nf-pair nf-type UDM
 nrf-discovery-group DISC1
 locality client LOC1
 locality preferred-server PREF_LOC
 locality geo-server GEO
exit
```

Configuring Locality for SMF

To configure the locality for SMF, use the following sample configuration.

This is a mandatory configuration if the SMF performs the NF discovery using the NRF.

```
config
  profile smf smf_profile_name
     locality value
     end
```

NOTES:

- **locality** *value*: Specify the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

To configure the NF profile that the configured Data Network Name (DNN) uses, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | udm } nf_profile_name
    end
```

NOTES:

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*: Specify one or more NF types, such as AMF, CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable the configuration, use the **no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* command.

Defining Locality within NF Profile

This section describes how to define the locality of the NF endpoints. For the NF endpoint selection, the SMF first considers the preferred locality that is configured with the **profile nf-pair** CLI command. The admin determines the preferred locality based on the proximity of the locality and the network function. The SMF then uses the geo-server locality configurations as the next preferred locality for the NF discovery. For information on the **profile nf-pair** command, see Configuring Locality for NF Types, on page 904 in the NRF Selection per Peer NF Type, on page 909 section.

The SMF selects the other locality endpoints if the **profile nf-pair** CLI command does not include the preferred server locality configuration, or if the **profile nf-client** CLI command does not include the endpoint configured with the preferred server or geo-server locality. For the other locality endpoint selection, the SMF uses the **priority** configuration within the **locality** CLI command.

To define the locality of the NF endpoints, use the following sample configuration.

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
    locality locality_name [ priority priority | service name type service_types
 { endpoint-profile epprofile_name } ]
    end
```

NOTES:

- **locality** *locality_name*: Specify the locality of the NF endpoint. The SMF uses the locality configurations (that is, the preferred server locality and geo-server locality) to select the appropriate NF endpoints.
- **priority** *priority*: Specify the priority for the locality configuration.
- **service name type** *service_types*: Specify the configured NF service types. The service types vary depending on the configured service.

  The AMF service supports the following service types:

  - namf-comm
  - namf-evts
  - namf-loc

- namf-mt

The CHF service supports the following service types:

- nchf-convergedcharging
- nchf-spendinglimitcontrol

The PCF service supports the following service types:

- npcf-am-policy-control
- npcf-bdtpolicycontrol
- npcf-eventexposure
- npcf-policyauthorization
- npcf-smpolicycontrol
- npcf-ue-policy-control

The UDM service supports the following service types:

- nudm-ee
- nudm-pp
- nudm-sdm
- nudm-ueau
- nudm-uecm

- **endpoint-profile** *epprofile_name*: Specify the endpoints at a per NF service level. The NF specific services are available within the locality configuration.
- You can configure multiple endpoints per profile name for the configured NF.

Configuring NF Endpoint Profile Parameters in NF Client Profile

This section describes how to configure the NF endpoint profiles within the service and its associated parameters.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the SMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

SMF provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, the structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot is a concatenation of the following parts:

- scheme ("http" or "https")

Important Both HTTP and HTTPS scheme URIs are allowed. See *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

- fixed string "://"
- authority (host and optional port) as defined in *IETF RFC 3986*
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NF endpoint profiles within the service and its associated parameters, use the following sample configuration:

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile }  nf_profile_name }
     locality locality_name [ priority priority | service name type service_type
 ]
        endpoint-profile epprofile_name
           api-root api_string
           api-uri-prefix uri_prefix_string
           capacity capacity
           endpoint-name ep_name { capacity capacity | primary ip-address {
ipv4 ipv4_address | ipv6 ipv6_address | port port_num }| secondary ip-address {
ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address {
 ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
           priority priority_value
           uri-scheme { http | https }
           version [ uri-version version_num full version version_num ]
           end
```

NOTES:

- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specify the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0–65535.

    The endpoint selection for sending the message is based on probabilistic load balancing algorithm (*IETF RFC 2782*) using the priority and capacity parameters.

- **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.
- **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
- **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.

- **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load balancing logic. *priority* must be an integer in the range 0–65535.
- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the API URI version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

NRF Selection per Peer NF Type

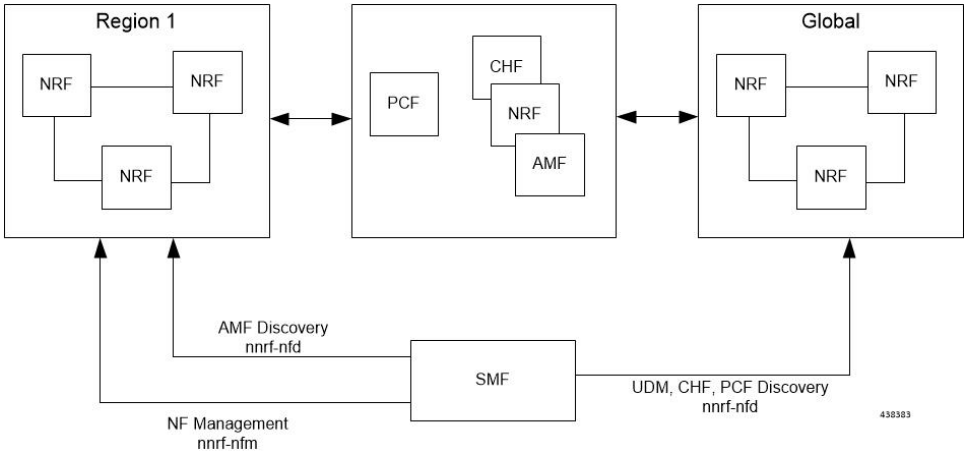
Feature Description

The Network Repository Function (NRF) deployment can be logically segmented as global, regional, and so on, for a reliable network management. You can accomplish this segmentation by specifying different NRF endpoint groups for the discovery of different network functions.

For example, the SMF interacts with Region 1 NRF endpoints for management and AMF discovery. For UDM, CHF, and PCF discovery, the SMF communicates with the global NRF endpoints.

The following figure illustrates the NRF deployment.

Figure 196: NRF Deployment



Standards Compliance

This feature complies with the following standard:

- *3GPP TS 29.510 version 15.4.0—5G System; Network function repository services; Stage 3*

Configuring the NRF Selection per Peer NF Type

This section describes how to configure the NRF selection per peer NF type.

Associating NRF Management and SMF Locality to NRF Endpoint

To configure the NRF management (nrf-group) and SMF locality, and associate them to NRF endpoint, use the following sample configuration.

```
config
  group nf-mgmt mgmt_name
    nrf-mgmt-group nrf_group_name
    locality locality_name
    message-handling-profile message_handling_profile_name
    end
```

NOTES:

- **nrf-mgmt-group** *nrf_group_name*: Specify the NRF management group.
- **locality** *locality_name*: Specify the locality information.
- **message-handling-profile** *message_handling_profile_name*: Specify the message handling profile for NRF.

Verifying the Association of the NRF Management and SMF Locality to NRF Endpoint

This section describes how to verify the configuration that associates the NRF management and SMF locality to NRF endpoint.

```
show running-config group nf-mgmt
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
```

Configuring Locality for SMF

To configure the locality for SMF, use the following sample configuration.

This is a mandatory configuration if the SMF performs NF discovery using the NRF.

```
config
  profile smf smf_profile_name
    locality value
    end
```

NOTES:

- **locality** *value*: Specify the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable the configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

To configure the NF profile used by the configured Data Network Name (DNN), use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | udm } nf_profile_name
    end
```

NOTES:

- **network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name*: Specify one or more NF types, such as AMF, CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable the configuration, use the **no network-element-profiles { amf | chf | pcf | udm }** *nf_profile_name* command.

Configuring Network Element Profile Parameters for the NF

To configure the network element profile parameters for the configured NF, use the following sample configuration.

```
config
  profile network-element { { amf | chf | pcf | udm } nf_profile_name }
    nf-client-profile profile_name
    query-params { dnn | limit | max-payload-size | requester-snssais |
 supi | tai | target-nf-instance-id | target-plmn }
    end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**: Specify one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specify the DNN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specify the limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specify the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specify the SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specify the TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specify the target NF instance identifier as the query parameter in the NF discovery request towards the NRF.

- **target-plmn**: Specify the target PLMN as the query parameter in the NF discovery request towards the NRF.

- This is an optional configuration. By default, the CLI commands are disabled.
- To disable this configuration, use the **no** variant of these commands. For example, **no nf-client-profile** CLI command.

Verifying the Local Configuration for the NRF Interface Per Endpoint

This section describes how to verify the configuration for the NRF interface per endpoint.

The following is an example of the NRF endpoint configuration.

```
show running-config profile dnn cisco
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit

profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 209.165.200.227
 bind-port        8008
instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

Caching for Discovered NF Profiles

Feature Description

The SMF provides caching support for discovered caching profiles. It uses the NF discovery (nnrf-disc) function to discover profiles, such as AMF, UDM, PCF, and CHF. The received discovery response is associated with validity time. SMF caches the discovery response and uses the same response for future NF selections until the cache is valid. This caching support helps in reducing the number of NRF interactions during an ongoing session.

Relationships

Caching support for NF Discovery has functional relationship with the following features:

- NRF Support for SMF Subscription and Notification
- NRF Selection per Peer NF Type

How it Works

The SMF maintains the cache data in a cache pod. It uses the cache pod to share the NF discovery cache across multiple instances of SBI pods. The SBI pod periodically updates the cache pod on receiving an NF discovery response. All SBI pods refresh its cache data periodically with the help of the cache pod.

If a message is sent to an NF that meets a specific criterion, the SMF looks up the cache data for further processing. During a cache lookup:

- On a cache hit without an expired entry, the selected cached NF response sends a message for an endpoint selection.
- On a cache hit with an expired entry, the SMF sends NF discovery requests to the NRF to fetch a new list of NF discovery responses.
- If there is a cache miss, the SMF sends NF discovery request to the NRF to retrieve a new list of NF discovery responses.

Call Flows

Cache Lookup Call Flow

This section describes the call flow for Cache Lookup.

SMF maintains a local cache and updates the external cache (cache-pod). The key for a cache is a combination of nfType and filter, which is a string that is prepared from multiple filter parameters in "key1=value, key2=value2" format.

On startup, SMF retrieves all the cache entries that were modified since epoch from cache-pod so that it can build the local cache. After the local cache is built, the same cache is used in the send message flow for lookup. A periodic refresh routine is initiated to refresh the local cache using the cache-pod. Local cache is periodically refreshed by getting all records from the cache-pod that were modified since last refresh. The resultant record list is traversed and the local cache is updated.

When smf-rest-ep (SBI) triggers a send message to UDM, the SMF looks up the local cache for the cache entry with the nfType and filter key. The NF profiles are load-balanced and a message is sent to the selected endpoint.

Standards Compliance

This feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 — 5G System; Network function repository services; Stage 3*

NF Discovery Cache Invalidation

Feature Description

SMF gives higher priority to the NFs that are discovered from NRF over the locally configured NFs. SMF uses the locally configured NFs only if the NRF endpoints are not configured or if no NFs are available as part of the NF discovery response. This response appears after the query filter criteria are met. Each NF discovery response has an associated validity time and SMF caches the NF discovery response, uses the cache for subsequent session activation. SMF performs NF discovery only if matching entries are unavailable for the query filter in its NF discovery response cache or if the entry in cache exists, however with the expired validity.

How it Works

SMF provides configuration to determine the behaviour when the NRF is unreachable and has an expired cache entry. The CLI provides the following options to determine:

- If the cache entry needs to invalidate on expiry.
- If the cache entry needs to be invalidated, along with the duration to retain the cache entry after the validity expiry.

These options are applicable only if the NRF is inactive. The configuration is according to the nf-pair profile. The configuration determines if SMF should use expired cache in case NRF becomes inactive and if it uses the expired cache, along with the duration to retain the cache entry after the validity expiry.

Configuring NF Discovery Cache Invalidation (Purge)

To configure the cache entry invalidation (purge) for the NF discovery cache, use the following sample configuration.

```
config
  profile nf-pair nf-type { amf | chf | pcf | udm }
    cache invalidation { false | true [ timeout integer ] }
    end
```

NOTES:

- **cache invalidation { false | true [timeout** *integer* **] }**: Configure the interval and cache invalidation rule. The default value is false.
  - **false**: Specify that the cache entry will never be invalidated.
  - **true timeout** *integer* : Specify that the cache entry will be invalidated. **timeout***integer* specifies the time period in milliseconds (ms) for controlling the usage of the expired cache entry (when NRF is unreachable). The default value is 0 ms.

The following configuration is an example that sets the cache invalidation to false for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation false
 end
```

The following configuration is an example that sets the cache invalidation to true for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation true timeout 10
 end
```

Static Configuration for Peer NF Management

Fallback to Static IP Address Support

Feature Description

The SMF follows a priority order for different NF selection options. The SMF prioritizes the NF discovered from the NRF over the local configuration. The SMF uses the locally configured NFs when the NF discovery response has no valid NFs.

Depending on the deployment, the preferred server and geo locality server are configured for each of the NFs. The general rule is to select NFs in the preferred server locality followed by NFs in the geo locality server in case the preferred server NFs fail.

For each NF, the SMF provides an option to configure preferred and geo server locality through the **profile nf-pair** parameter. For more details, see Configuring Locality for NF Types, on page 904 in the NRF Selection per Peer NF Type, on page 909 section.

In addition, each NF discovery response comes with associated validity time. The SMF caches this NF discovery response and uses it to fetch subsequent sessions.

The SMF performs the NF discovery in the following conditions:

- The NF discovery response cache has no matching entries.
- The NF discovery response cache has matching entries, but the validity has expired.

Relationships

The Fallback to Static IP Address feature has functional relationships with the following features:

- Caching Support for NF Discovery
- NF Discovery, NF Selection, and Load Balancing
- NRF Selection per Peer NF Type

How it Works

The SMF follows this sequence for NF selection if an NRF discovery group is configured:

1. It looks up the local cache (NF discovery response cache) for the NF.
2. If the NF is a valid entry (not expired), it uses that entry. Else, SMF proceeds to Step 3.
3. The SMF reaches NRF for discovery [see, NRF Discovery (Priority 1)]. Else, SMF moves to Step 4.

4. If SMF cannot use the NRF for discovery, it uses the expired NF cache [see, Expired NF Cache (Priority 2)]. If expired NF cache is not available, SMF moves to Step 5.
5. If SMF does not find the NF in the local cache nor is it able to get it in the NRF discovery response, it uses the locally-configured NF [see, NF Local configuration (Priority 3)].

The priority order for NF selection is as follows:

1. **NRF Discovery (Priority 1)**

   The SMS uses the NRF-provided, NF discovery service to discover NFs like AMF, UDM, and PCF. The SMF sets the preferred locality as provided in the "**profile nf-pair**" configuration in the discovery query. (For more details about the "**profile nf-pair nf-type**" CLI configuration, see Configuring Locality for NF Types, on page 904 in the NRF Selection per Peer NF Type, on page 909 section.) For each NF, the query parameters are configurable. (For more details, see Configuring Network Element Profile Parameters for the NF, on page 911 in the NRF Selection per Peer NF Type, on page 909 section). The NRF returns all the NFs matching the query criteria. When available, the NRF prefers NF profiles with a locality attribute that matches the preferred-locality. The NRF could return more NFs in the response, which are not matching the preferred target NF location. This occurs when there is no NF profile that is found matching the preferred target NF location. To avoid this, the NRF could set a lower priority for any additional NFs on the response not matching the preferred target NF location than those matching the preferred target NF location. The locality-aware NF selection logic of SMF is as follows:

   a. If the NF has both the preferred and geo locality server configurations, all the NFs in the response that are matching these are cached. SMF ignores the balance NFs. The load-balancing logic first selects the preferred locality NFs. If the preferred locality NFs fail, SMF picks the geo locality NFs for a retry. If N retry is allowed, N-1 retries are on the preferred locality and the last retry is on the geo locality NF. If the N-1 endpoints are unavailable in the preferred locality, SMF attempts all the endpoints of the preferred locality. Else, SMF picks up the geo locality endpoints for the remaining retries. Multiple retries on the same host (port) is not attempted.

   b. If the NF has only the preferred locality configuration, all the NFs in the response that match the preferred locality are cached. The load-balancing logic selects the endpoints from these NFs.

   c. If the NF does not have the preferred locality or geo locality configuration, then SMS caches all the discovery response NFs. The load-balancing logic selects from these NFs.

Note

- The load-balancing logic is based on priority, capacity, and load. The logic is similar to server selection as defined in IETF RFC 2782. However, the weight is considered as "capacity * (100 - load)".
- If SMF selects the NRF-discovered NFs (in any of the three cases), even when all attempts to reach preferred and geo locality fail, the SMF does not fall back to the local configuration NFs for a retry.

2. **Expired NF Cache (Priority 2)**

   The SMF performs an NF discovery only in the following scenarios:

   - If the matching entries are not available for the query filter in its NF discovery cache
   - If matching entries are available in its NF discovery cache. However, these entries have expired validity.

The retention of an expired cache entry is configuration-based. If the expired cache entry is available and the NRF is not reachable or returns an error, then SMF uses the expired cache entry for NF selection. You can configure the SMF to control the cache entry usage with the following options:

- Invalidate the cache entry on expiration of validity.
- Use the invalidated cache entry for a configurable time period (timeout) and fallback to the static configuration after the timeout expires.

Note The SMF controls the cache entry usage - only when the NRF is down - through these options. The configurations are based on the **profile nf-pair**. Additionally, the SMF provides flexibility in configuring different cache usage rule for different NFs. For instance, the SMF always uses the expired cache to discover PCF when the NRF is down. But, for discovering the UDM, the SMF uses the expired cache for a timeout period of 10 milliseconds (ms) when the NRF is down.

3. **NF Local Configuration (Priority 3)**

   The locally configured NFs are the last option for NF endpoint selection. The local configuration too considers the preferred and geo server locality for NF selection. The priority order is as follows:

   a. If the preferred server is configured for the NF [in **profile nf-pair**], SMF selects the NF endpoints under the preferred locality, first. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

   b. If the geo locality is configured for the NF [in **profile nf-pair**], SMF selects the NF endpoints under the geo locality as the fallback option. That is, if the preferred server locality NF endpoints fail or preferred server locality endpoints are not configured. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

   c. If the preferred server and geo locality server are not applicable, SMF picks up the locality based on the priority that is configured for each locality in the local NF configuration. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

Note The priority under locality is applicable only if the preferred and geo locality servers are not applicable.

The failure template is configurable for each of the NFs. Also, the message type in the template can set the retry count and action for the possible HTTP return codes.

Standards Compliance

The Fallback to Static IP Address feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 (2019-07) – 5G System; Network function repository services; Stage 3*

Configuring Fallback to Static IP Address

This section describes how to configure the support for Fallback to Static IP Address.

Configuring NF Client Profile

To configure the NF endpoints for AMF, CHF, PCF, and UDM, use the following sample configuration:

```
config
  profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
  end
```

NOTES:

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**: Specify the required NF client profiles and provide the local configuration for any of the following configured NFs:
  - **amf**: Enable the AMF local configuration
  - **chf**: Enable the CHF local configuration
  - **pcf**: Enable the AMF local configuration
  - **udm**: Enable the AMF local configuration

  For example, if you are configuring the **amf amf-profile** keyword, this command enables the AMF local configuration. The same approach applies for the other configured NFs.

  nf_profile_name must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable the configuration, use the **no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** command.

Configuration Example

The following is an example configuration.

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
```

```
  exit
exit
exit
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

Configuring Network Element Profile Parameters for the NF

To configure the network element profile parameters for the configured NF, use the following sample configuration.

```
config
  network-element-profiles { { amf | chf | pcf | udm } nf_profile_name }
    nf-client-profile profile_name
    query-params { dnn  | limit | max-payload-size | requester-snssais
| supi | tai | target-nf-instance-id | target-plmn }
    end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**: Specify one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specify a DNN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specify a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specify the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specify a SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specify a TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specify a target NF instance Identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specify a target PLMN as the query parameter in the NF discovery request towards the NRF.

- This is an optional configuration. By default, the CLI commands are disabled.
- To disable the configuration, use the **no** variants of these commands. For example, **no nf-client-profile** CLI command.

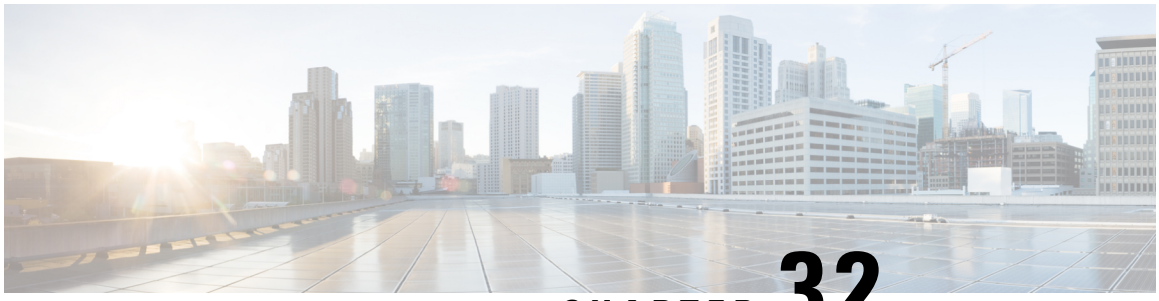
NRF Failure Handling

Feature Description

SMF uses the NF registration messages for tracking the liveliness of management NRF group. If SMF detects a failure in one of the NRFs in the management group, it uses the NRF failure handling mechanism.

Failure handling template is available for each of the NFs and its message types to set the retry count and action for the possible HTTP return codes.

For more information on failure handling, see the Failure Handling Support, on page 355 chapter.



CHAPTER 32

Overload Management

- Feature Summary and Revision History, on page 921
- Feature Description, on page 922
- SBA Interface Overload Control, on page 922
- GTP-C Load and Overload Control, on page 927
- Node Overload, on page 940

Feature Summary and Revision History

Summary Data

Table 343: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 344: Revision History

Revision Details	Release
Added support for GTPC peer overload control	2021.02.3
Added support for GTPC load and overload control	2021.02.0
Added support for message priority configuration.	2020.04.0
First introduced.	2020.03.0

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The SMF provides mechanisms to manage the overload and congestion that occur on the SMF and Service-based Architecture (SBA). The SMF receives ingress messages at a rate higher than the engineered capacity. The internal queues on the SMF may experience higher utilization level than the configured level. This scenario may occur on the SBA servers, directly or indirectly, due to overloaded traffic from the network or from the SMF.

SBA Interface Overload Control

Feature Description

An interface handles only a specified number of incoming requests. When the incoming requests exceed the specified numbers, the interface overloads. For example, an interface is overloaded when:

- A network element failure exists that causes large number of re-attaches
- Multiple users perform location update or transition from idle to active mode frequently

Overloading causes the interface to either drop the requests or delay processing the request. The overall network performance degrades due to the overloading at the interface. This scenario can lead to node congestion, failure, or collapse which in turn causes load increase on the other nodes.

The SMF measures different resources and defines the load based on those measurements. Also, the SMF updates the NRF about the load. Currently, the SMF applies overload protection on inbound messages. The external nodes throttle towards the SMF to come out of a congestion when overload protection is applied on the inbound interface (SBA Interface).

Note The scope of this feature is only on overload due to inbound requests on SBA interface.

How it Works

The SMF protects inbound requests from overloading at Endpoint and Application levels.

- Endpoint Level—The protection is based on the HTTP request method without taking the message type into account.
- Application Level—The protection is based on the message type.

Message Priority

The SMF applies the overload protection on the incoming request messages after evaluating the resources availability to process the request and the message priority. The high priority messages get the lower preference to throttle, and low-priority messages get higher preference. An overloaded NF applies the message prioritization schemes on the incoming messages during an overloaded condition. In such conditions, the NF excludes the messages of the highest priority from the overload protection mechanism.

Once you configure message priority, SMF starts classifying the messages based on their priority. This configuration is optional. If you chose not to use this configuration, SMF applies the overload protection technique without considering the message priority.

Overload Protection at Endpoint

For endpoints, the SMF offers overload protection at both the endpoint and client levels. The SMF defines the overload threshold limits for the inbound request messages. Based on the threshold range, the SMF can reject the inbound request messages. The SMF sends back an HTTP response with the configured status to the request initiator.

The following are the overload threshold limits defined in the SMF:

- **Low** – When this threshold is met, only the POST method (with generic URI contributing to resource allocation) is rejected.
- **High** – All messages are rejected with the configured (reject) statuses when this threshold is met.
- **Critical** – All messages are rejected with the configured (reject) statuses when this threshold is met.

Configuring Overload Protection

This section describes the configuration procedures involved in configuring the overload protection for inbound request messages.

Configuring Overload Protection at Endpoint Level

Use the following configuration to configure overload protection at endpoint level.

```
config
   instance instance-id gr_instance_id
      endpoint sbi
         overload-control threshold threshold_limit threshold_range action
action_status action_code range
         commit
         end
```

NOTES:

- **overload-control**: Specify the overload control at endpoint level.
- **threshold** : Specify the threshold limit and range.
- *threshold_limit*: Specify the threshold limit. *threshold_limit* must be one of the following:
  - *low*: Specify the low threshold limit for overload protection.

- *high*: Specify the high threshold limit for overload protection.
- *critical*: Specify the critical threshold limit for overload protection.

- *thershold_range*: Specify the threshold range. *threshold_range* must be an integer in the range of 10 – 100000.
- **action** : Specify the action to be taken for the threshold limit.
- *action_status*: Specify the action for the threshold limit. *action_status* must be:
  - **reject**: Reject the inbound messages if the specified threshold range is met.
- *action_code*: Specify the action status code. *action_code* must be:
  - **reject-code**: Specify the reject status code.
- *range*: Specify the range of the action code. *range* must be an integer in the range of 100 – 600.

The following is an example configuration:

```
overload-control threshold low 500 action reject reject-code 501
overload-control threshold critical 10000 action reject reject-code 329
```

Configuring Overload Protection at Client Level

Use the following sample configuration to configure overload protection at client level.

```
config
   instance instance-id gr_instance_id
      endpoint sbi
        overload-control client threshold threshold_limit threshold_range action
 action_status action_code range
         commit
         end
```

NOTES:

- **overload-control client**: Specify the overload control at client level.
- **threshold** : Specify the threshold limit and range.
- *threshold_limit*: Specify the threshold limit. *threshold_limit* must be one of the following:
  - *low*: Specify the low threshold limit for overload protection.
  - *high*: Specify the high threshold limit for overload protection.
  - *critical*: Specify the critical threshold limit for overload protection.
- *thershold_range*: Specify the threshold range. *thershold_range* must be an integer in the range of 10 – 100000.
- **action** : Specify the action to be taken for the threshold limit.
- *action_status*: Specify the action for the threshold limit. *action_status* must be:

- **reject**: Reject the inbound messages if the specified threshold range is met.

- *action_code*: Specify the action status code. *action_code* must be:
  - **reject-code**: Specify the reject status code.

- *range*: Specify the range of the action code. *range* must be an integer in the range of 100 – 600.

The following is an example configuration:

```
overload-control client threshold low 50 action reject reject-code 329
overload-control client threshold critical 20000 action reject reject-code
501
```

Verifying the Overload Protection Configuration

Use the **show running-config** command to view the overload protection configuration in the SMF Ops Center. The following is a sample output of the **show running-config** command.

```
[cluster1/data] example# show running-config
instance instance-id 1
 endpoint sbi
  overload-control threshold low 5000 action reject reject-code 555
  overload-control threshold high 7000 action reject reject-code 329
  overload-control threshold critical 10000 action reject reject-code 503
  overload-control client threshold low 750 action reject reject-code 329
  overload-control client threshold high 500 action reject reject-code 329
  overload-control client threshold critical 1000 action reject reject-code 503
  interface n11
  overload-control threshold low 4000 action reject reject-code 555
  overload-control threshold high 6000 action reject reject-code 329
  overload-control threshold critical 7000 action reject reject-code 503
  overload-control client threshold low 500 action reject reject-code 329
  overload-control client threshold high 700 action reject reject-code 329
  overload-control client threshold critical 800 action reject reject-code 503
 exit
exit
```

Configuring the Message Priority

Use the following configuration to configure message priority for the inbound request messages.

```
config
  overload-control threshold threshold_limit threshold_range action reject
reject-code range exclude message-priority priority_value
  end
```

NOTES:

- **overload-control** – Specify the overload control at endpoint level.
- **threshold***threshold_limit* – Specify the threshold limit and range.
- – Specify the threshold limit. *threshold_limit* must be one of the following:
  - low – Specify the low threshold limit for overload protection.
  - high – Specify the high threshold limit for overload protection.

    - critical– Specify the critical threshold limit for overload protection.

- *thershold_range* – Specify the threshold range. *thershold_range* must be an integer in the range of 10–100000.
- **action** – Specify the action to be taken for the threshold limit.
- *action_status* – Specify the action for the threshold limit.*action_status* must be:
    - **reject** – Rejects the inbound messages if the specified threshold range is met.
- **exclude message-priority** – Excludes the messages from the overload protection mechanism depending on the assigned priority.
- *priority_value* – Specifies the priority value.

The following is an example configuration:

```
overload-control threshold low 1000 action reject reject-code 100 exclude message-priority 8
```

```
overload-control threshold high 2000 action reject reject-code 100 exclude message-priority 5
```

If the priority value is 8, then the messages received with priority 8 or higher are not throttled. This applies even when the system threshold is lower than the priority value. The 3GPP defined message priority is 0–31 as per *3GPP TS 29.500 version 15.4.0*.

Monitoring and Troubleshooting

This section provides information regarding bulk statistics available to monitor and troubleshoot this feature.

Statistics

The following statistics are available in support of Overload Control.

Bulk Statistics	Statistics Type	Description
endpoint_overload_status	Gauge	Contains Endp Overload-Leve level(low/high be set to 1. In r
endpoint_client_overload_status	Gauge	Contains Endpo name and Ove level(low/high be set to 1. In r
endpoint_pending_request	Gauge	Display curren It contains Enc label.
endpoint_client_pending_request	Gauge	Display curren connected with name, Interfac connected to th

Bulk Statistics	Statistics Type	Description
endpoint_overload_exclude	Counter	Display the were exclud The metric bypasses th

GTP-C Load and Overload Control

Feature Description

Important The GTP-C Load and Overload Control is an optional feature.

The SMF uses the system load information to determine the operating status of the resources of the GTP-C entity. This information, when sent to the GTP-C peers, helps to balance the session load adaptively across entities supporting the same function based on their effective load.

A GTP-C overload occurs when the number of incoming requests exceeds the maximum request throughput supported by the receiving GTP-C entity. The GTP-C is over UDP transport, and it relies on the retransmissions of unacknowledged requests. When a GTP-C entity experiences overload (or severe overload), the number of unacknowledged GTP-C messages exponentially increase leading to a node congestion or collapse. An overload or a node failure leads to an increase of the load on the other nodes in the network.

Overload of the core network nodes in the network results in service degradation. Improved load distribution over the network helps in addressing the overload issue.

Overload conditions can occur in various network scenarios. The following are some examples of GTP-C signaling-based scenarios which lead to GTP-C overload:

- A traffic flood resulting from the failure of a network element, inducing a signaling spike.
- A traffic flood resulting from many users performing TAU or RAU or from frequent transitions between idle and connected modes.
- An exceptional event locally generating a traffic spike, for example, many calls (and dedicated bearers) being set up almost simultaneously.
- Frequent RAT reselection due to scattered non-3GPP (for example, Wi-Fi) coverage or a massive mobility between a 3GPP and non-3GPP coverage. This operation may potentially cause frequent or massive intersystem change activities.

GTP-C overload may result in any of the following service impacts:

- Emergency call drops
- Loss of PDN connectivity (IMS, Internet, and so on) and associated services.
- Loss of ability to set up and release radio and core network bearers necessary to support services, for example, GBR bearers.
- Loss of ability to report the change in—

- User information, for example, location information for emergency services and lawful intercept
- RAT or QoS

- Billing errors which result in loss of revenue.

GTP-C Load and Overload Control is a standards-driven feature. For standards compliance information, see the Standards Compliance, on page 932 section in this feature chapter.

GTP-C Load Control and Overload Control are complimentary concepts which can be supported and activated independently on the network.

This feature works both in a standalone deployment of SMF and an integrated deployment with cnSGWc.

Note This feature works only when the SMF interworks with PGW-C (that is, the EPS network). The term "SMF" used in this chapter denotes the combination of both SMF and PGW-C.

GTP-C Load Control

This feature enables cnSGWc and PGW-C to gather and send Load Control Information (LCI) to GTP-C peers (for example, MME via cnSGWc, and ePDG). In broad terms, GTP-C load control denotes a preventive action and GTP-C overload control indicates a corrective action.

The advantages of enabling GTP-C Load Control are as follows:

- Load control allows better balancing of the session load; this mechanism prevents the GTP-C overload scenario.
- LCI helps to balance the session load adaptively across entities supporting the same function according to their effective load.
- Load control does not trigger overload mitigation actions even if the GTP-C entity reports a high load.

GTP-C Overload Control

This feature enables cnSGWc and PGW-C to gather and send Overload Control Information (OCI) to GTP-C peers (for example, MME via cnSGWc, and ePDG). A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance.

The advantages of enabling GTP-C Overload Control are as follows:

- Avoids overloading of GTP-C entity
- Improves load distribution on SMF and cnSGWc which in turn reduces the occurrence of SMF overload.
- Aims at shedding the incoming traffic as much as possible when an overload has occurred

Message Throttling

Ingress Messages

GTP-C entity uses traffic reduction metric information in the Overload Control Information (OCI) for message throttling. To mitigate overload scenario, the GTP-C entity reduces the ingress message flow towards the overloaded peer based on the metric information.

When a node is in self-protection mode, the SMF rejects the ingress GTP-C messages based on the message throttling exclude configuration. For details on the exclude profile configuration, see the Create Exclude Profile, on page 934 section.

Egress Messages

To mitigate the GTP-C overload scenario, the SMF controls the egress message flow towards the overloaded GTP-C peer based on the information received within the OCI.

The SMF rejects the egress messages towards the GTP-C peers based on the exclude profile configuration. Exclusion profile contains the DNN list, 5QI list, ARP list, and priority corresponding to the messages to be excluded from throttling.

Peer overload control for GTP-C interface can be configured through the **profile overload** *profile-name* **peer-level interface gtpc action throttle** command.

Important Message throttling applies only to the initial messages. The SMF does not throttle the triggered request or response messages as it might result in retransmission of the corresponding request message.

For throttling, the SMF uses the loss algorithm as specified in 3GPP 29.274.

Message groups are formed based on the category of procedures mentioned in 3GPP 29.274, section 12.3.9.3.2. The following are the peer overload groups for message throttling.

- Group 1 corresponds to update of existing resources. This group includes the Update Bearer Request message.
- Group 2 corresponds to creation of new resources. This group includes the Create Bearer Request message.

Message groups allow the user to configure, in percentage, how many number of messages SMF is expected to generate in each message group. The default value for both the groups are 50%. The default value 50% means that, out of 100 outgoing messages, 50 messages are update bearer requests (group 1) and 50 messages are create bearer requests (group 2).

If the peer is overloaded and the overload reduction matrix is 30%, then the SMF throttles 30 create bearer request messages and sends all the remaining messages.

If the peer is overloaded and the overload reduction matrix is 70%, the SMF throttles 50 create bearer request messages and 20 update bearer request messages and sends the remaining 30 update bearer messages.

Overloaded Peer Detection

The SMF determines whether or not the GTP-C peer entity is overloaded based on the received Overload Control Information (OCI) IE information in any of the following GTP-C messages.

- Create Session Request

- Create Bearer Response
- Modify Bearer Request
- Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Modify Bearer Command
- Delete Bearer Command
- Bearer Resource Command

Note that all the GTP-C messages include the OCIs of cnSGWc, MME or S4-SGSN, and TWAN or ePDG except for Delete Bearer Command and the Bearer Resource Command messages.

The SMF receives OCI that corresponds to multiple GTP-C entities in a single message (for example, the OCI of cnSGWc and MME or S4-SGSN). The SMF service pod parses and stores all such OCI IEs received in a single message.

The SMF considers the GTP-C peer as overloaded when one of the following conditions is met.

- the validity period of the OCI expires
- the OCI is received as 0

In the case of geo redundancy (GR), it is expected that fresh cache records are built by the new instance with time based on OCI received from new messages.

When the primary cache pod is inactive, the secondary cache pod becomes active and serves all the cache requests.

How it Works

This section describes the detailed working mechanism of this feature.

1. The SMF fetches the system load periodically from the Application infrastructure. For details on load calculation, see the Node Overload, on page 940 section in this chapter.
2. The SMF identifies the current node overload state based on thresholds configured in the Overload Profile, and the system load value.
3. The SMF applies the overload control mechanism on the incoming request messages based on the node overload states.

Node Overload State	Definition	Criteria	Overload Control Action
Normal	The system is not under any overloaded condition.	Load < Minimum tolerance	Applies GTP-C Load Control
Overloaded	The system is overloaded.	Minimum tolerance <= Load < Maximum tolerance	Applies GTP-C Overload Control

Node Overload State	Definition	Criteria	Overload Control Action
Self-protection	The system has reached the extreme limits of overload.	Load >= Maximum tolerance	Applies Message Throttling

GTP-C Load Control Mechanism

The SMF communicates the LCI to the GTP-C peers (for example, MME or ePDG) upon meeting the following conditions:

- If the feature is enabled through the **profile load** *load_profile_name* **interface gtpc action advertise** command
- If the load profile and overload profile are associated with the SMF profile
- If the LCI is never sent to the peer
- Periodically as per the configuration **profile load** *load_profile_name* **advertise interval** *lci_broadcast_interval*
- If the difference between current load value and last indicated load value is greater than the configured change factor **profile load** *load_profile_name* **advertise change-factor** *load_value_change_factor*

Note The SMF exchanges LCI through GTP-C request and response messages without triggering extra signaling.

The SMF includes the LCI in the following messages:

- Create Session Response
- Create Bearer Request
- Modify Bearer Response
- Delete Bearer Request
- Delete Session Response
- Update Bearer Request

For message formats and LCI IE details, see the 3GPP TS 29.274 specification, version 15.4.0.

GTP-C Overload Control Mechanism

The SMF calculates and sends the overload metric based on the load value and the overload reduction-metric configuration. The SMF then communicates the OCI to the GTP-C peers upon meeting the following conditions:

- If the feature is enabled through the **profile overload** *overload_profile_name* **node-level interface gtpc action advertise** command
- If the OCI is never sent to the peer
- Periodically as per the configuration **profile overload** *overload_profile_name* **node-level advertise interval** *oci_broadcast_interval*

- If the difference between current reduction-metric and last indicated reduction-metric is greater than the configured change factor **profile overload** *overload_profile_name* **node-level advertise change-factor** *overload_value_change_factor*
- If the validity timer expires and the SMF is still in overloaded state

Note The SMF exchanges OCI through GTP-C request and response messages without triggering extra signaling.

The SMF includes the OCI in the following messages:

- Create Session Response
- Create Bearer Request
- Modify Bearer Response
- Delete Bearer Request
- Delete Session Response
- Modify Bearer Failure Indication
- Update Bearer Request
- Delete Bearer Failure Indication

For message formats and OCI IE details, see the *3GPP TS 29.274 specification, version 15.8.0.*

Message Throttling

In the self-protection mode, the SMF rejects the ingress GTP-C messages with failure cause set to "GTP-C Entity Congestion" as per the self-protection exclusion configuration.

Standards Compliance

The GTP-C Load and Overload Control feature complies with the following standards:

- *3GPP TS 29.807, version 12.0.0*
- *3GPP TS 29.274, version 15.8.0*

Limitations

The GTP-C Load and Overload Control feature has the following limitation:

- Allows configuration of only one load profile and one overload profile

Configuring GTP-C Load and Overload Control Feature

This section describes how to configure the GTP-C Load and Overload Control feature.

Configuring the GTP-C Load and Overload Control feature involves the following steps:

1. Create Load Profile, on page 933

2. Create Exclude Profile, on page 934
3. Create Overload Profile, on page 935
4. Associate Load and Overload Profiles, on page 938

Create Load Profile

Use the following sample configuration to create the load profile. This profile defines the parameters that are required to calculate the load of SMF.

```
config
   profile load load_profile_name
      load-calc-frequency load_calculation_interval
      load-fetch-frequency load_fetching_time
     advertise [ interval lci_broadcast_interval | change-factor lci_change_factor
 ]
      interface gtpc action advertise
      end
```

NOTES:

- **profile load** *load_profile_name*: Specify the load profile name. *load_profile_name* must be an alphanumeric string.

  Use the load profile for system load calculation and LCI broadcast.

- **load-calc-frequency** *load_calculation_interval*: Specify the system load calculation interval in seconds.

  load_calculation_interval must be an integer in the range of 5-3600. Default value is 10 seconds.

- **load-fetch-frequency** *load_fetching_time*: Specify the time interval at which service pod fetches load from cache pod.

  load_fetching_time must be an integer in the range of 5-3600. Default value is 10 seconds.

- **advertise interval** *lci_broadcast_interval*: Specify the periodic interval for sending LCI to the GTP-C peers.

  lci_broadcast_interval must be an integer in the range of 0-3600. Value 0 indicates that the LCI is sent in all the messages. Default value is 300 seconds.

- **advertise change-factor** *lci_change_factor*: Specify the minimum change between current LCI and last indicated LCI, after which the advertising occurs.

  lci_change_factor must be an integer in the range of 1-20. Default value is 5.

- **interface gtpc action advertise**: Specify to enable LCI publish or broadcast on GTP-C interface. By default, this option is disabled.

Verify Load Profile Configuration

Use the following command to view the load control profile configuration settings.

```
show running-config
```

The following is an example of the **show running-config** command output.

```
#show running-config
.
.
.
profile load loadprofile
load-calc-frequency  10
load-fetch-frequency 10
advertise interval 300
advertise change-factor 5
interface gtpc
  action advertise
exit
exit
```

Create Exclude Profile

Use the following sample configuration to create the exclude profile for use during self-protection state. This profile determines the session-related messages that should be excluded from throttling decisions.

```
config
   profile overload-exclude overload_exclude_profile_name
      arp-list list_of_arps
      dnn-list list_of_dnns
      message-priority s5 upto message_priority
      procedure-list session-delete
      qi5-list list_of_qos_identifiers
      end
```

NOTES:

- **profile overload-exclude** *overload_exclude_profile_name*: Specify the exclude profile name. *overload_exclude_profile_name* must be an alphanumeric string.

  You can configure multiple exclude profiles with this command. Be sure to reference the exclude profile name in the Overload Control configuration.

- **arp-list** *list_of_arps*: Specify the list of Allocation and Retention Priorities (ARPs) that must be excluded from throttling decisions.

  list_of_arps must be an integer in the range of 1-15.

  You can configure a maximum of eight entries.

- **dnn-list** *list_of_dnns*: Specify the list of DNNs that must be excluded from throttling decisions.

  You can configure a maximum of three entries.

- **message-priority s5 upto** *message_priority*: Specify the message priority up to which has to be excluded from throttling decisions.

  message_priority must be an integer in the range of 0-15.

- **procedure-list session-delete** : Specify the session deletion procedures that must be excluded from throttling decisions.

- **qi5-list** *list_of_qos_identifiers*: Specify the 5G QoS Identifiers that must be excluded from throttling decisions.

  list_of_qos_identifiers must be an integer in the range of 1-15.

Verify Exclude Profile Configuration

Use the following command to view the exclude profile configuration settings.

show running-config

The following is an example of the **show running-config** command output.

```
#show running-config
.
.
.
profile overload-exclude excludeProfile
dnn-list       [ starent.com.mnc456.mcc123.gprs ]
qi5-list        [ 1 2 ]
arp-list       [ 1 2 ]
procedure-list [ session-delete ]
message-priority s5
  upto 1
exit
exit
```

Create Overload Profile

The overload profile determines the various conditions for overload control and throttling decisions.

To create the overload profile, use the following sample configuration:

```
config
   profile overload overload_profile_name
      overload-exclude-profile self-protection overload_exclude_profile_name
      node-level
         tolerance minimum min_percentage maximum max_percentage
         reduction-metric minimum min_percentage maximum max_percentage
         advertise [ interval oci_broadcast_interval | change-factor
oci_change_factor | validity-period oci_validity_period ]
         interface gtpc overloaded-action advertise
      peer-level
         message-prioritization group1 weight group2 weight
         interface gtpc
            action throttle
         end
```

NOTES:

- **profile overload** *overload_profile_name*: Specify the overload profile name. *overload_profile_name* must be an alphanumeric string.

Important You can configure only one overload profile with this command. Create exclude profile before configuring overload profile.

- **overload-exclude-profile self-protection** *overload_exclude_profile_name*: Specify the exclude profile name that is configured for use during overload self-protection mode.

  overload_exclude_profile_name must be an alphanumeric string.

- **node-level**: Specify to apply the configuration only for the overloaded SMF node.

- **tolerance minimum** *min_percentage* **maximum** *max_percentage*: Specify the minimum and maximum percentage of the system load tolerance. *min_percentage* and *max_percentage* must be an integer in the range of 1-100.

  min_percentage: This value is the tolerance level below which the system is considered to be in Normal state. Default value is 80.

  max_percentage: This value is the tolerance level above which the system is considered to be in Self-protection state. Default value is 95.

  If the value is between the configured minimum and maximum tolerance values, then the system is in Overloaded state.

- **reduction-metric minimum** *min_percentage* **maximum** *max_percentage*: Specify the minimum and maximum percentage of the traffic reduction factor. *min_percentage* and *max_percentage* must be an integer in the range of 1-100.

  min_percentage: This value is the percentage of traffic reduction in tandem with minimum tolerance configuration. Default value is 10.

  max_percentage: This value is the percentage of traffic reduction in tandem with maximum tolerance configuration . Default value is 100.

- **advertise interval** *oci_broadcast_interval*: Specify the periodic interval for sending OCI to the GTP-C peers.

  oci_broadcast_interval must be an integer in the range of 0-3600. Value 0 indicates that the OCI is sent in all the messages. Default value is 300 seconds.

- **advertise change-factor** *lci_change_factor*: Specify the minimum change between current OCI and last indicated OCI, after which the OCI advertising occurs.

  oci_change_factor must be an integer in the range of 1-20. Default value is 5.

- **advertise validity-period** *oci_validity_period*: Specify the validity period of the advertised OCI value.

  oci_validity_period must be an integer in the range of 1-3600. Default value is 600 seconds.

- **interface gtpc overloaded-action advertise**: Specify to enable OCI publish or broadcast on GTP-C interface when the node is overloaded. By default, this option is disabled.

- **peer-level**: Specify to apply the configuration only for the overloaded peer.

- **message-prioritization group1** *weight* **group2** *weight*: Specify the ratio in which the messages need to be throttled for both the message groups. Each group contains a predefined set of messages from every SMF interface.

  weight must be an integer in the range of 1-100. The default value is 50.

- **interface gtpc action throttle** : Enables the throttling action over S6, S8, and S2b interfaces.

Verify Overload Profile Configuration

To view the overload control profile configuration settings, use the following command:

show running-config

The following is an example of the **show running-config** command output.

```
#show running-config
.
```

```
.
.
profile overload overloadprofile
overload-exclude-profile self-protection excludeProfile
node-level tolerance minimum 80
node-level tolerance maximum 95
node-level reduction-metric minimum 10
node-level reduction-metric maximum 80
node-level advertise interval 300
node-level advertise change-factor 5
node-level advertise validity-period 600
node-level interface gtpc
  overloaded-action [ advertise ]
exit
exit
```

To view the overload information of all the peers, use the following command:

show overload-info peer all

The following is an example of the **show overload-info peer all** command output.

```
[smf] smf# show overload-info peer all
                              OVERLOAD
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
------------------------------------------------------------------------------
SGW   S5         209.165.201.1    1632888445     5        2021-12-01 00:04:02 UTC
MME   S5         209.165.201.2    1632888445     6        2021-12-01 05:04:02 UTC
```

This command displays the overload information of all the peers.

To view the overload information of a specific peer, use the following command:

show overload-info peer all *peer-type*

The following is an example of the **show overload-info peer all SGW** command output.

```
[smf] smf# show overload-info peer all SGW
                              OVERLOAD
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
------------------------------------------------------------------------------
SGW   S5         209.165.201.1    1632888445     5        2021-12-01 00:04:02 UTC
```

This command displays the overload information of S-GW.

To view the overload information of peers at an interface level, use the following command:

show overload-info peer all interface S5

The following is an example of the **show overload-info peer all interface S5** command output.

```
[smf] smf# show overload-info peer all interface S5
                              OVERLOAD
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
------------------------------------------------------------------------------
SGW   S5         209.165.201.1    1632888445     5        2021-12-01 00:04:02 UTC
MME   S5         209.165.201.2    1632888445     6        2021-12-01 05:04:02 UTC
```

This command displays the overload information of all the peers at S5 interface.

To view the overload information by IP address of peer, use the following command:

show overload-info peer all peerIP *ip_address*

The following is an example of the **show overload-info peer all peerIP 209.165.201.2** command output.

```
[smf] smf# show overload-info peer all peerIP 209.165.201.2
                              OVERLOAD
                              CONTROL     OVERLOAD
PEER                          SEQUENCE    REDUCTION
TYPE  INTERFACE  PEER IP      NUMBER      METRIC     PERIOD OF VALIDITY
------------------------------------------------------------------------------
MME   S5         209.165.201.2    1632888445     6        2021-12-01 05:04:02 UTC
```

Associate Load and Overload Profiles

Use the following sample configuration to associate the load control profile and overload profile with the SMF service profile.

```
config
   profile smf smf_profile_name
      load-profile load_profile_name
      overload-profile overload_profile_name
      end
```

NOTES:

- **profile smf** *smf_profile_name*: Specify the existing SMF service profile name.

  smf_profile_name must be an alphanumeric string.

- **load-profile** *load_profile_name*: Specify the load profile name to associate with the SMF service profile.

  load_profile_name must be an alphanumeric string.

- **overload-profile** *overload_profile_name*: Specify the overload profile name to associate with the SMF service profile.

  overload_profile_name must be an alphanumeric string.

- Linking of the overload profile with SMF profile works only when the load profile is linked.

Verify Load and Overload Profile Association

Use the following command to view the association of load and overload profiles with the SMF service profile.

show running-config

The following is an example of the **show running-config** command output.

```
#show running-config
.
.
.
profile smf smf1
<……..>
load-profile  loadprofile
overload-profile overloadprofile
<……..>
exit
```

OAM Support for GTP-C Load and Overload Control

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The SMF maintains the following metrics as part of this feature.

- **node_lci_metric**

  Description: This counter indicates the current load (LCI) value at the node level that is, SMF with PGW-C.

  Metrics Type: Gauge

  Labels:

  - app_name
  - cluster
  - data_center
  - instance_id

- **node_oci_metric**

  Description: This counter indicates the current overload (OCI) value at the node level.

  Metrics Type: Gauge

  Labels:

  - app_name
  - cluster
  - data_center
  - instance_id

- **node_overload_status**

  Description: This counter indicates the current overloaded status at the node level.

  - 0 - Normal
  - 1 - OverLoaded
  - 2 - SelfProtection

  Metrics Type: Gauge

  Labels:

  - app_name
  - cluster
  - data_center
  - instance_id

- **smf_inc_msg_throttling_stats**

  Description: This counter provides the number of incoming messages throttled on each interface in self-protection mode.

  Metrics Type: Counter

  Labels:

  - app_name
  - cluster
  - data_center
  - instance_id
  - interface
  - message_type
  - cause

- **smf_og_msg_throttling_stats**

  Description: This counter provides the number of outgoing messages throttled on each interface when peer entity is overloaded.

  Metrics Type: Counter

  Labels:

  - app_name
  - cluster
  - data_center
  - gr_instance_id
  - instance_id
  - interface
  - message_type
  - service_name
  - throttled_target_peer_type
  - cause

Node Overload

The node overload refers to the resource utilization data of all the SMF pods in the NF deployment. The SMF periodically gathers the current resource utilization data for these pods. The default frequency to read the resource utilization data is 5 seconds. The SMF monitors the CPU, memory utilization, go-routines, and stores the average values for the current, last 5 minutes and 15 minutes for the pods.

Pod Level Load Factor

The maximum values against the current values for CPU, memory utilization and go-routines for a pod are used to calculate its load factor. The GOMAXPROCS environment variable is used to calculate the capacity of a pod. The maximum value per core is defined with constant values, which is used to derive the capacity of CPU, memory and go-routines.

An example of the maximum value per core is show below.

MAX_CPU_PERCENTAGE_PER_CORE = 100

MAX_MEMORY_PER_CORE = 4 GB

MAX_GO_ROUTINE_PER_CORE = 10,000

The **NewApplicationWithOptions** is used to get the maximum values. If the values are not provided by the application, then the default values are used.

The load factor for a pod is calculated as follows:

- CPU load factor = Current load percentage / Maximum load percentage at pod x 100
- Memory load factor = Current memory usage / Maximum memory at pod x 100
- Go-routine load factor = Go-routine count / Maximum Go-routine count at pod x 100

The maximum value from the CPU, memory and go-routines load factors is considered as the final load factor.

Self-NF Load Factor from an OAM Pod

The OAM pod periodically gathers the load factor data from each SMF pod and updates the cache pod. The OAM pod also receives the session load factor from the CDL and updates the cache pod at the same time.

The system APIs provide the load factor data based on the following logic:

- **Pod level load factor** - If an application queries the load factor for a pod to get its resource utilization data in the SMF, then the response contains the maximum load factor for all the pod type categories in that cluster.
- **System level load factor** - If an application queries the load factor at the system level, then the response contains the maximum load factor for all the pods in that cluster along with the session load factor data.
- **Load factor based on a category** - If an application queries the load factor for a specific type of service like, smf-service, smf-rest-ep, and so on, then the following conditions are met:
  - **Active-Active deployment** - The query response contains the average value of the load factors.
  - **Active-Standby deployment** - The query response contains the maximum value of the load factors.

A system level capacity to handle the number of sessions is configured in the SMF. The load factor for each session is calculated in the OAM pod as the Current session count / Maximum number of sessions.

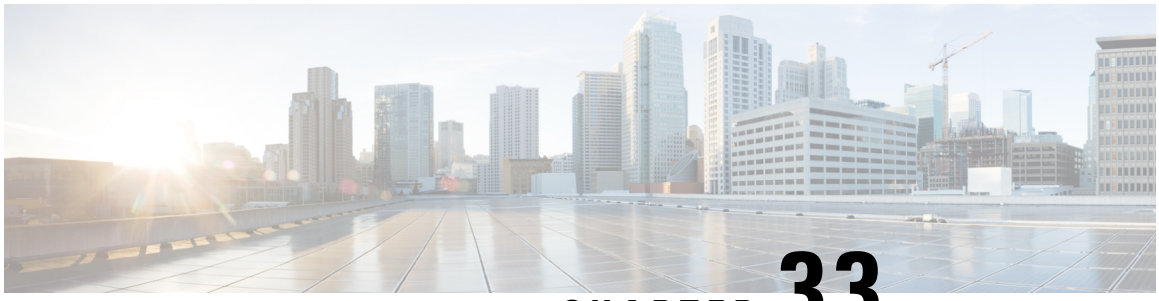
Maximum Sessions

A datastore configuration is used to include the session load factor for supported namespaces. The values must be set from the application while registering the session database. If the value is not set, then the default 1,000,000 is used to calculate the session load factor.

Application level ConfigMap Support for OAM

The OAM infra chart mounts the configmaps from the OAM application in the following ways:

- **Infra-OAM**
  - Update template to add volumes for configuration maps from render.yaml.
  - Update template to mount volumes from render.yaml by using volumeMounts.
- **Application-OAM**
  - Add configuration map with the same in application configuration chart.
  - Provide values from Values.yaml or from CLI for the configuration map.



CHAPTER 33

Performance Optimization Support

- Feature Summary and Revision History, on page 943
- Feature Description, on page 945
- Batch ID Allocation, Release, and Reconciliation Support, on page 945
- Cache Pod Optimization, on page 948
- CDL Flush Interval and Session Expiration Tuning Configuration, on page 948
- Domain-based User Authorization Using Ops Center, on page 949
- Edge Echo Implementation, on page 952
- Encoder and Decoder Optimization for GTPC Endpoint Pod, on page 953
- ETCD Peer Optimization Support, on page 954
- Roaming Peer Optimization, on page 955
- ETCD Traffic Optimization, on page 957
- ETCD Client Fallback, on page 958
- Flag DB Database Updates, on page 959
- Handling PDU Session Modifications based on RRC Inactive Cause Codes, on page 960
- Pod Failure Detection using K8 Liveness Probe, on page 967
- Resiliency Handling, on page 968

Feature Summary and Revision History

Summary Data

Table 345: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platforms	SMI

Feature Default Setting	Batch ID Allocation, Release, Reconciliation Support: Disabled – Configuration required to enable Cache Pod Optimization CDL Flush Interval and Session Expiration Tuning Configuration: Enabled – Configuration required to disable Domain-based User Authorization Using Ops Center Edge Echo Implementation: Enabled – Always-on Encoder and Decoder Optimization for GTPC Endpoint Pod: Disabled – Configuration required to enable ETCD Peer Optimization Support: Enabled - Always-on ETCD Traffic Optimization: Enabled - Always-on Roaming Peer Optimization- Disabled – Configuration required to enable Flag DB Database Updates: Enabled – Always-on GTPC IPC Cross-rack Support: Disabled – Configuration required to enable Handling PDU Session Modifications based on RRC Inactive Cause Codes: Disabled – Configuration required to enable Interservice Pod Communication: Disabled – Configuration required to enable Resiliency Handling: Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 346: Revision History

Revision Details	Release
Added the following support: • ETCD Traffic Optimization • ETCD Client Fallback • Improved liveness check of K8 pods • Diameter service pod in resiliency handling • Roaming Peer Optimization	2023.03.0

Revision Details	Release
Added the following support: • Cache Pod Optimization • Encoder and Decoder Optimization for GTPC Endpoint Pod • Flag DB Database Updates • Resiliency Handling	2023.01.0
First introduced. Added the following support: • Batch ID Allocation, Release, and Reconciliation Support • CDL Flush Interval and Session Expiration Tuning Configuration • Domain-based User Authorization Using Ops Center • Edge Echo Implementation • ETCD Peer Optimization Support • GTPC IPC Cross-rack Support • Handling PDU Session Modifications based on RRC Inactive Cause Codes	2022.04.0

Feature Description

This chapter describes about the performance optimization features.

Some of the performance optimization features are common across cnSGW-C and SMF.

For complete information on cnSGW-C features, see the *UCC 5G cnSGWc Configuration and Administration Guide*.

Batch ID Allocation, Release, and Reconciliation Support

Feature Description

The nodemgr allocates a unique ID to the subscriber that is in the attached state. When the subscriber detaches, the unique ID is released to the nodemgr. If the allocation and deallocation procedures increase, the nodemgr performance is impacted and the sgw-service continues to wait longer to complete these procedures.

The Batch ID Allocation, Release, and Reconciliation Support feature provide a mechanism to reduce the interaction between the sgw-service and nodemgr, which in turn optimizes the nodemgr's performance.

How it Works

This section describes how this feature works.

Batch ID Allocation:

Allocation of batch ID involves the following steps:

- The sgw-service manages the ID store by allocating the free IDs to the subscriber. When the IDs are unavailable in the store, the sgw-service sends the Batch ID Allocation Request to nodemgr.
- In response, nodemgr returns a batch of 128 IDs with the ID Reserve Report Interval. The sgw-service updates the ID store with the IDs received from the nodemgr and starts a timer for the ID Reserve Report Interval.
- If all the IDs are used before the duration configured in the ID Reserve Report Interval, sgw-service sends a Batch of ID Allocation Request to the nodemgr with a notification to reserve all IDs from the previous request.
- If the ID Reserve Report Interval timer expires before the sgw-service allocates all the IDs, sgw-service sends the unused IDs back to nodemgr through the Reserve Report Batch operation.

Batch ID Release:

Releasing of the batch ID involves the following steps:

- The sgw-service manages the IDs that the ID store releases for each nodemgr.
- The sgw-service returns the ID to the ID store whenever an ID is deallocated. If the ID store is full, the sgw-service sends a Batch ID Release Request and the released IDs to the respective nodemgr.
- When sgw-service starts adding IDs to the ID store, the ID release timer starts.
- If the ID release timer expires before the batch IDs are releases or the batch is full, sgw-service sends the released IDs to nodemgr.

Batch ID Reconciliation

Batch ID reconciliation occurs when the service pod and the nodemgr pod restarts.

On service pod restart:

1. When the service pod receives the batch IDs and becomes unresponsive before allocating the IDs, the nodemgr does not get the Batch ID Reserve Request causing the ID reserve procedure to time out. In such a scenario, the nodemgr reconciles the unreserved or unallocated IDs with CDL. The IDs that are not allocated to the subscribers are released to the ID store.
2. The service pod collects the IDs that are released and if it becomes unresponsive before releasing them to the nodemgr. In this scenario, the IDs are dropped.

On nodemgr pod restart:

1. The IDs existing in the in-flight Batch ID Reserve Request and Batch ID Release Request are dropped.

2. The nodemgr notifies cachemgr about the allocated IDs in a batch. If nodemgr becomes unresponsive before notifying the IDs to cachemgr, after a restart, nodemgr starts allocating the new IDs. The nodemgr allocated the IDs based on the last allocated ID and the batch size.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   sgw sgw_name
      resmgr-batch-operation [ disable | enable ]
      end
```

NOTES:

resmgr-batch-operation [disable | enable]—Configures the batch operation. By default, **resmgr-batch-operation** is disabled.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics

The following statistics are supported for the Batch ID Allocation and Release Support feature:

- sgw_resource_mgmt_stats—Captures the total number of the cnSGW-C resource management statistics.

  Sample queries:

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_alloc",instance_id="0",service_name="sgw-service",status="attempted"}
 3
:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_alloc",instance_id="0",service_name="sgw-service",status="success"}
 3
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1"
,id_req_type="id_batch_dealloc",instance_id="0",service_name="sgw-service",status="attempted"}
 2
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",id_req_type=
"id_batch_dealloc",instance_id="0",service_name="sgw-service",status="success"}
 2
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_dealloc_timeout",instance_id="0",service_name="sgw-service",status="attempted"}
 1
:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",id_req_type
="id_batch_dealloc_timeout",instance_id="0",service_name="sgw-service",status="success"}
 1
```

```
sgw_resource_mgmt_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
id_req_type="id_batch_release_timeout",instance_id="0",service_name="sgw-service",status="attempted"}
 1
-:sgw_resource_mgmt_stats{app_name="smf",cluster="Local",d-ata_center="DC",gr_instance_id="1",id_req_type
="id_batch_release_timeout",instance_id="0",service_name="sgw-service",status="success"}
 1
```

- nodemgr_rmgr_batch_reconcile_stats—Captures the total count of batches that are sent for reconciliation.

  Sample queries:

```
nodemgr_rmgr_batch_reconcile_stats{app_name="smf",cluster="Local",data_center="DC",instance_id="0",
service_name="nodemgr",status="success"} 1
```

- nodemgr_resource_mgmt_resp_stats—Captures the total number of IDs released due to reconciliation.

  Sample queries:

```
nodemgr_resource_mgmt_resp_stats{app_name="smf",cluster="Local",data_center="DC",error="",
gr_instance_id="0",instance_id="0",ip_ver_type="IP_TYPE_NONE",req_type="ID_REQ_REL_RECONCILE",
service_name="nodemgr",status="success"} 16
```

For more information on bulk statistics support, see *UCC Serving Gateway Control Plane Function Metrics Reference*.

Cache Pod Optimization

Feature Description

SMF supports the cache pod optimization to reduce the cache pod query at the GTPC endpoint. The get affinity query is used to receive the affinity information in an outgoing request or response message toward the GTPC endpoint. With this optimization, the GTPC endpoint pod doesn't send the query to the cache pod for the upcoming request messages.

CDL Flush Interval and Session Expiration Tuning Configuration

Feature Description

You can modify the default service-pod parameters to fine-tune the throughput performance and optimize the load performance.

Feature Configuration

To configure this feature, use the following configuration:

```
config
   profile sgw sgw_name
```

```
      timers [ session-expiration-in-secs session_expiration |
affinity-expiration-in-secs affinity_expiration | session-dbsync-interval-in-ms
 database_sync ]
      end
```

NOTES:

- **session-expiration-in-secs** *session_expiration* —Specify the duration for which the session is cached on service pod. *session_expiration* accepts value in the range of 1-600 milliseconds. The default value is 30 milliseconds.
- **affinity-expiration-in-secs** *affinity_expiration* —Specify the duration for which the session affinity keys are valid on the service pod and other pods. *affinity_expiration* accepts value in the range of 1-1200 seconds. The default value is 80 seconds.
- **session-dbsync-interval-in-ms** *database_sync* —Specify the duration after which the session is synchronized in the database. *database_sync* accepts value in the range of 1-10000 milliseconds. The default value is 500 milliseconds.

Domain-based User Authorization Using Ops Center

Feature Description

SMF and cnSGW-C support domain-based user authorization using the Ops Center. To control the access on a per-user basis, use the TACACS protocol in Ops Center AAA. This protocol provides centralized validation of users who attempt to gain access to a router or NAS.

Configure the NETCONF Access Control (NACM) rules in the rule list. Then, map these rules in the Ops center configuration to map the group to appropriate operational authorization. Use the configurations that are based on the following criteria and products:

- With the NACM rules and SMF domain-based group, configure the Ops center to allow only access or update SMF-based configuration.
- With the NACM rules and cSGW-C domain-based group, configure the Ops center to allow only access or update cSGW-C-based configuration.
- With the NACM rules and cSGW-C domain-based group, configure the Ops center to allow only access or update CCG-based configuration.

Note The NSO service account can access the entire configuration.

How it Works

To support this feature configuration in Ops Center, the domain-based-services configuration is added in the TACACS security configuration. The TACACS flow change works in the following way:

- If you have configured the **domain-based-services** parameter, then the configured user name that is sent to the TACACS process, splits user ID into user ID and domain. The split character, which is a domain

delimiter, is configured in domain-based-services. These split characters can be "@", "/", or "\" and are used in the following format to get the domain and user ID information.

- @ — <user id>@<domain>
- / — <domain>/<user id>
- \ — <domain>\<user id>

- The TACACS authenticates and authorizes as per the existing flow. However, if the domain-based-services feature is enabled and TACACS authenticates and authorizes the user, following steps are added to the TACACS flow procedure.
  - If Network Services Orchestrator (NSO) logs in as the NSO service account, then that session receives a specific NACM group that you configured in **domain-based-services nso-service-account group** *group-name*. This functionally is the same as the way NSO works.
  - If the specified domain exists in the group mapping, then the NACM group that you configured in **domain-based-services domain-service** *domain* **group** *group-name* is applied.
  - If the user does not have a domain or the domain does not exist in the domain to group mapping, then **no-domain** NACM group that you configured in **domain-based-services no-domain group** *group-name* is applied. If the **no-domain** configuration does not exist, then the user value is rejected.

To enable this feature, you must configure the **domain-based-services** CLI command with the following options:

- NSO service account
- Domain service
- Domain delimiter
- No domain

Feature Configuration

To enable domain-based user authorization using Ops Center, use the following sample configuration:

```
config
   tacacs-security domain-based-services [ domain-delimiter delimiter_option
 | domain-service domain_service_name [ group service_group_name ] | no-domain
group service_group_name | nso-service-account [ group service_group_name | id
service_account_id ] ]
   end
```

NOTES:

- **domain-based-services [domain-delimiter** *delimiter_option* **| domain-service** *domain_service_name* **[group** *service_group_name* **] | no-domain group** *service_group_name* **| nso-service-account [group** *service_group_name* **| id** *service_account_id* **]]**: Configure the required domain-based-services value. The **domain-based-services** includes the following options:
  - **domain-delimiter**: Specify the delimiter to use to determine domain. This option is mandatory and allows the following values:

- @—If domain-delimiter is "@", the user value is in the format: <user>@<domain>.
- /—If domain-delimiter is "/", the user value is in the format: <domain>/<user>.
- \—If domain-delimiter is "\", the user value is in the format: <domain>\<user>.

- **domain-service**: Specify the list of domains and their group mapping. The key is the name of the domain and group is the group that is assigned to the domain. You must configure at least one option in this list.
- **no-domain**: Specify the group that has no domain or if the domain is unavailable in the domain-service mapping, then this group is sent in the accept response.
- **nso-service-account**: Specify the NSO service account that has the ID and group. If you configure this parameter, then you must configure the ID and group fields. The ID and group must have string values.

Configuration Example

The following is an example of the domain-based user authorization in the tacacs-security mode:

```
config
   tacacs-security domain-based-services nso-service-account id nsid
      tacacs-security domain-based-services nso-service-account group nso-group
   tacacs-security domain-based-services no-domain group read-operational
   tacacs-security domain-based-services domain-delimiter @
   tacacs-security domain-based-services domain-service etcd
      group etcd
exit
tacacs-security domain-based-services domain-service sgw
   group sgw_1
exit
tacacs-security domain-based-services domain-service smf
   group smf
exit
```

Configuration Verification

To verify the configuration, use the following show command:

show running-config tacacs-security

The output of this show command displays all the configurations of the domain-based services within the TACACS security.

```
[smf] smf# show running-config tacacs-security
tacacs-security service smf
tacacs-security server 1
address 209.165.200.234
key $8$+twbdL2ZCgmjVswgp7kFJp8+SMXDjQRTZgoPVa3oEwY=
exit
tacacs-security domain-based-services nso-service-account id nsid
tacacs-security domain-based-services nso-service-account group nso-group
tacacs-security domain-based-services no-domain group read-operational
tacacs-security domain-based-services domain-delimiter @
tacacs-security domain-based-services domain-service etcd
group etcd
exit
tacacs-security domain-based-services domain-service sgw
```

```
group sgw_1
exit
tacacs-security domain-based-services domain-service smf
group smf
exit
```

Edge Echo Implementation

Feature Description

In a nonmerged mode, the udp-proxy pod acts as an endpoint, and the gtpc-ep responds to the Echo Requests from the peer node.

The gtpc-ep experiences traffic when the system receives a high number of inputs CEPS leading to a discrepancy between the rate at which gtpc-ep picks up the messages from udp-proxy and the rate at which udp-proxy gets the messages.

If the gtpc-ep is loaded, the queue between the udp-proxy and gtpc-ep gets full, and some of the messages at udp-proxy might get dropped. The peer detects path failure if these are Echo Request messages because an Echo Response is not received. Further, the peer clears all the sessions sent to the sgw-service.

How it Works

This section describes how this feature works.

Nodemgr processes the Echo Request in the following steps:

- The nodemgr preserves a self-restart counter cache for each GR instance ID and the GTPC peer.
- When the udp-proxy pod receives an Echo Request from a peer and the self-restart counter value is not available in the self-restart counter cache, the udp-proxy pod forwards the Echo Request to gtpc-ep.
- The gtpc-ep sends the self-restart counter as part of the UDP proxy message metadata in the Echo Response. The udp-proxy stores the self-restart counter in the self-restart counter cache. When the udp-proxy receives an Echo Request from a peer, and a self-restart counter value is available in the self-restart counter cache, the udp-proxy sends an Echo Response with the restart counter.
- The udp-proxy forwards the Echo Request message to the gtpc-ep. The gtpc-ep processes the Echo Request and forwards it to nodemgr, if necessary.
- If the peer restart counter value is modified, the nodemgr detects a path failure.
- In the Echo Response, the gtpc-ep sends the self-restart counter in the UDP Proxy Message metadata to the udp-proxy. If the self-restart counter differs from the counter that is stored in the self-restart counter cache, the udp-proxy updates the self-restart counter in the cache and drops the Echo Response received from the gtpc-ep.

Note The Edge Echo feature is not supported when the gtpc-ep is started in the merged mode.

Heartbeat

To handle the Echo Request and Echo Response messages for the GTPV2 interface, a heartbeat queue is implemented between the gtpc-ep and the udp-proxy pod. The heartbeat queue is responsible for handling the HeartBeat Request and HeartBeat Response Messages between the protocol and udp-proxy pod for the PFCP interface.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following statistics are supported for the Edge Echo Implementation feature:

- Heartbeat queue status:

```
sum(irate(ipc_response_total{rpc_name~=".ipc_stream_hb."}[10s])) by
(service_name,
instance_id, status, status_code, rpc_name, dest_host)
```

- Check the EdgeEcho messages:

```
sum(irate(udp_proxy_msg_total{ message_name ="edge_echo"}[30s])) by
(message_name,
message_direction, status)
```

To enable the Heartbeat queue and EdgeEcho messages statistics, configure the trace-level statistics for udp_proxy_msg_total using the following:

```
infra metrics verbose application
   metrics udp_proxy_msg_total level trace
   exit
```

Note Enabling the heartbeat and EdgeEcho messages statistics may lead to a performance degradation on the udp-proxy pod.

Encoder and Decoder Optimization for GTPC Endpoint Pod

Feature Description

SMF uses the **enable-direct-encdec** CLI command to optimize the encoding and decoding of the IEs that are associated with the GTPC endpoint pod. This optimization improves the memory management and reduces the garbage collection time.

Feature Configuration

You can enable this feature at run time. By default this feature is disabled.

To configure this feature, use the following sample configuration:

```
config
  instance instance-id instance_id
    endpoint gtp
    interface s5e
      enable-direct-encdec true | false
    interface s11
      enable-direct-encdec true | false
    exit
  exit
```

NOTES:

- **enable-direct-encdec true | false**: Choose the value as **true** to enable the encoder and decoder. By default, the value of this field is **false**.

ETCD Peer Optimization Support

Feature Description

When large numbers of GTPC peers are connected with SMF or cnSGW-C, the performance of ETCD is impacted. Each peer is a considered as a record in the ETCD, and the timestamp is updated every 30 seconds for each peer. This causes continuous updates on ETCD and generates huge traffic that impacts the overall system performance.

The ETCD Peer Optimization feature facilitates optimization in peer management and enables reduced performance impact on ETCD.

How it Works

This section describes how this feature works.

Instead of considering each peer as an ETCD record entry, several peers are grouped as a peer group based on the hash value of the IP address of each peer. This reduces the number of entries in ETCD. By default, a maximum of 200 peer groups can be created. For any changes related to a peer in a peer group:

- For a new peer, the peer group is persisted immediately in ETCD.
- For the change in timestamp for existing peers, the peer group is updated once every 3 seconds. This update:
  - Results in a cumulative group update for many peers that have undergone timestamp change within each peer group.
  - Reduces frequent updates to ETCD.

Roaming Peer Optimization

Feature Description

SMF identifies the peer nodes as roaming in the following two ways:

- **Roaming Peer Detection Based on Interface:** By configuring the S8 interface and let the CSR, MBR, and Echo Requests come via S8 to identify them as roaming peers.
- **Roaming Peer Detection by Application:** By configuring the serving network as roaming PLMN and let the messages come via S5 interface. Then, identify a peer as roaming if it appears in the list with the type as roaming.

How It Works

This section describes the way SMF detects and optimizes the roaming peers.

Roaming Peer Detection Based on Interface

SMF supports the configuration of S8 VIP under endpoint GTP. If a Create Session Request/Modify Bearer Request/Echo Request (CSR/MBR) from the peer lands on S8 VIP, the SMF marks the peer as ROAMING SGW and also updates the peer-type.

Roaming Peer Detection by Application

SMF supports PLMN-list configuration under the SMF profile. The SMF compares the serving and the UE-PLMN with the configured plmns to decide if the session is homer or roamer.

If the UE-PLMN is found listed in the configured PLMN list and the serving-PLMN is not found in the configured PLMN list, the session is marked as roamer (outbound roamer).

Upon getting a CSR for fresh session create or MBR for handoff, the SMF services detect that the session is a roamer session.

Note It is assumed that the first downlink control message from SMF to a partner SGW is a Create Session Response or a Modified Bearer Response.

Peer Optimization

Upon getting a CSR/MBR/Echo Request from a peer over S8 interface, the SMF marks the peer as Roaming SGW and uses the path management-related configuration done for the S8 interface.

There is no difference in path failure detection logic for partner SGWs. Upon detecting the session as roaming session via the S5 interface, SMF marks the peer as Roaming SGW and updates the path management-related configuration done for the S8 interface.

SMF provides an option to disable the path management by disabling the Echo for S8 interface. Disabling Echo can be done by configuring the Echo Interval as 0. In this case, no Echo would be initiated from the SMF for the roaming SGWs.

SMF, by default, adds a route for roaming SGW, if there is no VRF association at the VIP interface. If the VRF association exists, then SMF will not install the routes.

Note A smaller cp-idle/up-idle timeout for roamer sessions is recommended so that peer restart impact can be minimized. It can minimize the (stale session) non-detection of peer path failure or peer restart.

Limitations

Following is the known limitation of roaming peer optimization in SMF:

- If Echo is disabled for roaming SGW, the SMF will not do any peer path management based on the restart counter.

Feature Configuration

SMF optimizes the roaming peers using the following configuration:

```
config
   instance instance-id gr_instance_id
   endpoint gtp
      interface { s2b | s5 | s5e | s8 | s11 }
      echo interval echo_interval
      echo retransmission-timeout retransmission_timeout_value
      echo max-retransmissions max_retry_count
      end
```

NOTES:

- **interval** *echo_interval*—The echo interval range is <300-3600> seconds. The default value is Default 300 seconds. Configuring echo interval with 0 second disables the outbound echo. This change is applicable irrespective of the interface type. For other interfaces like s2b, s5, s5e, and s11, the echo interval range is <60-3600> seconds.
- **retransmission-timeout** *retransmission_timeout_value*—The retransmission timeout range for the S8 interface is <60-180> seconds. The default value is 60 seconds. For other interfaces like s2b, s5, s5e, and s11, the retransmission-timeout range is <1-20> seconds.
- **max-retransmissions** *max_retry_count*—The value range of maximum number of retries for GTP Echo Request is 0-4. The default value is 4. For other interfaces like s2b, s5, s5e, and s11, the max-retransmissions range is <0-10>.

Note These parameters are applicable only for the S8 interface. For other interfaces, the existing configuration is applicable.

Configuration Example

Sample configuration of S8 interface:

```
[unknown] smf# config
Entering configuration mode terminal
[smf] smf(config-instance-id-1)# endpoint gtp
[smf] smf(config-endpoint-gtp)# interface s8
[smf] smf(config-interface-s8)# vip-ip 192.0.2.1 vip-interface bd2.pgs5.3051
echo interval          300
   echo retransmission-timeout 60
   echo max-retransmissions 4
  exit
```

Configuration Verification

The `show peers` command displays all the roaming SGWs and their node information.

```
[smf] smf# show peers all
GR INSTANCE ENDPOINT LOCAL ADDRESS PEER ADDRESS DIRECTION POD INSTANCE TYPE CONNECTED TIME
 RPC ADDITIONAL DETAILS INTERFACE NAME VRF
```

```
1 N4 10.1.3.185:8805 10.1.3.234:8805 Inbound nodemgr-1 Udp 4 hours UPF Capacity:
65535,LoadMetric: 0,LoadSeqNo: 0,Mode: Online,OverloadMetric: 0,OverloadSeqNo: 0,Priority:
 65535  N4 NA
1 S5/S8 10.1.3.248:2123 10.1.3.245:2123 Inbound nodemgr-0 Udp 4 hours SGW MaxRemoteRcChange:
 N/A,Recovery: 100 S8 NA
1 S5/S8 10.1.1.23:2123  10.1.3.245:2123 Inbound nodemgr-0 Udp 4 hours SGW MaxRemoteRcChange:
 N/A,PeerType: Roaming,Recovery: 100 S5 NA
```

ETCD Traffic Optimization

Extended Distributed Key Value (ETCD) is a distributed key-value store used to store configuration data, state data, and other data used by distributed systems.

Feature Description

The current implementation of the topology data in Extended Distributed Key Value (ETCD) stores both internal and external data with specific prefixes, and the application creates context for all the data and handles all the changes in the ETCD data. This behaviour results in lot of traffic towards ETCD from each pod, including some pods that aren't interested in these notifications and records.

To address this issue, this feature allows the pods to opt in/out for these notifications and reloads. This "restricted notifications" and "reload" functionality is optional. With this feature, the notifications are only received for subscribed services and peer data.

Note It's important to retain the current key structure to avoid any impact on the existing production deployment during the upgrade.

ETCD traffic optimization improves the reliability, performance, scalability, and security of distributed systems that rely on ETCD for configuration management and service discovery.

How It Works

There are two major data categories stored in ETCD:

1. Internal topology data, includes instance information, endpoint information, and leader information in the ETCD.
2. External Peer information added by applications.

Both these categories of data are stored in ETCD and are used to store and notify the internal topology data and external peer information data. The current implementation of the topology data and notifications results in increased traffic towards ETCD. The traffic can be reduced by implementing restricted notifications and reload functionality that allows pods to opt in/out for these notifications and reloads.

The current topology data is broadcasted to all the app-infra based pods, including pods that aren't interested in these entries. This results in unwanted notifications from ETCD that can be avoided.

Furthermore, all the data is reloaded every 10 seconds, which means that the records from ETCD and local cache are reconciled. If there's a discrepancy, then a notification is raised. While this approach ensures consistency between ETCD and local cache, it can result in excessive traffic towards ETCD.

To optimize this process, the new implementation is to apply the selective approach to notifications and reloading, where only pods that require certain entries or changes are notified, instead of broadcasting to all pods. Also, instead of reloading all data every 10 seconds, it is efficient to reload only the subscribed data. This selective approach helps to reduce the volume of data between various pods and ETCD and improves the overall performance of the system. As a result, the traffic between ETCD and all the pods is reduced.

The following pods no more receives the external peer data and hence the traffic is reduced:

- cache-pod
- rest-ep
- udp-proxy
- radius-ep
- li-ep
- dns-proxy
- gtpp-ep
- georeplication-pod
- oam-pod

ETCD Client Fallback

Feature Description

The ETCD client implements the following components:

- Balancer that establishes the gRPC connections to an ETCD cluster.

- API client that sends RPCs to an ETCD server.
- Error handler that decides whether to retry a failed request or switch endpoints.

The App-infra-based pods using memory cache in 5G communicate with the ETCD server. This communication is to store their critical data on a distributed system through the ETCD client load balancer. The memory cache uses the ETCD client 3.3 version, which implements the clientv3-grpc1.7 library.

ETCD Client Load Balancer

SMF supports the ETCD client, version 3.4.21, which implements the clientv3-grpc1.14 library. This library is backward compatible.

The clientv3-grpc1.14 library has the following key points:

- Simplify the balancer failover logic instead of maintaining a list of unhealthy endpoints.
- Create multiple subconnections, which implies one subconnection per endpoint, when multiple endpoints are available. For example, in a five-node cluster, clientv3-grpc1.14 balancer requires five TCP connections.
- Provide more flexible load balancer with a better failover performance by preserving the pool of TCP connections.
- Extend the default round robin balancing policy to support other types of balancers, such as power of two and pick leader.
- Use the gRPC resolver group and implement balancer picker policy to delegate complex balancing work to upstream gRPC.
- Implement retry in the gRPC interceptor chain that handles gRPC internal errors automatically and enables advanced retry policies, such as backoff.

ETCD Client Retry Mechanism

After receiving an error for a PUT request, the ETCD client retries this request thrice. The ETCD client performs each retry after a timeout of one second. The ETCD client completes all the three retries within three seconds, which meet the existing SLA with the applications. After three retries, the ETCD client returns the outcome to the application.

Flag DB Database Updates

Feature Description

SMF updates the CDL when the subscriber state changes from idle to active, and when the ULI, UeTz, or the serving network is modified.

When the transaction requests driven to CDL increases, SMF incurs a higher CPU utilization. To prevent the needless CPU utilization, SMF updates only a subset of the CDL with the changed attributes.

Flag DB database is updated for the following SMF procedures:

- MBR with only ULI change—SMF handles MBR with only ULI change, in a stateless way to send the response. After sending the response, the smf-service updates the CDL, which impacts the CPU utilization. To optimize the CPU usage, SMF notifies the CDL about the ULI only with the partial updates.
- 4G RAT Handover—During an inter S-GW handover, the smf-service receives the MBR with a ULI change and the TEID change. To optimize the CPU usage, SMF notifies the CDL about peer TEID and ULI only with the partial updates, if the handover is successful for all the bearers.
- N2 Handover—When the N2 handover procedure ends, the smf-service updates the CDL which impacts the CPU utilization. To optimize the CPU usage, the SMF notifies the CDL about only the ULI and TEID with the partial updates, if the handover is successful for all the existing QFI.

Handling PDU Session Modifications based on RRC Inactive Cause Codes

Feature Description

The Radio Resource Control (RRC) is a layer within the 5G NR protocol stack. It exists only in the control plane, in the UE, and in the gNB. The existing state of PDU sessions controls the behaviour and functions of the RRC.

During the PCF-initiated modification, the AMF sends those received unsuccessful transfer radio networks cause codes in the N2 content of the SmContextUpdate message to the SMF under the following conditions:

- When the Xn-handover is in progress.
- When the AN is released.
- When the UE is in the RRC inactive state.
- When the UE isn’t reachable.

The SmContextUpdate message with the N2 cause codes acts as a bridge and converter from AMF to SMF or from SMF to AMF.

How it Works

This section describes how this feature works.

During the PCF-initiated modification, when the Xn-handover is in progress, the following scenarios are noted:

- The AN gets released or the UE is in RRC inactive state and not reachable.
- The AMF relays the received unsuccessful transfer radio network cause code, in the N2 content of the **SmContextUpdate** message to SMF.
- These cause codes could be standard radio network causes or there could be some customized radio network cause codes being sent from the gNB.

Previously, these cause codes were rejected by the SMF and the PCF was attempting multiple times the same PCF modifications. Now, the SMF doesn't reject immediately, and behaves differently for different cause codes, based on the new N2 trigger configuration to avoid multiple reattempts from the PCF.

The following scenarios are supported in the SMF for the PDU Modify procedure, based on the received N2 cause code:

- When the cause code indicates that the Xn-handover is in progress or the AN gets released, then the following activities occur:
  - The SMF suspends the ongoing PDU session modification.
  - It resumes back after the Xn-handover or the AN Release.
- When the cause code indicates that the UE is RRC inactive and not reachable, then the following activities occur:
  - The SMF rejects the PDU session modification.
  - It reports the rule failure to the PCF.

By default, this feature gets activated for a few standard RRC inactive cause codes with default guard timeout and zero max-retry.

For the following cause codes, the SMF suspends session modification, and resumes only after the Xn-handover activity gets over:

- **_RadioNetwork_NG_intra_system_handover_triggered**
- **_RadioNetwork_NG_inter_system_handover_triggered**

For the following cause codes, the SMF rejects the session modification:

- **_RadioNetwork_UE_in_RRC_INACTIVE_state_not_reachable**

Along with the standard cause codes, a new N2 trigger CLI is introduced to configure the different customized radio network cause codes, and the corresponding SMF actions.

Note The non-roaming PCF-initiated modification scenarios are supported as a part of this feature.

Call Flows

This section describes the key call flows for this feature.

Modifications for PCF-initiated gNB Transfer State

This section describes about the gNB transfer state activities in the PCF-initiated modifications call flow procedure.

The following figure describes Modifications for PCF-initiated gNB Transfer State call flow.

Figure 197: Call Flow for the Modifications for PCF-initiated gNB Transfer State

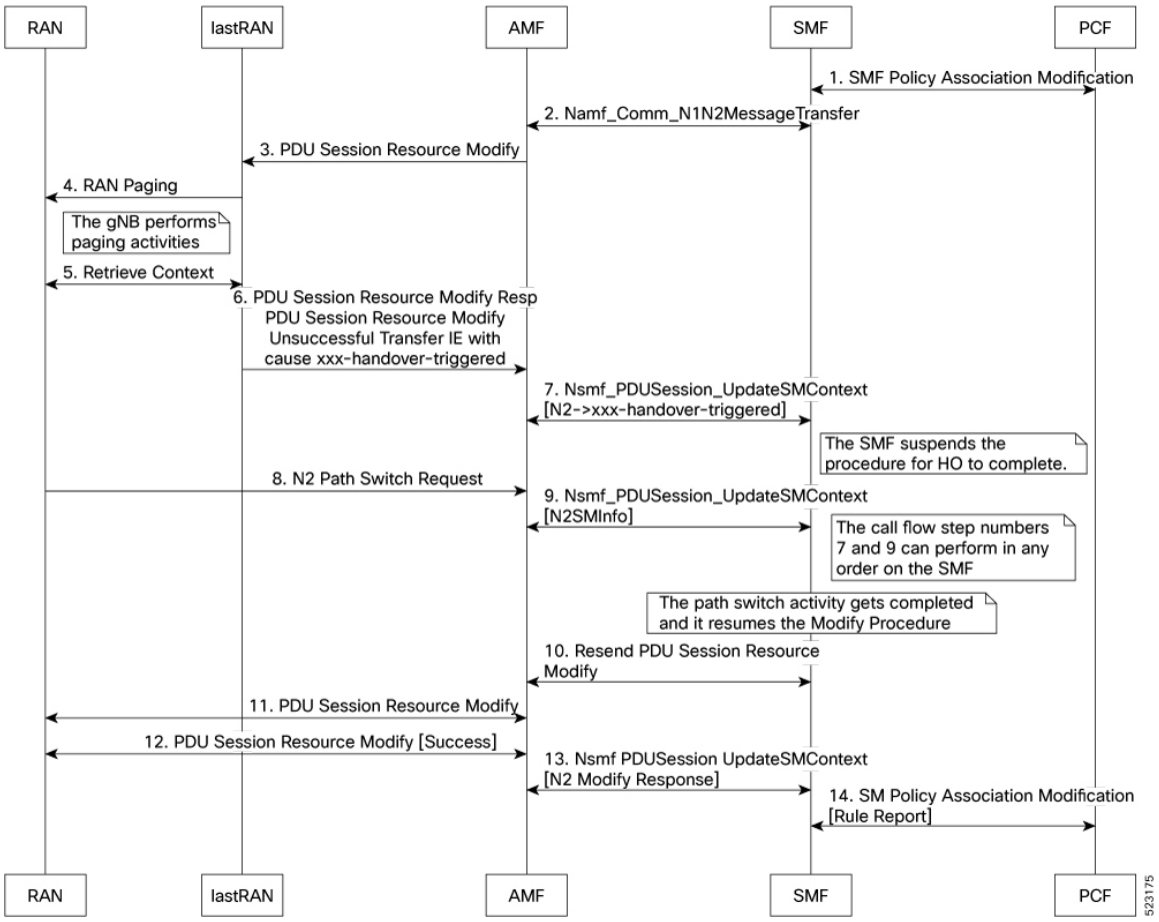


Table 347: Call Flow Description for the Modifications for PCF-initiated gNB Transfer State

Step	Description
1	The PCF sends the SMF Policy Association Modification Request to the SMF. It's an interchangeable action as it also receives the same message from the SMF.
2	The SMF sends the Namf Comm N1N2MessageTransfer Request to the AMF. It's an interchangeable action as it also receives the same message from the AMF.
3	The AMF sends the PDU Session Resource Modify Request to the lastRAN.
4	The lastRAN requests the RAN for paging activities.
5	The gNB performs the paging activities and retrieves the context between the RAN and the lastRAN. The lastRAN sends the Retrieve Context message to the RAN. It's an interchangeable action as it also receives the same message from the RAN.

Step	Description
6	The lastRAN sends the PDU Session Resource Modify Response to the AMF. It also includes the PDU Session Resource Modify Unsuccessful Transfer IE with cause xxx-handover-triggered message.
7	The AMF processes and sends the Nsmf PDUSession UpdateSMContext message (N2 to xxx-handover-triggered) to the SMF. It's an interchangeable action as it also receives the same message from the SMF. **Note** During this step, the SMF suspends the further procedure and initiates the HO to complete it.
8	The RAN sends the N2 Path switch Request to the AMF.
9	The AMF sends the Nsmf PDUSession UpdateSMContext (N2SMlnfo) response message to the SMF. **Note** The steps number 7 and 9 can proceed in any order towards the SMF or from the AMF.
10	The SMF resends the PDU Session Resource Modify message to the AMF. It's an interchangeable action as it also receives the same message from the AMF. **Note** During this step, the path switch gets completed and it resumes the modify procedure.
11	The AMF sends the PDU Session Resource Modify message to the RAN. It's an interchangeable action as it also receives the same message from the RAN.
12	The RAN sends the success note PDU Session Resource Modify (success) message to the AMF. It's an interchangeable action as it also receives the same message from the AMF.
13	The AMF sends the modified response Nsmf PDUSession UpdateSMContext (N2 modify response) message to the SMF. It's an interchangeable action as it also receives the same message from the AMF.
14	The SMF sends the report SM Policy Association Modification (rule report) message to the PCF. It's an interchangeable action as it also receives the same message from the PCF.

Modifications for PCF-initiated UE Not Reachable State

This section describes about the UE not reachable state activities in the PCF-initiated modification call flow procedure.

The following figure describes the Modifications for PCF-initiated UE Not Reachable State.

Figure 198: Call Flow for the Modifications for PCF-initiated UE Not Reachable State

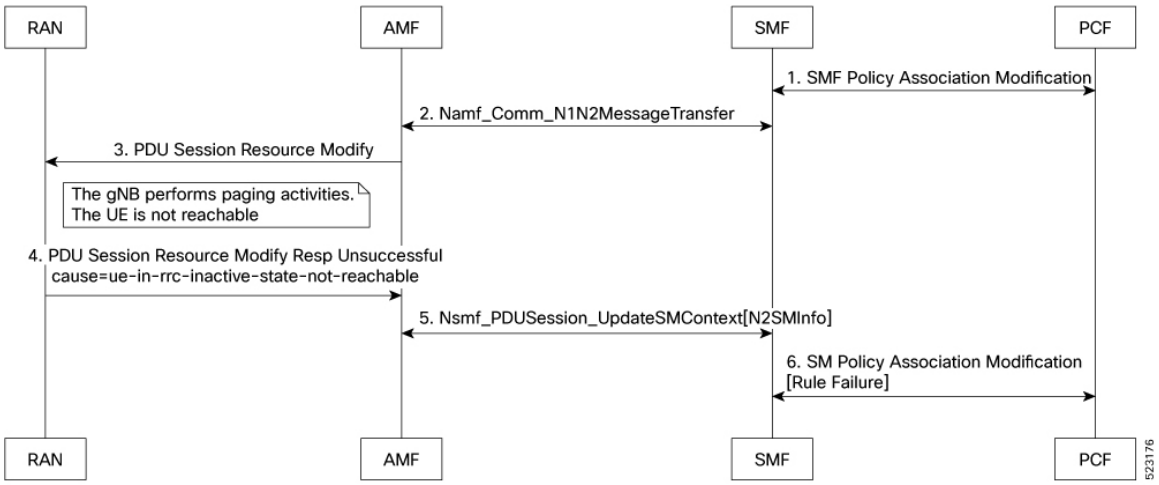


Table 348: Call Flow Description for the Modifications for PCF-initiated UE Not Reachable State

Step	Description
1	The PCF sends the SMF Policy Association Modification Request to the SMF. It's an interchangeable action as it also receives the same message from the SMF.
2	The SMF sends the Namf Comm N1N2MessageTransfer Request to the AMF. It's an interchangeable action as it also receives the same message from the AMF.
3	The AMF sends the PDU Session Resource Modify Request to the RAN. **Note** During this step, the gNB performs the paging activities as the UE isn't reachable.
4	The RAN sends the PDU Session Resource Modify Response Unsuccessful message to the AMF. It also includes the failure cause ue-in-rrc-inactive-state-not-reachable message.
5	The AMF sends the Nsmf PDUSession UpdateSMContext (N2SMInfo) response message to the SMF. It's an interchangeable action as it also receives the same message from the SMF.
6	The SMF sends the failed report SM Policy Association Modification (rule failure report) message to the PCF. It's an interchangeable action as it also receives the same message from the PCF.

Modifications for PCF-initiated Inactive to Idle State

This section describes about the inactive to idle state activities in the PCF-initiated modification call flow procedure.

The following figure describes the Modifications for PCF-initiated Inactive to Idle State call flow.

Figure 199: Call Flow for the Modifications for PCF-initiated Inactive to Idle State

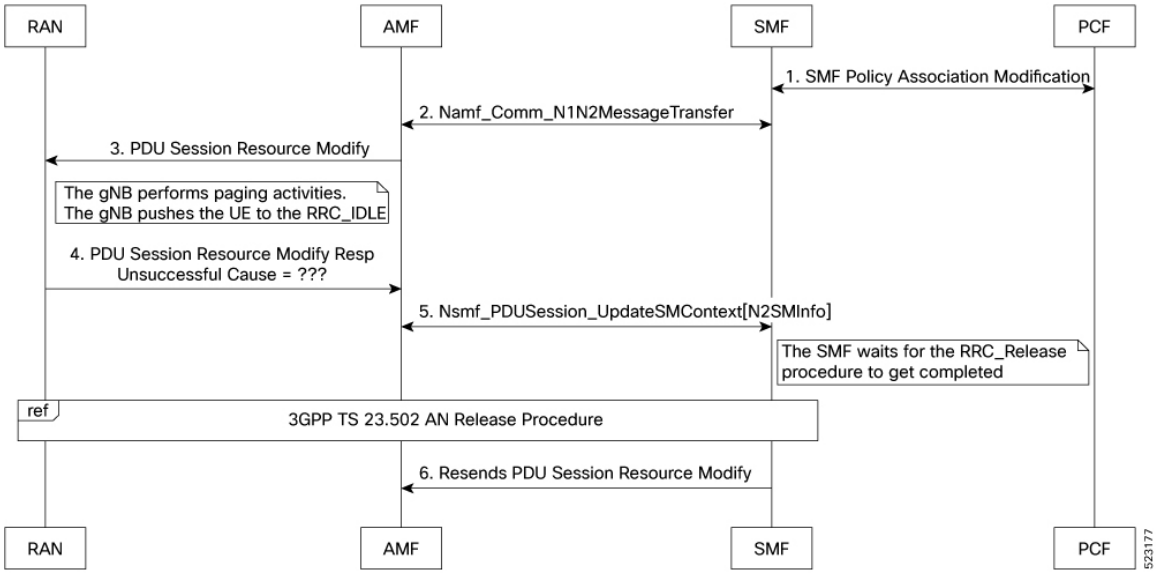


Table 349: Call Flow Description for the Modifications for PCF-initiated Inactive to Idle State

Step	Description
1	The PCF sends the SMF Policy Association Modification Request to the SMF. It's an interchangeable action as it also receives the same message from the SMF.
2	The SMF sends the Namf Comm N1N2MessageTransfer Request to the AMF. It's an interchangeable action as it also receives the same message from the AMF.
3	The AMF sends the PDU Session Resource Modify Request to the RAN. **Note** During this step, the gNB performs the paging activities as the gNB pushes the UE to the RRC_IDLE mode.
4	The RAN sends the PDU Session Resource Modify Response Unsuccessful message to the AMF. It also includes the unknown failure cause message.
5	The AMF sends the Nsmf PDUSession UpdateSMContext (N2SMInfo) response message to the SMF. It's an interchangeable action as it also receives the same message from the SMF. **Note** During this step, the SMF waits for the RRC_Release procedure to get completed.
6	The SMF resends the PDU Session Resource Modify message to the AMF. **Note** This step follows the 3GPP TS 23.502 AN release procedure.

Feature Configuration

To configure this feature, use the following sample configuration:

```
config
profile access access_profile_name
   n2 trigger { ho-in-progress | temp-not-reachable } { guard-timeout
timeout | max-retry retry_count | value retry_count_range }
   n2 trigger ue-not-reachable value notreachable_count_range
   end
```

NOTES:

- **profile access** *access_profile_name*—Specify a name for the access profile.
- **n2 trigger**—Specify the N2 trigger type. Trigger can be the traffic type. Must be one of the following:
  - **ho-in-progress**—Specify the handover-in-progress trigger configuration list of cause-codes.
  - **temp-not-reachable**—Specify the temporary not reachable trigger configuration list of cause-codes.
  - **ue-not-reachable**—Specify the UE not reachable trigger configuration list of cause-codes.
- **guard-timeout** *timeout*—Specify the Handover in progress guard timeout in milliseconds, within the range of 500-30000 milliseconds. The default value is 10000 milliseconds.
- **max-retry** *retry_count*—Specify the maximum retry count value for the handover in progress or temporary not reachable options, within the range of 0-64. The default value is 0.
- **value** { *notreachable_count_range* } | { *retry_count_range* }—The numbered value in the range of counts for UE not reachable or the maximum retry range.

Note The defined configurations are used to match the received unsuccessful transfer (radio network standard and customized) causing the code to decide the RRC inactive action. It has the following scenarios:

- The PCF-initiated modification gets rejected in the case of **ue-not-reachable**, **ho-in-progress**, and **temp-not-reachable** cases. It gets suspended and resumes back after the xn-handover activities in the AN release.
- The Guard Timer gets started, when the RRC inactive action is either in the **ho-in-progress** or the **temp-not-reachable** trigger profile. It waits for the ongoing PCF-initiated modification to suspend. It restarts the xn-handover activities in the AN release within the given time. If this action fails, then the PCF-initiated modification gets rejected. As a result, this action reported as the rule failure note to the PCF.
- The maximum retry allows the maximum continuous reattempt after the first attempt gets failed. It's a result of receiving the same trigger category cause code repeatedly for each and every attempt. If this action fails, the PCF-initiated modification gets rejected. As a result, this action reported as the rule failure note to the PCF, after reaching the maximum retry attempt.
- This feature gets activated for the standard RRC inactive cause codes with a default guard timeout and zero maximum-retry.

Configuration Example

The following is an example configuration.

```
config
smf(config)# profile access access1
 smf(config-access-access1)# n2 trigger [ ho-in-progress | temp-not-reachable ] [ value 1
] [ guard-timeout 10000 ] [ max-retry 10 ]
 smf(config-access-access1)# n2 trigger ue-not-reachable value [10]
 exit
exit
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config profile access access1 n2
profile access access1
  n2 trigger ho-in-progress value [ 50 51 52 53 ] guard-timeout 12000 max-retry 3
  n2 trigger temp-not-reachable value [ 54 55 56 57 ] guard-timeout 11000 max-retry 2
  n2 trigger ue-not-reachable value [ 58 59 60 61 ]
exit
```

Pod Failure Detection using K8 Liveness Probe

Kubernetes uses Liveness probe to periodically monitor the health of all pods. With this mechanism, it is easy to detect the pod failures. The K8 configuration parameter values for Liveness probe are adjusted to enable faster detection of pod failures and timely restart of faulty pods.

The configuration changes are applicable to the following pods:

- bgpspeaker-pod
- cache-pod
- diameter-ep
- dns-proxy
- edr-monitor
- georeplication-pod
- gtpc-ep
- gtpc-ep-s11
- gtpp-ep
- li-ep
- nodemgr
- oam-pod (infra-oam)
- protocol
- radius-ep
- rest-ep

- sgw-service
- smf-service
- udp-proxy

The early detection of pod failures by K8 enables backup or standby pod to take over message processing and achieve seamless communication.

Resiliency Handling

Feature Description

The Resiliency Handling feature introduces a CLI-controlled framework to support the service pod recovery, when you observe a system fault or a reported crash. It helps in recovering one of the following service pods:

- sgw-service pod
- smf-service pod
- gtpc-ep pod
- protocol pod
- diameter-ep pod

These service pods are software modules containing the logic to handle several session messages. The service pods are fault-prone due to any one of the following or a combination of multiple scenarios:

- Complex call flow and collision handling
- Inconsistent session state
- Incorrect processing of inbound messages against the session state
- Unexpected and unhandled content in the inbound messages

Whenever you observe the system fault or a crash, the fault behavior results into a forced restart of the service pod. It impacts the ongoing transaction processing of other sessions. The crash reoccurs even after the pod restart.

To mitigate this risk, use the CLI-based framework with actions defined to clean up subscriber sessions or terminate the current processing.

How it Works

This section describes how you can use the fault recovery framework to define actions for the crash. The framework allows you to define any of the following actions:

- Terminate—When a fault occurs, this action terminates the faulty transactions, and clears the subscriber session cache. It’s applicable for smf-service and sgw-service pods.

Note The pod doesn't get restarted. The database doesn't get cleared during this action.

- Cleanup—When a fault occurs, this action clears the faulty subscriber session and releases the call. It's applicable for smf-service and sgw-service pods.
- Graceful reload—When a fault occurs, this action restarts the pod. It's applicable for gtpc-ep, protocol, and diameter-ep pods. It handles the fault signals to clean up resources, such as the keepalive port and closes it early. It also allows the checkport script to detect the pod state and initiates the VIP switch processing for the corresponding pods.
- Reload—When the pod crashes, it initiates the reloading activity. It's a default setting or value applicable for all the pods.

Feature Configuration

To configure this feature and to enable the system fault recovery, use the following sample configuration:

```
config
   system-diagnostics { diameter |  gtp | pfcp | service | sgw-service }

      fault
         action { abort | cleanup { file-detail | interval | num | skip
{ ims | emergency | wps } } | graceful-Reload | reload }
         end
```

NOTES:

- **system-diagnostics { diameter | gtp | pfcp | service | sgw-service }**—Specify the required type of service pods for system diagnostics. The available pod options are diameter, gtp, pfcp, smf-service, and sgw-service.
- **fault**—Enables fault recovery while processing sessions.
- **action { abort | cleanup | graceful-Reload | reload }**—Specify one of the following actions to take on fault occurrence. The default action is reload.
  - **abort**—Deletes the faulty transaction and clears its session cache. The database doesn't get cleared.

Note It's an exclusive option to the smf-service pod.

  - **cleanup { file-detail | interval | num | skip }**—Enable the cleanup activity. It has the following selections to mitigate the fault action:
    - **file-detail**—Lists the file names with line numbers. It excludes the file name details from the recovery.
    - **interval**—Specifies the duration of the interval in minutes. This duration specifies the permissible interval within which it allows the maximum number of faults. Must be an integer in the range 1–3600.

- **num**—Specifies the maximum number of tolerable faults in an interval. Must be an integer in the range 0–50.
- **skip { ims | emergency | wps }**—Enable the skip cleanup of a subscriber session for an active voice call, or the WPS, or an emergency call.
  - To detect the active voice calls, use the following command:

    profile dnn *dnn_name* **ims mark qci** *qos_class_id*
  - When you enable the skip cleanup configuration, the SMF deletes the faulty transaction, and clears its session cache.
  - When a fault occurs during the session setup or the release state, the SMF performs the following:

    – Deletes the transactions on the session end.

    – Overrides the configured fault action during these states.

    – Clears the session cache and database entries for the faulty transaction.
  - It allows the dynamic configuration change.

Note It's an exclusive option to smf-service and sgw-service pods.

- **graceful-Reload**—Specify the option to gracefully reload the pod. The service pod handles fault signals to clean up resources like the keepalive port and continues with crash processing (pod restart processing).

Note It's an exclusive option to diameter-ep, gtpc-ep, and protocol service pods.

- **reload**—Reloads the pod, when it crashes due to a faulty behavior. It's an option applicable to all the service pods. It’s also the default option.

Configuration Example

The following example configuration allows three crashes of smf-service or sgw-service pods, within a duration of 10 minutes interval, and with the fault occurrence action as subscriber cleanup.

```
config
    system-diagnostics { service | sgw-service }
        fault
            num 3 interval 10
            action cleanup
            end
```

The following example configuration allows graceful fault handling for the diameter or gtpc-ep pod or the protocol pod to close the keepalive port on receiving a fault signal.

```
config
    system-diagnostics { diameter | gtp | pfcp }
        fault
```

```
            action graceful-Reload
            end
```

Configuration Verification

To verify the configuration:

```
smf# show running-config system-diagnostics service
 fault num 3
 fault interval 10
 fault action cleanup
exit

show running-config system-diagnostics sgw-service
 fault num 3
 fault interval 10
 fault action cleanup
exit

show running-config system-diagnostics gtp
 fault action graceful-Reload
exit

show running-config system-diagnostics pfcp
 fault action graceful-Reload
exit

show running-config system-diagnostics diameter
 fault action graceful-Reload
exit
```

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Bulk Statistics Support

The following bulk statistics are supported for the resiliency handling feature.

recover_request_total—This statistic includes the following new labels:

- **action**—Defines the fault action.
- **reason**—Defines the fault reason.
- **status**—Defines the fault status.

The following is an example of bulk statistics for the resiliency handling feature.

```
recover_request_total{action="panic_recovery_cleanup",
app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
reason="creating panic",service_name="sgw-service",status="success"} 1
```

For more information on bulk statistics support for SMF, see the *UCC 5G SMF Metrics Reference* document.

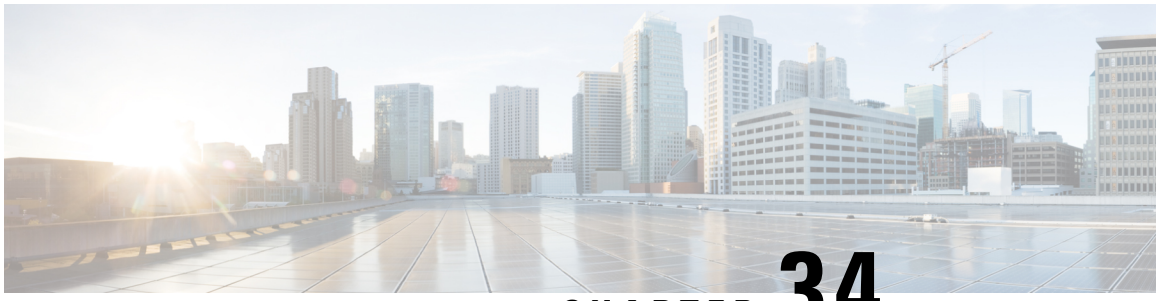
For more information on bulk statistics support for cnSGW-C, see the *UCC 5G cnSGW-C Metrics Reference* document.

Monitoring Support

To monitor the system faults and determine the fault recovery actions applied for multiple pods, use the error logs with the following transaction errors:

- Txn error type 10003 (`ErrorPanicRecovery`) for cleanup action
- Txn error type as 1802 (`ErrorAffinityAddEntryFailed`) for skip cleanup and abort actions.

Note The monitoring support for Resiliency Handling feature is only applicable in the SMF.



CHAPTER 34

Pods and Services Reference

- Feature Summary and Revision History, on page 973
- Feature Description, on page 974
- Associating Pods to the Nodes, on page 983
- Viewing the Pod Details and Status, on page 983
- GTPC Protocol Endpoint Merge with UDP Proxy Bypass, on page 985
- UDP Proxy Functionality Merge into Protocol Micro-services, on page 985

Feature Summary and Revision History

Summary Data

Table 350: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 351: Revision History

Revision Details	Release
The node-monitor pod is supported to enable monitoring of all K8 pods.	2021.02.0
The grafana-dashboard-app-infra pod is removed.	2021.02.3.t3
First introduced.	Pre-2020.02.0

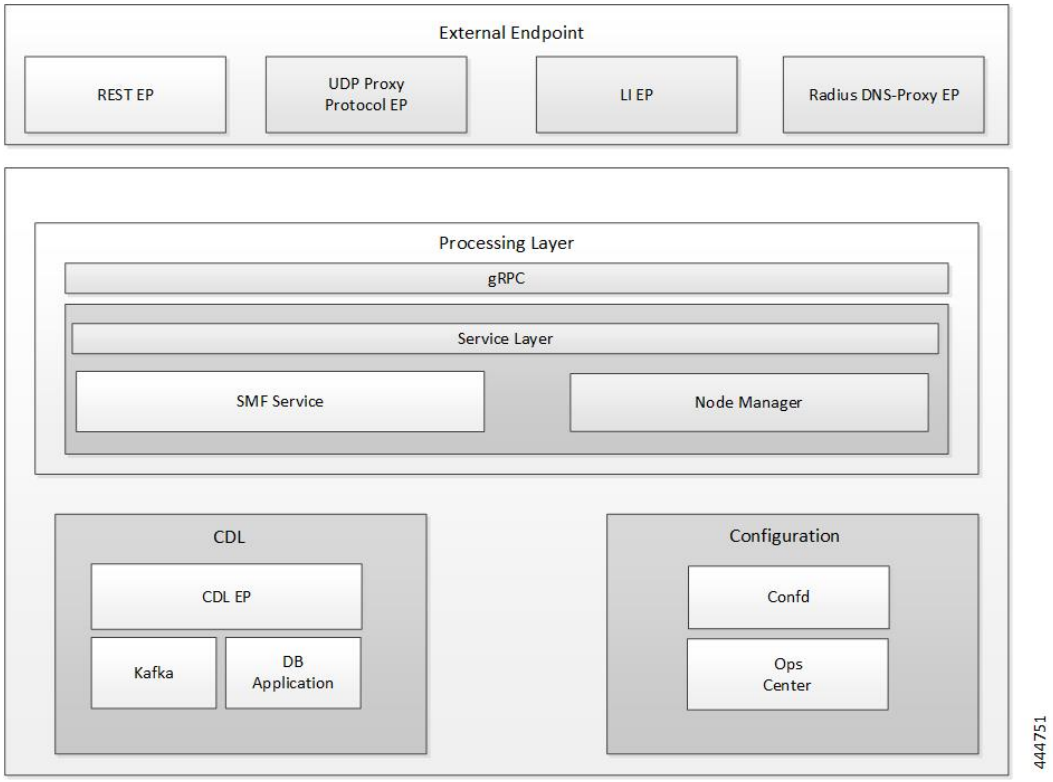
Feature Description

The SMF is built on the Kubernetes cluster strategy, which implies that it has adopted the native concepts of containerization, high availability, scalability, modularity, and ease of deployment. To achieve the benefits offered by Kubernetes, SMF uses the construct that includes the components, such as pods and services.

Depending on your deployment environment, the SMF deploys the pods on the virtual machines that you have configured. Pods operate through the services that are responsible for the intrapod communications. If the machine hosting the pods fails or experiences network disruption, the pods are terminated or deleted. However, this situation is transient and Kubernetes spins new pods to replace the invalid pods.

The following workflow provides a high-level visibility into the host machines, and the associated pods and services. It also represents how the pods communicate with each other. The representation may differ based on your deployment infrastructure.

Figure 200: Communication Workflow of Pods



Kubernetes deployment includes the kubectl command-line tool to manage the Kubernetes resources in the cluster. You can manage the pods, nodes, and services.

For information on the Kubernetes concepts, see the Kubernetes documentation.

For more information on the Kubernetes components in SMF, see the following:

- Pods
- Services

Pods

A pod is a process that runs on your Kubernetes cluster. Pod encapsulates a granular unit known as a container. A pod contains one or multiple containers.

Kubernetes deploys one or multiple pods on a single node which can be a physical or virtual machine. Each pod has a discrete identity with an internal IP address and port space. However, the containers within a pod can share the storage and network resources.

The following table lists the SMF pod names and the hosts on which they are deployed depending on the labels that you assign. For information on how to assign the labels, see Associating Pods to the Nodes.

Table 352: SMF Pods

Pod Name	Description	Virtual Machine Name
api-smf-ops-center	Functions as the *confD* API pod for the SMF Ops Center.	OAM
base-entitlement-smf	Supports Smart Licensing feature.	OAM
cache-pod	Operates as the pod to cache any sort of system information that will be used by other pods as applicable.	Protocol
cdl-ep-session	Provides an interface to the CDL.	Session
cdl-index-session	Preserves the mapping of keys to the session pods.	Session
cdl-slot-session	Operates as the CDL session pod to store the session data.	Session
dns-proxy	Operates as DNS endpoint of SMF	Protocol
diameter-ep-gx-client	Operates as a Diameter endpoint to enable communication between SMFand PCRF through Gx interface	Protocol
diameter-ep-gy-client	Operates as a Diameter endpoint to enable communication between SMF and PCRF through Gy interface	Protocol
documentation	Contains the documentation.	OAM
edr-monitor pod	Contains the EDR files that are maintained in a persistent volume.	OAM
etcd-smf-etcd-cluster	Hosts the etcd for the SMF application to store information, such as pod instances, leader information, NF-UUID, endpoints, and so on.	OAM
grafana-dashboard-cdl	Contains the default dashboard of CDL metrics in Grafana.	OAM
grafana-dashboard-smf	Contains the default dashboard of SMF service metrics in Grafana.	OAM
gtpc-ep	Operates as GTPC endpoint of SMF.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol
li-ep	Operates as Lawful Intercept endpoint of SMF.	Protocol

Pod Name	Description	Virtual Machine Name
nodemgr	Performs node level interactions, such as N4 link establishment, management (heart-beat), and so on. Also, generates unique identifiers, such as UE IP address, SEID, CHF-ID, Resource URI, and so on.	Service
node-monitor pod	Monitors all the K8 nodes and performs self-reboot on encountering an issue, which in turn triggers an GR to other rack.	NA
oam-pod	Operates as the pod to facilitate Ops Center actions like show commands, configuration commands, monitor protocol monitor subscriber, and so on.	OAM
ops-center-smf-ops-center	Acts as the SMF Ops Center.	OAM
protocol	Operates as encoder and decoder of application protocols (PFCP, GTP, RADIUS, and so on) whose underlying transport protocol is UDP.	Protocol
radius-ep	Operates as RADIUS endpoint of SMF	Protocol
rest-ep	Operates as REST endpoint of SMF for HTTP2 communication.	Protocol
service	Contains main business logic of SMF.	Service
smart-agent-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM
udp-proxy	Operates as proxy for all UDP messages. Owns UDP client and server functionalities.	Protocol
swift-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM
zookeeper	Assists Kafka for topology management.	OAM

For details on UDP proxy, see the UDP Proxy Pod, on page 977 section.

These SMF pods communicate with the Common Execution Environment (CEE) pods. For the complete list of CEE pods, see the *UCC CEE Configuration and Administration Guide*.

Replicas

Each pod runs on a single instance of an application. To provide more resources by running more instances, you can use multiple Pods, one for each instance. This concept in Kubernetes is referred to as replication. Replicated Pods or replicas are usually created and managed as a group by a workload resource and its controller.

With multiple replicas, Kubernetes can distribute the load between them. During node failures, replicas can be used.

Note Replicas are based on the hardware and deployed call model.

UDP Proxy Pod

Feature Description

The SMF has UDP interfaces toward the UPF (N4) and SGW (s5 or s8 for EPS interworking). With the help of the protocol layer pods (smf-protocol and gtp-ep), the messages are encoded and decoded and exchanged on these UDP interfaces.

For achieving the functionalities mentioned on the 3GPP specifications:

- It is mandatory for the protocol layer pods to receive the original source and destination IP address and port number. But the original IP and UDP header is not preserved when the incoming packets arrive at the UDP service in the Kubernetes (K8s) cluster.
- Similarly, for the outgoing messages, the source IP set to the external IP address of the UDP service (published to the peer node) is mandatory. But the source IP is selected as per the egress interface when different instances of protocol layer pods send outgoing messages from different nodes of the K8s cluster.

The protocol layer POD spawns on the node, which has the physical interface configured with the external IP address to achieve the conditions mentioned earlier. However, spawning the protocol layer pods has the following consequences:

- It is not possible to achieve the node level HA (High Availability) because the protocol pods are spawned on the same node of the K8s cluster. Any failure to that node may result in loss of service.
- The protocol pods (smf-protocol, gtp-ep, and radius-ep) must include their own UDP client and server functionalities. In addition, each protocol layer pod may require labeling of the K8s nodes with the affinity rules. This restricts the scaling requirements of the protocol layer pods.

The SMF addresses these issues with the introduction of a new K8s POD called "udp-proxy." The primary objectives of this POD are:

- The “udp-proxy" POD acts as a proxy for all kinds of UDP messages. It also owns the UDP client and server functionalities.
- The protocol pods perform the individual protocol (PFCP, GTP, Radius) encoding and decoding and provide the UDP payload to the "udp-proxy" POD. The "udp-proxy" POD sends the UDP payload out after it receives the payload from the protocol pods.
- The "udp-proxy" POD opens the UDP sockets on a virtual IP (VIP) instead of a physical IP. This ensures that the "udp-proxy" POD does not have any strict affinity to a specific K8s node (VM). Thus, enabling node level HA for the UDP proxy.

Note One instance of the "udp-proxy" POD is spawned by default in all the worker nodes in the K8s cluster.

The UDP proxy for SMF feature has functional relationship with the Virtual IP Address feature.

Architecture

The "udp-proxy" POD is placed in the worker nodes in the K8s cluster.

1. Each of the K8s worker node contains one instance of the "udp-proxy" POD. However, only one of the K8s worker node owns the virtual IP at any time. The worker node that owns the virtual IP remains in the active mode while all the other worker nodes remain in the standby mode.
2. The active "udp-proxy" POD binds to the virtual IP and the designated ports for listening to the UDP messages from the peer nodes (UPF and SGW).
3. The UDP payload received from the peer nodes are forwarded to one instance of the protocol, gtp-ep, or radius-ep pods. The payload is forwarded either on the same node or different node for further processing.
4. The response message from the protocol, gtp-ep, or radius-ep pods is forwarded back to the active instance of the "udp-proxy" POD. The "udp-proxy" POD sends the response message back to the corresponding peer nodes.
5. The SMF-initiated messages are encoded at the protocol, gtp-ep, or radius-ep pods. In addition, the UDP payload is sent to the "udp-proxy" POD. Eventually, the "udp-proxy" POD comprises of the complete IP payload and sends the message to the peer. When the response from the peer is received, the UDP payload is sent back to the same smf-protocol, gtp-ep, or radius-ep POD from which the message originated.

Protocol Pod Selection for Peer-Initiated Messages

When the "udp-proxy" pod receives the peer node (for instance UPF) initiated messages, it is load balanced across the protocol instances to select any instance of the protocol pod. An entry of this instance number is stored along with the source IP and source port number of the peer node. This ensures that the messages form the same source IP and source port are sent to the same instance that was selected earlier.

High Availability for the UDP Proxy

The UDP proxy's HA model is based on the keepalived virtual IP concepts. A VIP is designated to the N4 interface during deployment. Also, a keepalived instance manages the VIP and ensures that the IP address of the VIP is created as the secondary address of an interface in one of the worker nodes of the K8s cluster.

The "udp-proxy" instance on this worker node binds to the VIP and assumes the role of the active "udp-proxy" POD. All "udp-proxy" instances in other worker nodes remain in the standby mode.

Node Monitoring Pod

Node monitor pod runs on all Kubernetes nodes, such as master and worker nodes to periodically check the operating state of other nodes. The nodes might become unreachable due to network issue or hardware transient issue.

Depending on the operating state of nodes, the node monitor pod switches to different modes. SMF uses **nodemonitor** CLI command in Global Configuration mode to switch between the modes.

The following configuration section provides more information on the command and modes.

Configure Node Monitoring Pod

The node monitoring pod switches to different modes to resolve the hardware transient issues.

To switch between the modes, use the following sample configuration:

```
config
   nodemonitor mode { 0 | 1 | 2 | 3 interval wait_time }
   end
```

NOTES:

- **nodemonitor mode { 0 | 1 | 2 | 3 interval** *wait_time* **}**
  - **mode 0**—Disables the node monitoring functionality.
  - **mode 1**—Enables the node monitoring and performs self-reboot only after reaching a hardcoded value of 2 seconds when two or more nodes are not reachable. This is the default setting.
  - **mode 2**—Enables the node monitoring and performs self-reboot when two or more nodes are not reachable but not all the nodes.
  - **mode 3 interval** *wait_time*—Specify the time interval in seconds, after which the node monitoring pod is rebooted when two or more nodes are not reachable.

    wait_time must be an integer in the range of 5–300.

Configuration Example

The following is an example of node monitoring pod configuration.

```
config
   nodemonitor mode 3 interval 15
   end
```

As per this example, the node monitoring pod waits for 15 seconds and then performs self-reboot when two or nodes are not reachable.

Configuration Verification

To verify the configuration, use the **show running-config nodemonitor** command.

The output of this show command displays the configuration related to mode of the node monitoring pod.

```
smf# show running-config nodemonitor
nodemonitor mode 3 interval 15
```

Services

The SMF configuration consists of several microservices that run on a set of discrete pods. Microservices are deployed during the SMF deployment. SMF uses these services to enable communication between the pods. When interacting with another pod, the service identifies the pod's IP address to initiate the transaction and acts as an endpoint for the pod.

The following table describes the SMF services and the pod on which they run.

Table 353: SMF Services and Pods

Service Name	Pod Name	Description
base-entitlement-smf	base-entitlement-smf	Supports Smart Licensing feature.
datastore-ep-session	cdl-ep-session	Responsible for the CDL session.
datastore-notification-ep	smf-rest-ep	Responsible for sending the notifications fro CDL to the *smf-service* through *smf-rest-ep*.
datastore-tls-ep-session	cdl-ep-session	Responsible for the secure CDL connection.

Service Name	Pod Name	Description
diameter-ep-gx-client	diameter-ep-gx-client	Responsible for sending gRPC messages to Diameter endpoint for Credit Control messages, which are converted to Diameter CCR message by Diameter endpoint and sent to the Gx server.
diameter-ep-gy-client	diameter-ep-gy-client	Responsible for sending gRPC messages to Diameter endpoint for Credit Control Messages, which are converted to Diameter CCR message by Diameter endpoint and sent to the Gy server.
documentation	documentation	Responsible for the SMF documents.
edr-monitor	edr-monitor	Responsible for maintaning EDR files in persiste volume
etcd	etcd-smf-etcd-cluster-0, etcd-smf-etcd-cluster-1, etcd-smf-etcd-cluster-2	Responsible for pod discovery within the namespace.
etcd-smf-etcd-cluster-0	etcd-smf-etcd-cluster-0	Responsible for synchronization of data among t *etcd* cluster.
etcd-smf-etcd-cluster-1	etcd-smf-etcd-cluster-1	Responsible for synchronization of data among t *etcd* cluster.
etcd-smf-etcd-cluster-2	etcd-smf-etcd-cluster-2	Responsible for synchronization of data among t *etcd* cluster.
grafana-dashboard-app-infra	grafana-dashboard-app-infra	Responsible for the default dashboard of app-inf metrics in Grafana.
grafana-dashboard-cdl	grafana-dashboard-cdl	Responsible for the default dashboard of CDL metrics in Grafana.
grafana-dashboard-smf	grafana-dashboard-smf	Responsible for the default dashboard of SMF-service metrics in Grafana.
gtpc-ep	gtpc-ep	Responsible for inter-pod communication with GTP-C pod.
helm-api-smf-ops-center	api-smf-ops-center	Manages the Ops Center API.
kafka	kafka	Processes the Kafka messages.
li-ep	li-ep	Responsible for lawful-intercept interactions.
local-ldap-proxy-smf-ops-center	ops-center-smf-ops-center	Responsible for leveraging Ops Center credentia by other applications like Grafana.
oam-pod	oam-pod	Responsible to facilitate Exec commands on the Ops Center.
ops-center-smf-ops-center	ops-center-smf-ops-center	Manages the SMF Ops Center.
ops-center-smf-ops-center-expose-cli	ops-center-smf-ops-center	To access SMF Ops Center with external IP address.
smart-agent-smf-ops-center	smart-agent-smf-ops-center	Responsible for the SMF Ops Center API.

Service Name	Pod Name	Description
smf-sbi-service	smf-rest-ep	Responsible for routing incoming HTTP2 mes to REST-EP pods.
smf-n10-service	smf-rest-ep	Responsible for routing incoming N10 mess to REST-EP pods.
smf-n11-service	smf-rest-ep	Responsible for routing incoming N11 mess to REST-EP pods.
smf-n40-service	smf-rest-ep	Responsible for routing incoming N40 mess to REST-EP pods.
smf-n7-service	smf-rest-ep	Responsible for routing incoming N7 messa REST-EP pods.
smf-nrf-service	smf-rest-ep	Responsible for routing incoming NRF mes to REST-EP pod.
smf-nodemgr	smf-nodemgr	Responsible for inter-pod communication w *smf-nodemgr* pod.
smf-protocol	smf-protocol	Responsible for inter-pod communication w smf-protocol pod
smf-radius-dns	smf-radius-dns	Responsible for inter-pod communication w smf-radius-dns pod
smf-rest-ep	smf-rest-ep	Responsible for inter-pod communication w smf-rest-ep pod
smf-service	smf-service	Responsible for inter-pod communication w smf-service pod
swift-smf-ops-center	swift	Operates as the utility pod for the SMF Ops C
zookeeper	zookeeper	Assists Kafka for topology management
zookeeper-service	zookeeper	Assists Kafka for topology management

Open Ports and Services

The SMF uses different ports for communication purposes. The following table describes the default open ports and the associated services.

Table 354: Open Ports and Services

Port	Service	Usage
9003	gRPC	This is the default gRPC port for all the application pods that aren't using the host network.
8080	TCP/HTTP	This is the default prometheus server port for all the application pods that aren't using the host network.
8090	TCP/HTTP	SMF uses the HTTP2 REST endpoint for the SBI interface endpoint.
2024	SSH	SMF Ops Center uses this port to provide the ConfD CLI access.

Port	Service	Usage
2379-2380	TCP	SMF uses the etcd server client endpoint to store and retrieve system data.
8882	gRPC	This is the CDL session DB endpoint used by all other application pods.
8890	gRPC	Application REST endpoint uses this port to receive the call-back timer or notification from the CDL.
8883	gRPC	This is the TLS - CDL session DB endpoint used by all other application pods.
2123	UDP	SMF uses the 3GPP standard GTP-C port for the signaling of GTP-C protocol messages (control path).
2152	UDP	SMF uses the 3GPP standard GTP-U port for the signaling of GTP-U protocol messages (data path).
8805	UDP	SMF uses the 3GPP standard PFCP port for the signaling of PFCP protocol messages.
8765	TCP6	SMF uses this port as the readiness probe port for the UDP proxy pod.
7179, 7189	TCP/HTTP	Pprof Server endpoint serves runtime profiling data from GTP-C endpoint interface-specific pods, such as S11 and S5.
23300, 23310	TCP/gRPC	SMF uses the TLS GRPC IPC server endpoint for the GTP-C endpoint interface-specific pods.
9005, 9015	TCP/gRPC	Non-TLS GRPC IPC server port for the GTP-C endpoint interface-specific pods.
27000, 27010	TCP	SMF uses the KeepAliveD endpoint for GTP-C endpoint interface-specific pods.
7279, 7289	TCP	This port is the admin endpoint internal port that is used in the GTP-C endpoint interface-specific pods. This port is used for liveness and readiness probe.
7079, 7089	TCP/HTTP	SMF uses the prometheus server port for the GTP-C endpoint interface-specific pods.
8083	TCP/HTTP	SMF uses the prometheus server port for the protocol pod.
9006	TCP/gRPC	SMF uses the non-TLS GRPC IPC Server endpoint for the protocol pod.
8003	TCP/HTTP	SMF uses the prometheus server port for the protocol pod.
23100	TCP/gRPC	SMF uses the TLS GRPC IPC server endpoint for the protocol pod.
7679	TCP/HTTP	The Pprof server endpoint serves runtime profiling data from the protocol pod.
7879	TCP	This port is the admin endpoint internal port that is used in the protocol pod. This port is used for the liveness and readiness probe.
27500	TCP	SMF uses this KeepAliveD endpoint for the protocol pod.
28000	TCP	SMF uses this KeepAliveD endpoint for the UDP proxy pod.
23200	TCP/gRPC	SMF uses the TLS GRPC IPC server endpoint for the UDP proxy pod.
9004	TCP/gRPC	Non-TLS GRPC IPC server endpoint for the UDP proxy pod.

Port	Service	Usage
7879	TCP	This port is the admin endpoint internal port that is used in the UDP proxy pod. This port is used for the liveness and readiness probe.
8850	TCP/HTTP	The Pprof server endpoint serves runtime profiling data from the UDP proxy pod.

In addition to the preceding ports, SMF uses the ports that are destined for SMI for routing information between hosts. For information on SMI ports, see the *Ultra Cloud Core Subscriber Microservices Infrastructure Operations Guide*.

Associating Pods to the Nodes

This section describes how to associate a pod to the node based on their labels.

After you have configured a cluster, you can associate pods to the nodes through labels. This association enables the pods to get deployed on the appropriate node based on the key-value pair.

Labels are required for the pods to identify the nodes where they must get deployed and to run the services. For example, when you configure the protocol-layer label with the required key-value pair, the pods are deployed on the nodes that match the key-value pair.

To associate pods to the nodes through the labels, use the following sample configuration:

```
config
  k8 label vm_group key label_key value label_value
  end
```

NOTES:

- **k8 label** *vm_group* **key** *label_key* **value** *label_value*: Configures the K8 node affinity label parameters.
  - *vm_group*: Specify the VM group. It must be one of the following:
    - cdl-layer
    - oam-layer
    - protocol-layer
    - service-layer
  - **key** *label_key*: Specify the label key. *label_key* must be a string.
  - **value** *label_value*: Specify the label value. *label_value* must be a string.
- If you choose not to configure the labels, then SMF assumes the labels with the default key-value pair.

Viewing the Pod Details and Status

If the service requires additional pods, SMF creates and deploys the pods. You can view the list of pods in your deployment through the SMF Ops Center.

You can run the **kubectl** command from the master node to manage the Kubernetes resources.

The pod details are available in YAML format.

Use the following sample configuration to view the comprehensive pod details:

kubectl get pods -n smf *pod_name* **-o yaml**

The output of this command displays the following information:

- The IP address of the host where the pod is deployed.
- The service and application that is running on the pod.
- The ID and name of the container within the pod.
- The IP address of the pod.
- The current state and phase in which the pod is.
- The start time from when the pod is in the current state.

To view all the pods in the SMF namespace, use the following sample configuration:

kp get pods -n *smf_namespace* **-o wide**

States

Understanding the pod's state lets you determine the current health and prevent the potential risks. The following table describes the pod's states.

Table 355: Pod States

State	Description
Running	The pod is healthy and deployed on a node. It contains one or more containers.
Pending	The application is in the process of creating the container images for the pod.
Succeeded	Indicates that all the containers in the pod are successfully terminated. These pods cannot be restarted.
Failed	One ore more containers in the pod have failed the termination process. The failure occurred as the container either exited with non zero status or the system terminated the container.
Unknown	The state of the pod could not be determined. Typically, this could be observed because the node where the pod resides was not reachable.

GTPC Protocol Endpoint Merge with UDP Proxy Bypass

Feature Description

Bypass proxy is introduced to enable this GTP packets directly land on gtpc-ep pod. This will avoid the processing at udp-proxy and one hop will be reduced in packet forwarding.

All the features supported by existing gtpc-ep and udp-proxy are integrated in new merged path

following features are integrated from udp-proxy:

- Transaction SLA
- DSCP marking for GTP packets
- Adding BGP routes for roamer subscriber on the fly
- Supporting Dispatcher feature and incoming retransmission
- SGW Cache integration for DDN
- MBR cache integration

Following features are integrated from gtpc-ep:

- Retransmissions based on n3t3 config for outbound requests
- Monitor protocol and Monitor Subscriber
- Echo message handling

GTPC Endpoint with GR-Split

For handling scaled GTP traffic and for the optimal use of CPU, multiple active instances of GTPC-EP are started, and traffic split is done based on GR Instances.

UDP Proxy Functionality Merge into Protocol Micro-services

Feature Description

The UDP Proxy micro-services provide UDP transport termination for protocols (PFCP, GTPC, and RADIUS) that require UDP. The UDP proxy provides user space packet forwarding and IPC communication towards protocol micro-services. It uses host networking for source IP address observability and operates in Active/Standby mode.

Multiple protocol micro-services depend on UDP proxy for UDP transport, therefore UDP proxy is a scale bottleneck and single point of failure. Merging UDP Proxy functionality into respective protocol micro-services will help mitigate the scale bottleneck and improve CPU usage by virtue of reducing one hop across micro-services in the signaling path.

How it Works

PFCP Protocol Endpoint with UDP Proxy Bypass

Protocol endpoint bypasses UDP proxy and sends N4/Sxa messages towards UPF directly. Incoming N4/Sxa messages from UPF also bypass UDP poxy and land on Protocol pod. (Subject to UPF support for Source IP Address IE in heartbeat request message). Protocol pod continues to use non-host networking mode of operation.

Kubernetes service starts to listen on the configured VIP IP address and standard port, ensuring incoming N4/Sxa UDP packets are sent to Protocol pods. A separate Kubernetes service created for N4 & Sx with separate target ports to identify the interface associated with the incoming message/packet. Kubernetes client IP address affinity is availed to ensure retransmitted packets from UPF are sent to the same Protocol pod instance to hit the retransmission cache successfully.

Current Mode (No Bypass)

In this mode of operation the message exchange for N4, Sxa, GTP-U happen through the UDP proxy. The UDP proxy is responsible for connecting to or receiving connections from UPF.

All the node related messages, or session that is related on PFCP are initiated either by the service or from the UPF and their responses pass through the UDP proxy.

Outbound Bypass Proxy Mode

This mode of operation is enabled by default for all messages that are initiated by S-GW or SMF service and sent by the system toward UPF using PFCP through Kubernetes Pod environment variable “OUTBOUND_PROXY_BYPASS”. The messages that are sent by SMF (Protocol pod) directly to UPF are session that is related and as follows:

1. PFCP Session Establishment Request
2. PFCP Session Modification Request
3. PFCP Session Deletion Request

In this mode, the GTP-U messages from UPF or initiated by Service toward UPF continue to be exchanged through the UDP proxy. In this mode, only the session related messages (that is, the ones initiated by SMF Service) flow directly from Protocol towards the UPF.

Protocol pod receives the UPF IP address from the service, which is used to set up connection with UPF and subsequently use the same for session related message exchange. The node related messages continue to take the UDP proxy to protocol or Node Manager path.

Complete Bypass Mode (Inbound and Outbound)

In this mode, both inbound and outbound messages are sent and received by Protocol pod bypassing UDP Proxy. The protocol pod will listen on N4 and GTPu or Sxa ports based on the configured VIPs. Protocol pod ceases to be on a Kubernetes service network and remains in Host based networking mode. Protocol pods gets the IP of the node or VM that it is on, this condition is triggered based on an environment variable present or available for both Protocol and UDP proxy pods (UDP_PROXY_BYPASS). By default, this variable is false and UDP proxy and Protocol continue as they do today with UDP-Proxy exchanging messages with UPF.

UDP_PROXY_BYPASS is set to true only if both the following conditions are met:

1. VIP is configured under endpoint PFCP interface N4 or interface Sxa.
2. There is no VIP configured under endpoint protocol interface N4 or interface Sxa.

With change in value of UDP_PROXY_BYPASS variable, both UDP proxy and Protocol pods are restarted to enable this new mode of working or to fallback to earlier mode of message exchange trhough UDP proxy.

Triggering Bypass Mode using CLI

To trigger the bypass mode or protocol-proxy merged working, the VIP-IPs must be configured under endpoint PFCP as shown here:

```
no instance instance-id 1 endpoint protocol interface n4
no instance instance-id 1 endpoint protocol interface gtpu
instance instance-id 1 endpoint pfcp interface n4 vip-ip X.X.X.X
instance instance-id 1 endpoint pfcp interface gtpu vip-ip X.X.X.X
```

Important With the preceding configuration the value of environment variable UDP_PROXY_BYPASS will change. This triggers a restart of both pods UDP proxy and Protocol.

Every feature that is present under endpoint→ protocol must be correspondingly configured under endpoint → PFCP and which include features like DSCP, SLA, and Dispatcher related configurations. The configurations for all features take effect only if internal VIP-IP is configured under endpoint → PFCP and interface N4 or interface Sxa. There should be interface N4 and VIP-IP or interface Sxa and VIP-IP present under endpoint → protocol.

Rendering CLI Values

Based on N4 and Sxa VIP configuration, the rendering logic calculates which values to publish under endpoint protocol. The configuration is rendered in pods having the key as “endpointIp”. The configuration path in each individual pod is located at /config/AppName/vip-ip/endpointIp.yaml. The affected pods are:

1. Protocol
2. Node Mgr
3. SMF-Service
4. SGW Service.

Having endpoint → pfcp configurations render under endpoint → protocol helps in avoiding changes to background configuration read logic.

Node Management

In this case Protocol starts a PFCP endpoint for peers to connect with it. At the same time, it will also establish connection with UPF as and when the app service initiates a PFCP message towards the UPF. Following messages are included:

1. PFCP Association Setup Request/Response
2. PFCP Association Update Request/Response
3. PFCP Session Report Request/Response

4. PFCP Node Report Request/Response
5. Heartbeat Request/Response
6. PFCP PFD Management Request/Response

Session Management

Session Management messages initiated by the service and sent directly to UPF through the Protocol pod. The protocol pod initiates connection with UPF to send these messages, this is the reason protocol pod must be in “Host networking” to take the IP address of the node on which it is on.

Standardized Port Numbers

While triggering the “Merged” mode, the protocol pod transitions into Host based networking. Protocol pod takes the IP address of the Host or the Node much like the existing UDP proxy pod. It is essential that UDP proxy, GTPC-EP, and Protocol do not share the same ports. The thumb rule for port calculation is:

```
Port_Value = Base_Port _Value + (Gr_Instance_Id_index *50) + (Logical_Instance_id mod 50)
```

Gr_Instance_id: The GR Instance ID supplied in the configurations using CLI.

Logical_Instance_id: Identifier for the logical SMF instance.

Prometheus Port:

With complete UDP proxy bypass the Prometheus port of 8080 is not used, instead the start port for Prometheus 8004 for instance 1. The "instance-Id” added with 8003 must be the port number.

Proxy Keep-Alive Port:

The proxy keepalive port starts from 27500+ “Instance-Id”.

1. GR Instance 1 & Logical Instance Id 0 :- 27500 + (0 * 50) + (0 % 50) = 27500
2. GR Instance 2 & Logical Instance Id 0 :- 27500 + (1 * 50) + (0 % 50) = 27550

Admin Port for Keepaive and Liveness Probe:

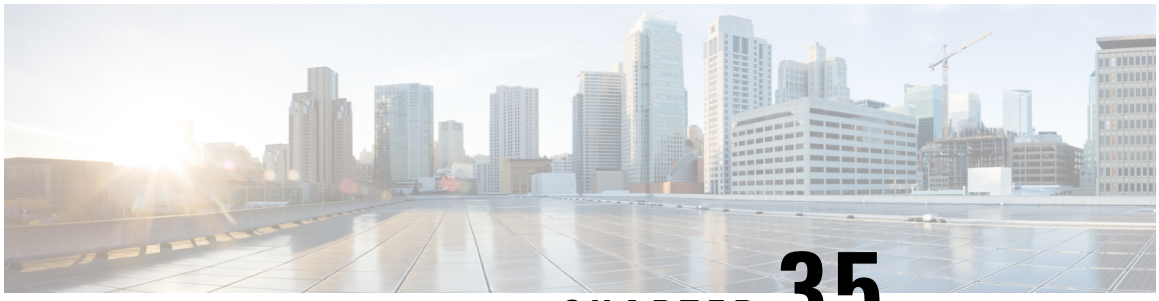
Admin Port will be 7879 + (Gr_Instance_Id_index *50) + (Logical_Instance_id mod 50)

Infra Diagnostics Port:

Infra Diag Port will be 7779 + (Gr_Instance_Id_index *50) + (Logical_Instance_id mod 50)

PProf port:

PProf Profiling port will be 7679 + (Gr_Instance_Id_index *50) + (Logical_Instance_id mod 50)



CHAPTER 35

Policy and User Plane Management

- Feature Summary and Revision History, on page 989
- Feature Description, on page 991
- QoS Management on SMF, on page 992
- Bit Rate Mapping Support, on page 1000
- Handling of Authorized QoS for Default Bearer, on page 1003
- GBR Bearer Creation Based on Local Policy, on page 1006
- SMF-triggered Metadata for EDR Generation on UPF, on page 1015
- Dynamic Configuration Update, on page 1015
- Dynamic PCC Rules Enforcement, on page 1018
- Dynamic QoS Flow-based Application Detection and Control, on page 1039
- Static PCC Rules Support, on page 1041
- Predefined PCC Rules, on page 1056
- Bearer QCI Support, on page 1057
- Non-standard QCI Support for Dynamic PCC and Session Rules, on page 1059
- Support for Configuring the Bandwidth ID, on page 1061
- Generating UE Camping Report for PCF, on page 1063
- UPF Node Selection, on page 1063
- Support for UPF Node Reports and Proprietary Session Reports, on page 1084
- Outer Header Format, on page 1090
- Usage Monitoring over PCF, on page 1092
- QoS Group of Ruledefs Support over N7, on page 1098

Feature Summary and Revision History

Summary Data

Table 356: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required

Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 357: Revision History

Revision Details	Release
Added support for prioritization of packets to support dedicated UE services such as PTT service.	2024.01.1
• Added support for GBR bearer creation without PCF interaction for 4G and 5G. • Added the N7 optimization support. • Added support for optional PCF or PCRF configuration for local policy configuration.	2023.04.0
Added support for the following features: • QoS group of ruledefs over N7 • IPv6 support for N3 interface on UPF	2023.01.0
Added support for SMF— • to allocate UPFs with unique IP pools • to select the UPF based on PDN type	2022.04.0
Introduced support for Diff-Serv-Code-Point (DSCP) or Type of Service (ToS) QoS functions during interaction with PCF.	2021.02.3.t3
Introduced support for the following features: • Usage Monitoring over PCF • N4 QoS Mismatch Correction • Dynamic QoS Flow-based Application Detection and Control • IP Threshold-based UPF Selection	2021.02.3
Introduced support for non-standard QCI for dynamic PCC and session rules	2021.02.2

Revision Details	Release
Introduced support for the following features: • Bit rate mapping • UPF Selection based on Slice and Location • UP Optimization	2021.02.0
Introduced support for the following: • Co-located UPF Selection • Enhanced Limits for Maximum Groups in Bandwidth Policy Configuration • Handling Session Report Rejection Procedure • New Format of Outer Header information element (IE)	2021.01.0
Introduced support for the following: • UPF node selection based on DNN and PDU Session type • Modification of authorized default QoS • Additional session report and UPF node report request	2020.03.0
First introduced.	Pre-2020.02.0

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The SMF is one of the control plane NFs that provide the Session Management service in the 5G core network. The SMF manages the PDU session lifecycle through the following session management procedures:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

This chapter describes the policy and user plane management features.

- Policy Management—Policy Control Function (PCF) or the local configuration controls the policies managed on SMF. The PCF sends Policy and Charging Control (PCC) rules along with the applicable

QoS and charging information to the SMF. The SMF uses this information to define QoS flows and apply QoS enforcement (via User Plane Function (UPF) and charging towards Charging Function (CHF). The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

- User Plane Management—The user plane management on SMF includes selection of UPF and maintaining per session and node level user plane data. The SMF performs Path management of the UPF nodes. At a per session level, SMF publishes the Packet Detection Rules (PDRs), QoS Enforcement Rules (QERs), Forwarding Action Rules (FARs), and Usage Reporting Rules (URRs) to the UPF. Then, the SMF enforces the policy rules received from PCF or configured locally.

QoS Management on SMF

Feature Description

The primary functionality of the SMF is to manage the flow-based QoS model. SMF interacts with the Unified Data Management (UDM) and Policy Control Function (PCF) to get the subscribed and authorized QoS parameters for GBR and non-GBR flows and passes on the relevant information to UE (NAS), gNB (NGAP), and UPF (PFCP) so that all nodes on the network provide the desired QoS to the PDU session.

Use Cases

This section describes the various use case scenarios that can lead to creation, modification, and deletion of QoS-Profile and the corresponding actions taken.

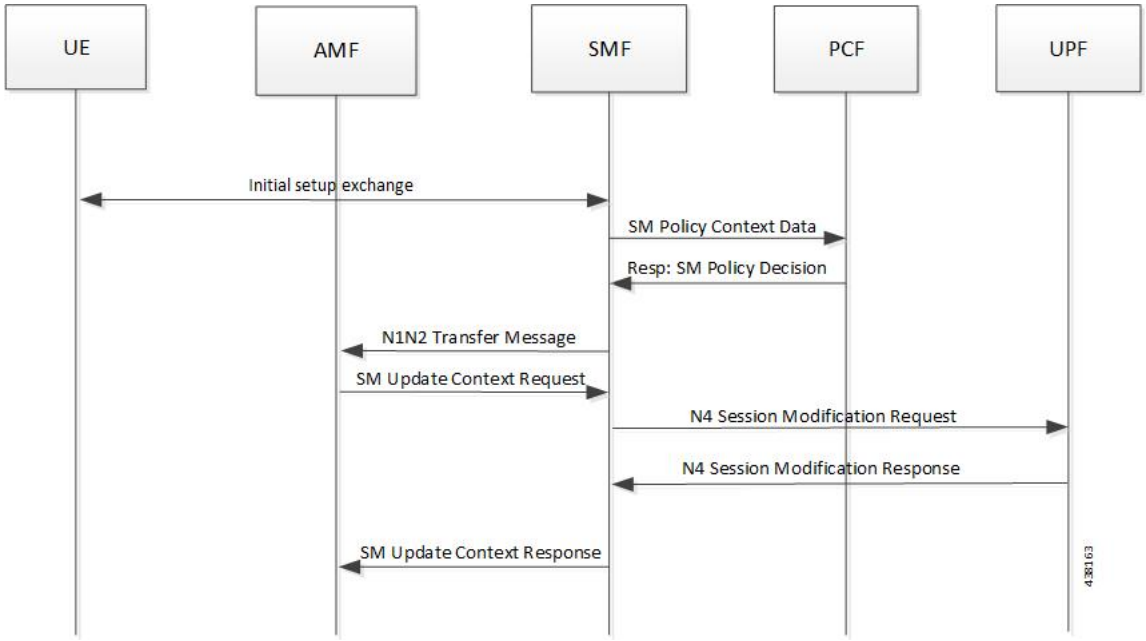
QoS-Profile associated to the PDU Context will be modified in the following scenarios:

- Response from PCF for SMPolicyContextData
- Update Notify from PCF
- Update response from PCF on behalf of Update request sent initially from SMF
- Update request from SMF will be triggered in the following cases:
  - UE triggered modify request
  - AN triggered modify request
  - UDM triggered modify request

Setup Creation

The following figure illustrates the setup creation call flow.

Figure 201: Setup Creation Call Flow



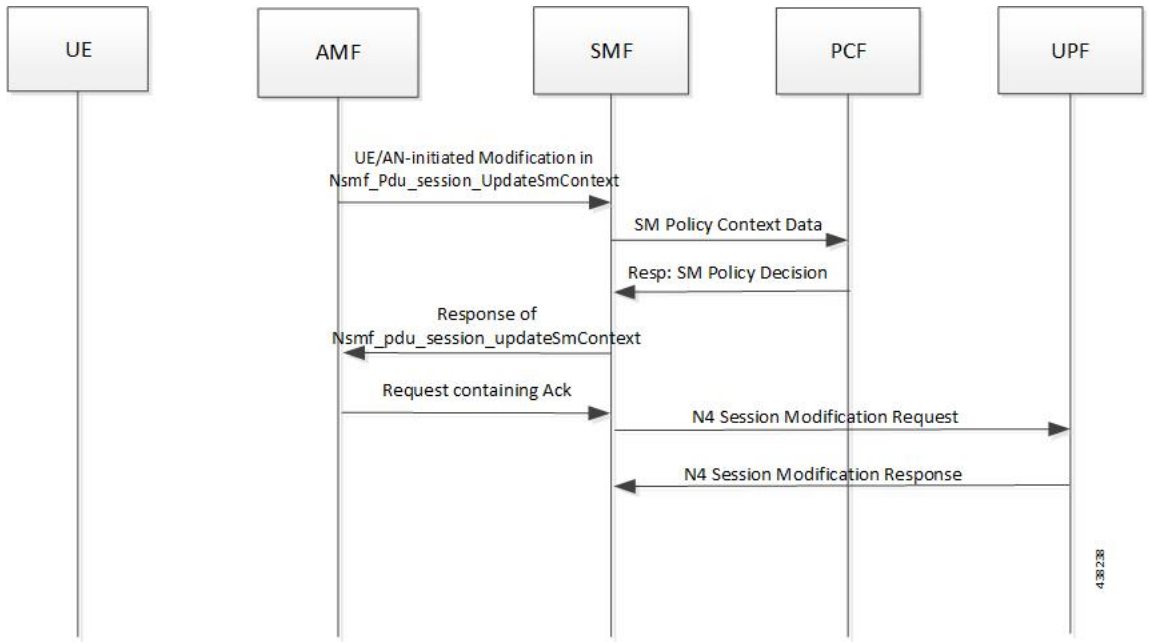
Based on the content received in SM Policy Decision, SMF pushes the following towards various interfaces.

- UPF:
  - Set of PDR derived from PCC rules
  - Set of QER derived from QoS flows which in turn are derived from QosDescription/QosCharacteristics from PCF
  - One extra QER derived from SessRules
- N1:
  - Set of QoS rules derived from QosFlows
  - Each QosRule has its associated packet filter
- N2:
  - Set of QoS Flow information

UE/AN-initiated Modification

The following figure illustrates the UE/AN-initiated modification call flow.

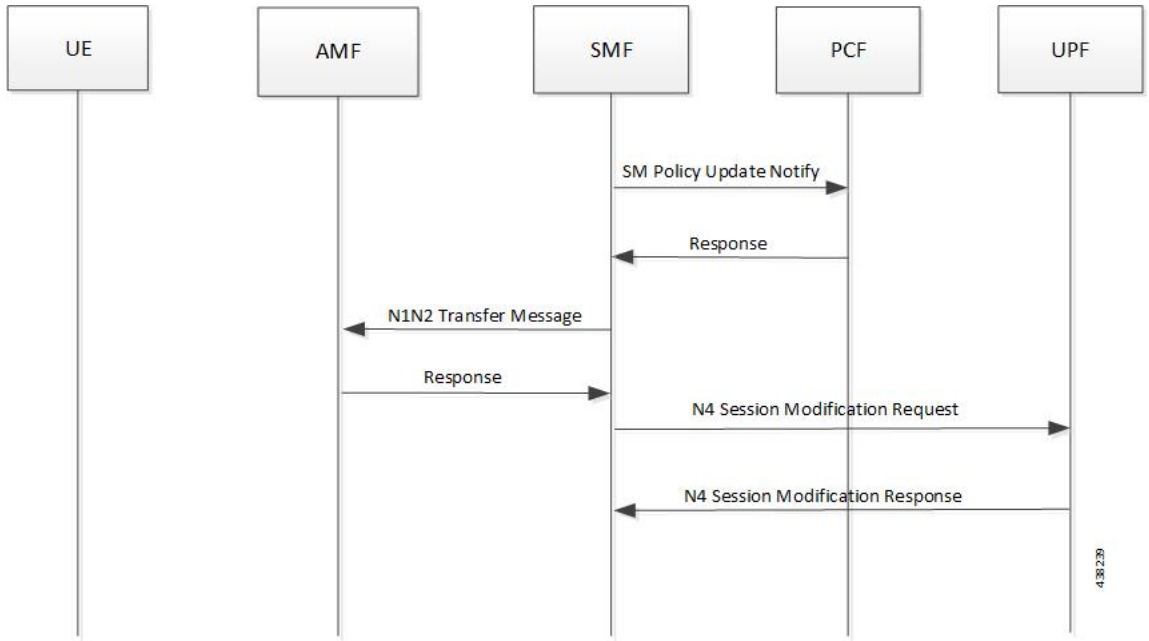
Figure 202: UE/AN-initiated Modification Call Flow



UDM/PCF-initiated Modify

The following figure illustrates the UDM/PCF-initiated Modify call flow.

Figure 203: UDM/PCF-initiated Modify



- N1:
  - PDU Session Modification command will be triggered from SMF. It can change Session-AMBR and QoS rules.

- PDU Session Modification Request will be triggered from UE. It can change the QoS rules and maximum number of support-ed packet filters.

  In either case, the QoS rule change can happen from the following:

  - Packet filter add/delete/replace
  - Rule Precedence of QoS Rule
  - QoS Parameter – 5QI/MBR/GBR

- N2:
  - PDU Session Resource Modify Request will be triggered from SMF. It can change the existing QoS flow that is installed or delete the QoS flow already installed. If the Modify request is received, the parameters - ARP, GBR/MBR, Priority level, and so on, can change.
  - PDU Session Resource Notify will be triggered from AN. This happens when certain flow is to be released, not fulfilled any-more and fulfilled again.

Subscribed QoS

The UDM NF maintains the subscribed QoS for the UE in the Session Management Subscription Data. During the PDU setup procedure, the SMF posts an HTTP2 GET request (see *3GPP TS 29.503*) for a resource URI "/{supi}/sm-data" to fetch the Session Management Subscription Data. The subscription data has a set of DNN configurations, one for each DNN which the subscriber is allowed to access. Each DNN configuration consists of the following parameters:

- sessionAMBR: The maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session.
- 5gQosProfile: The default 5G QoS Indicator (5QI) and default ARP values are provided to the SMF in the Session Management Subscription Data in this attribute of the DNN configuration.

The SMF saves the subscribed QoS parameters and sends this across to the PCF during the SM Policy Association Establishment procedure.

QoS Negotiation

The SMF negotiates the QoS with the PCF by initiating a Policy Association Establishment procedure as defined in *3GPP TS 23.502, section 4.16.4*. The sessionAMBR and 5gQosProfile parameters that are received from subscription are included in the Npcf_SMPolicyControl_Create request to PCF. The response from PCF may contain the following:

- Session Rules—A session rule consists of policy information elements that are associated with the PDU session. The QoS related information is Authorized session AMBR and Authorized default QoS.
  - Policy Charging and Control (PCC) Rules—The PCC rule includes the FlowDescription, FlowDirection, and RefQosData parameters among other information. There could be one or more PCC rules in the response from PCF.
    - FlowDescription—This parameter contains packet filters for IP flows. For IP PDU Session Type, the Packet Filter Set supports packet filtering based on at least any combination of:

      - Source / Destination IP address or IPv6 prefix

- Source / Destination port number
- Protocol ID of the protocol above IP/Next header type
- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and mask
- Flow Label (IPv6)
- Security parameter index

- FlowDirection—This parameter indicates the direction of data traffic on which the rule has to be applied. This could be UPLINK, DOWNLINK, or BIDIRECTIONAL.
- RefQosData—This parameter refers to the QoS description to be applied to this PCC Rule. This matches the QosId of at least one of the QoS Description entries in the response from PCF.

- QoS Characteristics—The QoS characteristics include the following parameters:
  - Resource Type (GBR, Delay critical GBR, or non-GBR)
  - Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Averaging Window
  - Maximum Data Burst Volume (for the Delay-critical GBR resource type only)

    This attribute in the response from PCF is meant to be used only for non-standard 5QI values. For standard 5QI values, the characteristics are already defined in *3GPP TS 23.501, section 5.7.4*.

- QoS Description—The QoS Description parameter consists of the following:
  - 5QI – Standard or non-standard from the QoS Characteristics attribute
  - Uplink and Downlink GBR
  - Uplink and Downlink MBR
  - Maximum Packet Loss Rate
  - QosId – Referenced in PCC rules
  - Default QoS Indication

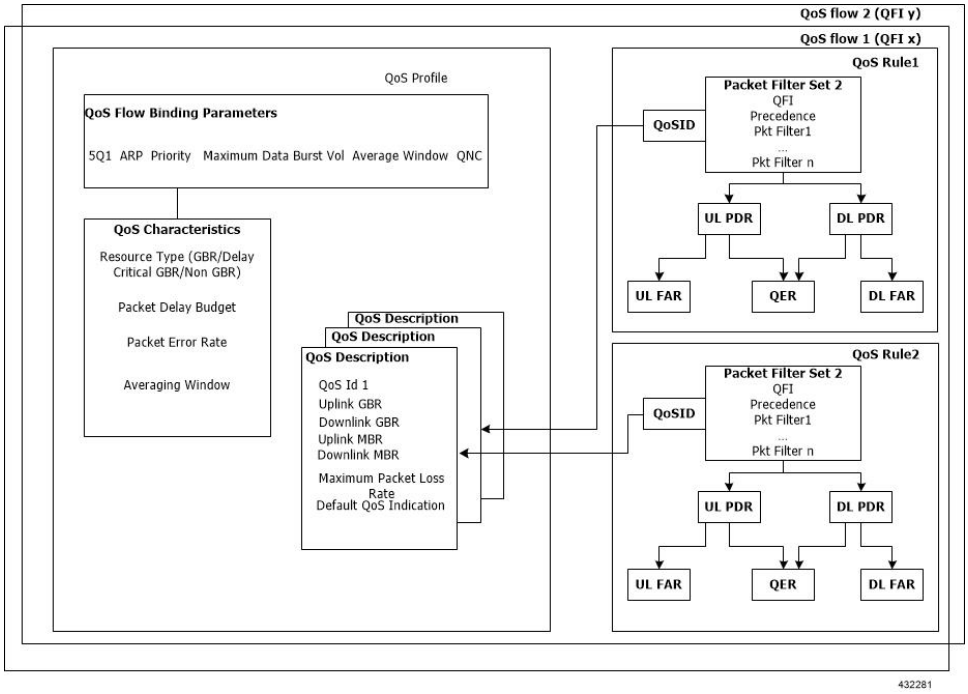
    There could be more than one QoS Description attribute in the response from PCF.

QoS Flow Management

The information, that is received from PCF in the Npcf_SMPolicyControl_Create response, is used to create and update QoS Flows in the SMF. Each QoS flow has a unique QoS Flow ID (QFI) and one or more PCC rules map to a single QoS flow.

The following figure illustrates how to manage the QoS information at the SMF.

Figure 204: QoS Information Management at SMF



Each QoS Flow in SMF is a combination of three sets of information:

- QoS profile: A QoS profile stores all QoS attributes for a particular QoS Flow.
  - Some QoS parameters known as the QoS flow binding parameters make a unique combination for one QoS Flow of one PDU Session. This means that, for a PDU session, each unique combination of these parameters represents a separate QoS Flow. These parameters are – 5QI, ARP, Priority, Maximum Data Burst Volume, Average Window and QNC.
  - If the 5QI for the QoS profile of a QoS Flow is non-standard, some additional QoS characteristics, such as Resource Type, Packet Delay Budget, Packet Error rate, and Averaging Window are also saved in the QoS profile.
  - The QoS profile also maintains multiple QoS Descriptions, each with a unique QoSId for a specific PDU session. Each QoS Description contains the uplink and downlink GBR, uplink and downlink MBR, maximum packet loss rate and default QoS indication.
- QoS Rules: A QoS rule is a collection of packet filters that associates with a particular QoS Description in the QoS profile of the QoS flow. The packet filters directly map to the flow descriptions received in the PCC rules in the Npcf_SMPolicyControl_Create response from PCF. The QoS rules have a reference to the QoSId of the QoS Descriptions that the rules associate with.
- PDRs: Each QoS rule maps to two Packet Detection Rules (PDR) to be sent to the UPF. One PDR is for uplink direction and the other PDR is for downlink direction. The Service Data Flow (SDF) filters in the Packet Detection Information (PDI) attribute within the PDRs map the packet filters of the QoS rule. Each PDR then maps to a Forwarding Action Rule (FAR), which determines the forwarding action for the packets matching the SDF filters. Each PDR is also associated to a QoS Enforcement Rule (QER) which carries the QoS information and it maps to the QoS description associated with the QoS rule.

QoS Communication on 3GPP Interfaces

The negotiated QoS mainly needs to be communicated to the UE (N1 interface using NAS protocol), gNB (N2 interface using NGAP protocol), and UPF (N4 interface using PFCP protocol).

- N1 Interface: On the N1 interface, the session management messages are exchanged between UE and SMF through AMF. The NAS messages are encoded into an N1 container and sent to SMF or received from SMF.
  - All the negotiated/authorized QoS related information that needs to be sent out to the UE are found in the Authorized QoS rules and Session-AMBR attributes of the PDU SESSION ESTABLISHMENT ACCEPT message in an N1 container, during the PDU session establishment (see *3GPP TS 24.501, section 8.3.2*).
  - The PDU SESSION MODIFICATION REQUEST message from UE contains the Requested QoS Rules during the UE initiated QoS modification.
  - The Authorized QoS rules and Session-AMBR attributes are also present in the PDU SESSION MODIFICATION COMMAND message sent from SMF to UE during the PCF/SMF initiated QoS modification.
  - The format of the QoS Rule NAS attribute is defined in *3GPP TS 24.501, section 9.10.4.9*. This attribute mainly consists of the packet filter list, QFI, and QoS parameters on a per QoS rule basis. This information is available in the QoS rule within the QoS flow.
- N2 Interface: On the N2 interface, SMF sends an N2 container to the gNB through AMF. The N2 container is ASN.1 encoded data and consists of specific information elements of NGAP messages. All the QoS related information to gNB is encoded and sent/received in N2 containers to/from SMF. The NGAP IEs and the corresponding NGAP messages that will finally carry the IE from AMF to gNB are listed in *3GPP TS 29.502, section 6.1.6.4.3*.
  - During the PDU session setup, the SMF sends N1N2MessageTransfer to AMF with the N2 container in the PDU Session Re-source Setup Request Transfer IE. This IE contains PDU Session Aggregate Maximum Bit Rate and QoS Flow Setup Request List. The QoS Flow Setup Request List contains QoS Flow Level QoS Parameters (GBR flow information, 5QI, and so on). These are defined in *3GPP TS 38.413, section 9.3.1*.
  - Similar information (QoS Flow Level QoS Parameters) is also sent by SMF in the PDU Session Resource Modify Request Transfer IE in an N2 container during the PCF/SMF initiated QoS Modification procedure.

    The information required to create the N2 container in SMF is present in the QoS profile of a QoS flow as described in the previous section.
- N4 Interface: On the N4 interface, the SMF sends the QoS information in the form of Packet Detection Rule (PDR), Forwarding Action Rule (FAR), and QoS Enforcement Rule (QER).
  - The PDR contains the SDF filters in the PDI IE. These SDF filters are the packet filters set in the QoS Rule of a QoS flow.
  - The QER contains the QoS parameters as per the QoS Description to which the QoS rule is associated.

    The contents of PDR, FAR, and QER are defined in *3GPP TS 29.244*.

QoS Modification

QoS modification may result in one of the following scenarios:

- QoS Flow Addition: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Max Data Burst Volume, QNC). If there is no QoS Flow with the received combination of the flow binding parameters, SMF adds a new QoS flow and the received PCC rules will be mapped against the new QoS flow. As a result, the new QoS flow rules/QoS descriptions/PDR/QER are created and the corresponding interfaces (N1, N2, and N4) are updated by creating new flows.
- QoS Flow Modification: Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Maximum Data Burst Volume, QNC). If there exists a QoS flow with the same combination of binding parameters, the QoS profile, QoS rules, PDR, and QER for that QoS flow are updated on N1, N2 and N4 interfaces.

Qos Capability Support for PCF and SMF Interaction

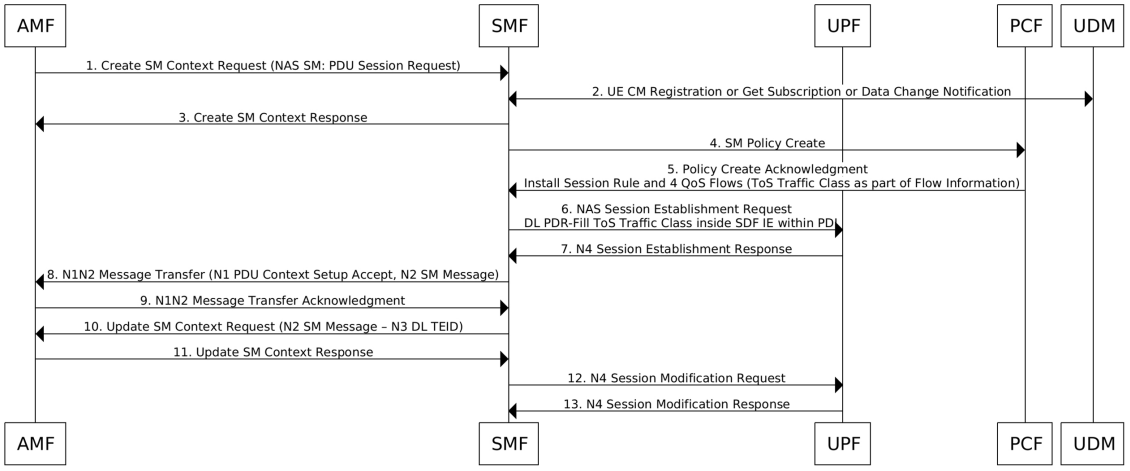
SMF supports Diff-Serv-Code-Point (DSCP) or Type of Service (ToS) QoS functions during interaction with PCF. Traffic defined at SMF can be prioritized based on the `tosTrafficClass` value that SMF receives from PCF. Using the ToS values provided, UPF performs DSCP packet match in the downlink direction and UE performs DSCP packet match in the uplink direction. This feature allows packet matching using ToS values, even if no `FlowDescription` values exist.

The following functions enable this feature:

- PCF sends `tosTrafficClass` IE which is part of `FlowInformation` within the PCC rule from PCF. SMF decodes it and stores it as part of the respective QoS Flow.
- SMF populates the `tosTrafficClass` IE value received from PCF in the `tosTrafficClass` inside SDF IE within PDI while creating the downlink PDR.
- Support for `tosTrafficClass` toward UE.

The following call flow describes the flow from PCF to SMF to support `tosTrafficClass` IE:

Figure 205: Call Flow to Support tosTrafficClass IE



- You can deploy basic PCF which supports minimal functionality. The PCF need not support northbound interfaces and installs dedicated flows which are based on local configuration.
- UE only creates a single session (default bearer) to support data, voice, and video. PCF triggers four flows during PDU session creation, one each for voice, video, data, and network management.
- PCF based on local configuration sends four PCC rules each with `FlowInformation` carrying `tosTrafficClass` IE in the N7 create response.
- SMF supports flow creation for PCC rules mapped with `FlowInformation` having only `tosTrafficClass` and no `FlowDescription`.
- PCF may include `FlowDescription` within `FlowInformation` with filters, such as `permit in IP from any to any` or `permit out IP from any to any`.
- PCF includes QoS Data in `smPolicyDecision` for each of the pcc rules indicating the associated QCI. SMF creates QoS Flow for each of the QCI.
- SMF includes `tosTrafficClass` inside SDF IE in the downlink PDR in `N4SessionEstablishmentReq` to UPF while installing the rules from PCF with mapped `tosTrafficClass`.
- SMF sends the N1 PDU establishment response to PCF. This response includes details, such as QoS rules containing packet filters that are configured with type of service or traffic class type, based on the information that is received from PCF. If the SMF doesn't receive the flow direction from PCF, packet filter direction is populated as `bidirectional` and packet filter component type identifier is populated as `Type of service` or `Traffic class type`.

Note `FlowDirection` is an optional parameter and its default value is **`bidirectional`**.

Bit Rate Mapping Support

Feature Description

Bit Rate Mapping support for 5G Core Network

The SMF receives QoS values for uplink and downlink traffic in bits per seconds (bps) from PCF.

If an interface other than GTPv2 interface sends Access Point Name Aggregate Maximum Bit Rate (APN-AMBR), the SMF converts the received value to kilobits per seconds (kbps). This conversion results in truncation of fractional value to the nearest integer (floor value), and hence the loss of information.

To minimize the bandwidth loss, the CLI command **bitrates rounded-up** is introduced to control the rounding off of the fractional QoS value to ceiling value or floor value. This behavior is in compliance with the 3GPP 29.274 specification, version 12. If the CLI command is enabled within **profile network-element pcf** configuration, the SMF sends the ceiling value over N1, N4, S5, or S8 interface.

In roaming scenarios, when the SMF acts as hSMF and the Bit Rate Mapping Support feature is enabled, then the hSMF sends the rounded-up bit rates in qosFlowDescription over N16 and N4.

When the SMF acts as vSMF and this feature is enabled, vSMF forwards the qosFlowDescription as received over N16 interface and rounds up the Session-AMBR value before sending over N1 and N4 interfaces.

Note vSMF does not communicate with PCF. In order to support this feature, vSMF must have network-element-profiles pcf configured with the feature enabled.

Note The **bitrates rounded-up** CLI command is applicable to both roaming and non-roaming scenarios.

By default, the SMF rounds off the bit rate to the floor value during conversion.

This feature impacts the following procedures:

- 5G session establishment
- 4G session establishment with dedicated bearer
- WiFi call establishment
- Handover scenarios
  - NR to Wi-Fi
  - Wi-Fi to NR
  - Wi-Fi to 4G
  - 4G to Wi-Fi
  - 4G to NR
  - NR to 4G
- PDU session establishment with different Data Network Names (DNNs)

Important If the PCF responds with a bit rate greater than 4.2 Gbps, then the SMF limits the bit rate to 4.2 Gbps only when the Dual Connectivity New Radio (DCNR) is disabled for a 4G-capable UE.

How it Works

This feature works only when the **bitrates rounded-up** CLI command is enabled within **profile network-element pcf** configuration. Upon enabling this feature, the SMF rounds off the QoS value upwards.

For example, if the SMF receives a bit rate of 123,456 bps over N7 interface, it converts the 123,456 bps to 123 kbps and loses the fractional value. With this feature enabled, the SMF converts 123,456 bps to 124 kbps.

Standards Compliance

The Bit Rate Mapping feature complies with the following standard:

- *3GPP TS 29.274, Release 12 – 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*

Configuring Bit Rate Mapping

To enable the Bit Rate Mapping feature, use the following sample configuration.

```
config
  profile network-element pcf profile_name
    bitrates rounded-up
    exit
```

NOTES:

- **profile network-element pcf** *profile_name*: Specify a profile name for the PCF.
- **bitrates rounded-up**: Configure this keyword to round off the fractional QoS value to the ceiling value. The SMF sends the ceiling value over the intended network interface.

  By default, the SMF rounds off the bit rate to the floor value during conversion.

Verifying the Feature Configuration

Use the following command to verify the status of Bit Rate Mapping feature.

```
show full-configuration profile network-element pcf
```

If the bit rate round up is enabled within the PCF profile, then the **bitrates round-up** string is displayed. Otherwise, the string does not appear.

The following configuration is a sample output of this show command:

```
show full-configuration profile network-element pcf
profile network-element pcf pcf1
nf-client-profile PP1
failure-handling-profile FH1
query-params [ dnn ]
rulebase-prefix cbn#
predefined-rule-prefix crn#
bitrates rounded-up
exit
```

Bitrate Mapping across Diameter Interfaces

The SMF receives QoS values for uplink and downlink traffic in bits per seconds (bps) from PCRF.

If an APN-AMBR for uplink and the APN-AMBR for downlink are received from an interface other than the GTPv2 interface, the SMF converts the APN-AMBR for uplink and the downlink values in bits per second to kilobits per second. If this conversion results in fractions, then the value of APN-AMBR for uplink and the APN-AMBR for downlink gets rounded upwards.

By default, if the configuration isn't configured, the SMF rounds off the bit rate to the CEIL value during conversion.

This feature impacts the following procedures:

- 4G session establishment
- Default bearer update over RAR/CCA-U

Configuring Bit Rate Mapping with Diameter Interfaces

To enable Bitrate mapping across Diameter and GTPv2 interfaces, use the following sample configuration.

Note Use the same configuration for dedicated bearer bitrates conversion such as MBR/GBR/APN-AMBR.

```
config
  profile network-element pcrf profile_name
    bitrates rounded-down
    diameter-client-profile Diameter Client_Profile Name
    subscription-idsubscription-id
    exit
```

NOTES:

- **profile network-element pcrf** *profile_name*: Specify a profile name for the PCRF.
- **bitrates rounded-down**: Configures bitrates round down. The SMF sends the Floor value over the intended network interface.

  By default, the SMF rounds off the bit rate to the CEIL value during conversion and the bitrates are rounded-up.

Handling of Authorized QoS for Default Bearer

Feature Description

The CHF server interacts with PCF to report the user quota exhaustion. Then, the PCF initiates a policy update request towards SMF to modify the authorized default Quality of Service (QoS) of a session rule. The QoS can be QoS Class Identifier (QCI) or 5G QoS Indicator (5QI), session Aggregate Maximum Bit Rate (AMBR), or both QCI/5QI and session AMBR.

Whenever the quota of user exhausts, this QoS modification results in downgrading:

- the DSCP marking of the data packets for the session
- the AMBR of the session

When you replenish the quota, the PCF reverts to the previous authorized QoS for the default bearer.

Be aware of the following changes whenever the QCI/5QI changes for the default flow or bearer.

- The QCI/5QI information is updated in the Event Data Record (EDR) generated for that session. Then, the SMF sends the updated bearer level information over Packet Forwarding Control Protocol (PFCP) message to support the EDR functionality.
- DSCP marking for the data packets is updated for all Packet Detection Rules (PDRs) pertaining to the default bearer or flow.
- Any QCI information sent in LI packets are updated.

- Rulebase change and Ruledef activation or deactivation work as expected along with 5QI change and session AMBR change.
- Any modified QoS is sent in Charging Data Request (Update) message to the CHF. Also, change in QCI/5QI in the authorized QoS is treated as a QoS change trigger for charging and CDR-U is sent.

How it Works

This section provides detailed changes in SMF to support change of QCI/5QI value in authorized QoS once the PDU session is established.

Default-Bearer QoS Handling for 4G and WiFi Sessions

The following procedure explains how the SMF handles the modification of authorized default QoS in 4G and WiFi sessions.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed QCI/5QI in AuthorizedDefaultQoS and/or a different session AMBR value.
2. The SMF initiates Update Bearer Request towards S-GW for the default bearer.
   a. In the Update Bearer Request, Bearer Context IE is included for the default bearer and the corresponding Bearer QoS is updated with the changed QCI value.
   b. For the 4G session, the extended Protocol Configuration Options (ePCO), if supported, is included in the Update Bearer Request message. The ePCO includes 5G Authorized QoS Flow Information with updated QCI value for the default flow when the interworking (IWF) is enabled for the session. Otherwise, PCO IE is sent with the same details.
   c. For the WiFi session, Additional Protocol Configuration Options (APCO) is included in the Update Bearer Request message. The APCO contains 5G Authorized QoS Flow Information with updated QCI value for the default flow.
3. The SMF accepts the Update Bearer Response from S-GW.
4. On the N4 interface, the following changes are done:
   a. New instance of the BearerLvlInfo IE is included with the changed QCI value for default bearer tunnel.
   b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
   c. FAR associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling for 5G Sessions

The following procedure explains how the SMF handles the modification of authorized QoS for the default bearer in a 5G session.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed 5QI in AuthorizedDefaultQoS and/or a different session AMBR value.

2. The SMF initiates N1N2MessageTransfer procedure with AMF to send N1 PDU Session Modification Command and N2 PDU Session Resource Modify Request Transfer IE in this message.
   a. In the N1 message, the default QoS flow is modified in Authorized QoS Flow Description IE to update the 5QI value.
   b. In the N1 message, the Mapped EPS Bearer Context IE is modified to update the QCI of the default bearer.
   c. In the N2 message, the QoS flow level QoS parameter for the default flow is modified to update the 5QI value.
3. The SMF accepts the SMContextUpdate Request from AMF with the responses for the N1 and N2 requests sent in N1N2Message Transfer message.
4. On the N4 interface, the following changes are done:
   a. New instance of the BearerLvlInfo IE is included with the changed 5QI to QFI mapping.
   b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
   c. Forwarding Action Rule (FAR) associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

Default-Bearer QoS Handling During WiFi Handovers

The following procedure explains how the SMF handles the modification of authorized default QoS during WiFi handover and other handovers.

1. The SMF sends SMPolicy Update Request to the PCF at the end of each handover procedure. For example, when the PCF arms different policy triggers, the SMF sends SMPolicy Update Request to the PCF. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.
2. For all handovers (excluding WiFi-NR/EPS and NR/EPS-WiFi), the SMF sends SMPolicy Update Request to the PCF indicating the RAT type change. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.

The handovers involving WiFi are different from the other handovers. The SMF triggers SMPolicy Update Request towards PCF during the handover and not after the handover. For the handovers involving WiFi, the target RAN installs the flows and bearers as new instead of an update. The SMF sends the latest QCI received in the response from PCF while installing the default flow and bearer during the handover.

Default-Bearer QoS Modification During Failure Handling

For a 5G session, the modification of QCI/5QI typically does not fail on the N1 or N2 interface as the default flow is a non-GBR flow and no resource reservation is required for the QCI/5QI modification. However, if the modification procedure fails due to no N1 or N2 responses from AMF, the modification is rolled back and the session continues with the old QCI/5QI and session AMBR values. If the N2 rejects the flow modification, the session is deleted as it cannot remain without the default flow.

For a 4G session, the Update Bearer response does not fail for default bearer modification. However, if the Update bearer Response is missing or if it fails, the modification is rolled back and the session continues with the old 5QI and session AMBR values.

For both 4G and 5G sessions, if the N4 update fails or the response is not received, then the SMF takes the action according to the UPF failure handling template configuration. For 4G and WiFi sessions, if there is a failure on the N4 interface, another Update Bearer Request is sent with the old 5QI and AMBR values to S-GW and ePDG respectively.

The failure handling mechanism remains the same for the PCF-initiated modification procedure.

Limitations

The Authorized QoS Handling for Default Bearer feature has the following limitations:

- The combination of QoS flow binding parameters, such as 5QI and ARP, for the authorized QoS never remains the same as that of a dedicated bearer or flow. That is, change in QCI/5QI should not result in the default flow having the binding parameters similar to another flow.
- The SMF does not support changes to all the binding parameters except Allocation and Retention Priority (ARP) and the QCI/5QI (with or without session AMBR) in the Session Rules.
- When the QCI/5QI changes, the existing default bearer flow is modified toward N1, N2, and N4 interfaces. In this case, the SMF does not delete the existing flow instead of creating a new flow.

Authorized QoS Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF maintains the label "SESSRULE_CHANGE" to indicate any changes to the AMBR value, QCI/5QI value, or a combination of both AMBR and QCI/5QI values.

GBR Bearer Creation Based on Local Policy

Feature Description

In cases where a minimum bit-rate guarantee is required, GBR bearers are needed to be created. With the N7 interface, the GBR bearers are created upon receiving the request from the PCF. However, in the absence of PCF, the GBR bearers can be created right after the session creation using the local policy configured in the SMF.

SMF allows creating GBR bearers based on local policies in 4G and 5G RATs.

How It Works

In this approach, there are two bearers created:

1. **Default Non-GBR Bearer**: The default non-GBR bearer/flow is created based on the QoS received from UDM or local configuration in case of New Radio (NR) and the QoS received from MME is used in case of EUTRA.
2. **Dedicated GBR Bearer**: Dedicated GBR flows/bearers are additionally created based on local policy configuration.

Creating Default Non-GBR Bearer and Dedicated GBR Bearer Without PCF

For creating the default bearer/flow, the negotiated QoS profile is chosen.

- For 4G sessions, if N7 interaction is disabled, MME provided QoS is used.
- For 5G sessions, if N7 and N10 interaction is disabled, the locally defined QoS profile, which is associated to the DNN profile is used.

For creating Dedicated Bearer/Flow without PCF intervention, event management policies are required. The association of event management policies with the DNN profile takes place with the help of a configuration. Whenever an event is triggered, the event management policy associated to that DNN is executed. Each event policy configured under the event management policies are executed in a sequence of priority, until a match is found based on event and rule.

The new configuration allows define the event management policies. Multiple priority-based event handling policies can be configured under the event management policy. Each of the event policies configured are executed in the order of priority till a match is found based on event and rule.

In case of NR, the dedicated and default flow parameters are sent to the UE in N1 PDU Session Establishment Accept and to the gNB in N2 Setup Request. In case of E-UTRA, the Default Bearer creation is done as part of the Create Session Response and a GBR Dedicated Bearer is created by triggering a Create Bearer Request (CBR) immediately after sending the Create Session Response. This is similar to the piggy-backed CBR triggered by PCF, which is already supported in SMF.

Note This feature does not supports the real piggybacked-CBR, where CBR and CSR response are sent in the same message.

5G Attach with Dedicated GBR Bearer Creation

The following call flow displays the process of 5G attach with Dedicated GBR Bearer creation:

Figure 206: Call Flow for 5G Attach with Dedicated GBR Bearer Creation (Without PCF Interaction)

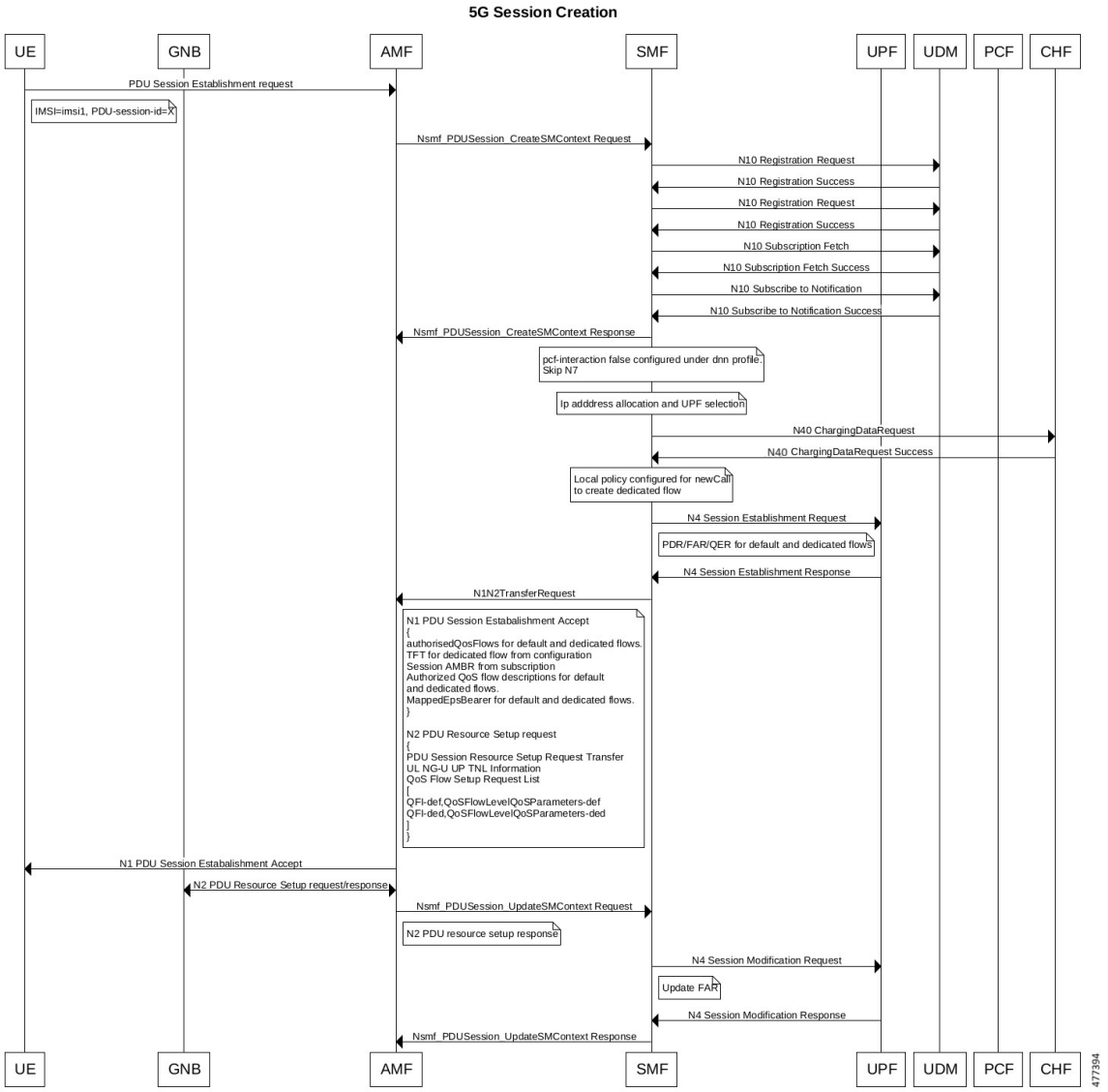


Table 358: Call Flow Description for 5G Attach with Dedicated GBR Bearer Creation (Without PCF Interaction)

Step	Description
1.	The UE initiates the PDU Session Establishment procedure by sending a NAS message to the AMF, containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID and IMSI.
2.	If the AMF does not have an association with an SMF for the PDU Session ID provided by the UE, the AMF invokes the Nsmf_PDUSession_CreateSMContext Request. The AMF forwards the PDU Session ID together with the N1 SM container containing the PDU Session Establishment Request received from the UE.

Step	Description
3.	SMF sends the N10 Registration Request to the UDM. Then, UDM sends the N10 Registration Response to the SMF.
4.	SMF sends the N10 Subscription Fetch Request to the UDM. Then, UDM sends the N10 Subscription Fetch Response to the SMF.
5.	SMF sends the N10 Subscribe to Notification Request to the UDM. Then, UDM sends the N10 Subscribe to Notification Success Response to the SMF.
6.	If the SMF is able to process the PDU Session Establishment Request, the SMF creates an SM context. Then, SMF sends the Nsmf PDU Session CreateSMContext Response to the AMF. If the PCF is not deployed, hence **pcf-interaction false** has to be configured on the SMF. Hence, SMF applies the local configuration to perform the mapping of PCC rules and 5G QoS parameters. At this stage, the SMF also selects one or more UPFs.
7.	(Optional) The SMF sends a charging data request over the N40 interface to the CHF. Then, the CHF responds back to the SMF with N40 ChargingDataRequest Success response.
8.	At this stage, the local policy is used to configure a new call to create a dedicated flow. If the predefined rules are mapped to a dedicated flow/bearer, SMF sends the N4 Session Establishment Request to the UPF. SMF also sends Create PDR/FAR/QER/URR Request for both default and dedicated flows to the UPF.
9.	The UPF responds to SMF with the N4 Session Establishment Response.
10.	SMF sends the NamfCommunication N1N2 Message Transfer request to AMF. This message contains N1 PDU Session Establishment Accept with authorized QoS Flows for both default and dedicated flows, TFT for dedicated bearer from configuration, Session AMBR from subscription, Authorized QoS flow descriptions for default and dedicated flows, and Mapped EPS bearers for default and dedicated flows. The NamfCommunication N1N2 Message Transfer request also contains N2 PDU Resource Setup Request containing PDU Session Resource Setup Request Transfer, UL NG-U UP TNL Information, and QoS Flow Setup Request List.
11.	The N1 PDU Session Establishment Accept is sent from AMF to the UE.
12.	The N2 PDU Resource Setup Request is sent from the AMF to the gNB. In response, the gNB sends the N2 PDU Resource Setup Response to the AMF.
13.	AMF sends the Nsmf PDU Session UpdateSMContext Request (N2 PDU Resource Setup Response) to SMF. This message contains N2 PDU Resource Setup Request.
14.	SMF sends the N4 Session Modification Request to UPF. This request is to update FAR with GNB tunnel information.
15.	UPF sends the N4 Session Modification Response to SMF.
16.	SMF sends the Nsmf PDU Session UpdateSMContext Response to AMF.

4G Attach with Dedicated GBR Bearer Creation

The process of 4G attach with the Dedicated GBR Bearer creation follows the given steps:

Figure 207: Call Flow for 4G Attach with Dedicated GBR Bearer Creation

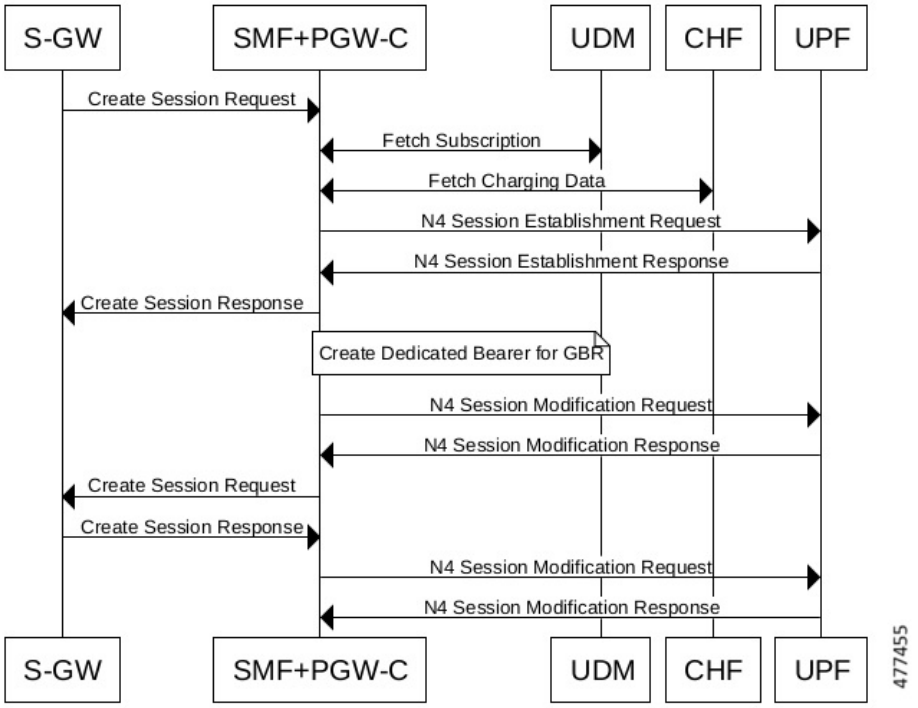


Table 359: Call Flow Description for 4G Attach with Dedicated GBR Bearer Creation

Step	Description
1.	S-GW sends the Create Session Request to SMF.
2.	SMF sends the Subscription Fetch Request to the UDM. Then, UDM sends the Subscription Fetch Response to SMF.
3.	SMF sends the Charging Data Request to CHF. Then, CHF sends the N40 Charging Data Response to the SMF.
4.	SMF sends the N4 Session Establishment Request to UPF.
5.	After the creation of the tunnel, UPF sends the N4 Session Establishment Response to SMF.
6.	SMF sends the Create Session Response to S-GW. This response includes the 4G default bearer tunnel information.
7.	Dedicated GBR bearer creation is initiated based on local policy configuration. At this stage, SMF sends the N4 Session Modification Request to the UPF. This message includes a request for creating a dedicated GBR bearer.

Step	Description
8.	UPF sends the N4 Session Modification Response to the SMF.
9.	SMF sends the Create Bearer Request to S-GW. This request includes information on the bearer context list, which contains information about QOS, TFTs, and UPF FTEIDs.
10.	SGW sends the Create Bearer Response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
11.	SMF sends the N4 Session Modification Request to UPF. This request is to update FAR with SGW-U tunnel information for each bearer
12.	UPF responds with N4 Session Modification Response to the SMF and the bearer is established on SMF.

Limitations

Following are the known limitations of this feature:

- This feature supports 4G calls without PCF and not without PCRF.

Configuration for Creating Default Non-GBR Bearer and Dedicated GBR Bearer without PCF

To create Default Non-GBR and Dedicated GBR bearers, the following step-wise configuration is required:

1. Associate QoS profile and event management policy to the DNN profile. A new CLI is introduced for this configuration.
2. Create QoS configuration for the default flow/bearer. This is an existing configuration. For more details, refer to Configuring QoS Parameters.
3. Add an event management configuration by defining the priority, the event to be executed, the rules, and the actions to be performed, if there is a rule match.
4. Add rule definition policies by specifying the conditions for rules.
5. Add action definition policies, the action will be to activate the rulebase to create GBR bearer/flow.
6. Configure rulebase, pre-defined rules, and charging-action. This is an existing configuration. For more details, refer to Configuring ACS Rulebase in ACS Configuration Mode.
7. Configure QoS for each of the dedicated bearer/flow QCI/ARP. This is an existing configuration. For more details, refer to Configuring Bandwidth ID.

Configuration for Associating QoS Profile and Event Management Policy to the DNN Profile

Associating the QoS profile and event management policy to the DNN profile can be done through following configuration:

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    eventmgmt-policy eventmgmt_policy_name
    exit
```

NOTES:

- **eventmgmt-policy** *eventmgmt_policy_name*—This CLI allows configuring priority-based event handling associated to a DNN. Each of the event policy configured under **eventmgmt-policy** are executed in the order of priority till a match is found based on event and rule.
- **qos-profile** *qos_profile_name*—This CLI allows associating the QoS profile and the event management policy to the DNN profile. This QoS profile will be used to read QoS values for 5G default flow, if the UDM does not provide it.

Configuration for Adding Event Management Policy

Adding an event management policy happens through the following configuration:

```
config
  policy eventmgmt policy_eventmgmt_name
    priority  event_priority [ event event_name ] ruledef ruledef_name actiondef
 actiondef_name
    exit
```

NOTES:

- **eventmgmt** *policy_eventmgmt_name*—This CLI allows configuring the event management policies and defining the attributes.
- **priority** *event_priority*—Allows defining the priority of a particular event management policy.
- **event** *event_name*—This is an optional CLI that defines an event for which a particular action is to be performed. It supports only **new-call** as the event name. For semantic and syntactic error handling scenarios, it supports **cbr-resp** as the event name.

  If the **event** is not configured, **actiondef** is executed for all the defined events if there is a rule match.
- **ruledef** *ruledef_name*—Defines a rule for a local policy that when matched an action is performed.
- **actiondef** *actiondef_name*—Configures the action name to be executed.

Configuration for Adding Rule Definition Policies

The following configuration allows adding rule definition policies:

```
config
  policy rulemgmt policy_rulemgmt_name
    ruledef rule_def condition condition_string
    exit
```

- **rulemgmt** *policy_rulemgmt_name*—Defines a rule to be added in the policies.
- **ruledef** *rule_def*—Configures a rule attribute. A ruledef is declared when the conditions match.

- **condition** *condition_string*—Defines the use cases for a rule. It only supports **any** and **cause matches "cause"** conditions.

Configuration for Adding Action Definition Policies

The following configuration adds action definition policies:

```
config
  policy actionmgmt policy_actionmgmt_name
    actiondef actiondef_name
      priority priority_number action action_name [ attributes { rulebase
rulebase_name [ rules rules_name ] } ]
      exit
```

NOTES:

- **actionmgmt** *policy_actionmgmt_name*—Configures the action to be executed.
- **actiondef** *actiondef_name*—Defines the action attributes to be executed. Currently, it supports only **activate-rulebase** as the action.

  In the semantic and syntactic error handling, the actions differ while the UE is in the 4G or 5G RAT.
- **priority** *priority_number*—Defines the priority in which the actions are to be executed.
- **action** *action_name*—Defines the actions associated with an actiondef in the order of priority. In case of GBR creation failure, SMF supports **release-session** action.
- **attributes** —Defines the attributes of a particular action. This is an optional command.
- **rulebase** *rulebase_name*—Defines a collection of protocol rules to match a flow and associated actions to be taken for matching the flow.
- **rules** *rules_name*—Defines a list of rules to be executed.

Note The existing configurations of charging action, bandwidth policy, and packet filter are used to configure QoS parameters of each rule.

Configuration Example

Following is the sample configuration for associating QoS profile and event management policy to the DNN profile:

```
config
profile dnn dnnprof-data
qos-profile qos camera_profile
eventmgmt-policy emp
end
```

Following sample configuration adds the event management policy:

```
policy eventmgmt emp
 priority 1 event new-call ruledef rd1 actiondef ad1
end
```

Following is the sample configuration for adding the **any** and **cause matches "cause"** rule definition policies:

```
policy rulemgmt rm1
  ruledef rd1
    condition "any"
    end
```

```
policy rulemgmt rm1
ruledef rd1
condition cause matches [ 83 ] source ue
```

Following is the sample configuration for adding action definition policies:

```
policy actionmgmt am1
  actiondef ad1
    priority 1 action activate-rulebase  attributes rulebase rb1 rules [r1,r2]
    exit
end
active-charging service olympics
rulebase rb1
bandwidth default-policy bw_policy1
action priority 1 dynamic-only ruledef r1 charging-action ca1
action priority 2 dynamic-only ruledef r2 charging-action ca2
exit

charging-action ca1
allocation-retention-priority 1
qos-class-identifier 6
tft packet-filter tft1
flow limit-for-bandwidth id 1
end

packet-filter tft1
direction bi-directional
ip protocol 6
ip remote-port range start 1002 end 1005
end

active-charging service acs1
bandwidth-policy bw_policy1
flow limit-for-bandwidth id 1 group-id 1
group-id 1 direction uplink peak-data-rate 1000000000 peak-burst-size 100 violate-action
discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
group-id 1 direction downlink peak-data-rate 2000000000 peak-burst-size 100 violate-action
 discard committed-data-rate 1000 committed-burst-size 100 exceed-action discard
```

For handling the case where dedicated bearer creation fails, it is recommended to have the following configuration:

```
policy eventmgmt emp
  priority 2 event cb-resp ruledef rd3 actiondef ad3
      exit

policy rulemgmt rm1
      ruledef rd3
               condition cause matches "cause"
            exit
     exit

policy actionmgmt am1
      actiondef ad3
priority 1 action release-session
            exit
exit
```

OAM Support

This section discusses the metrics and statistics supported in this feature.

Metrics

As part of this feature the following label is added in the **smf_service_stats**:

- **policy_status**: This metric is associated with the configured local policy.

SMF-triggered Metadata for EDR Generation on UPF

The SMF provides the following metadata to the User Plane Function (UPF) to enable EDR generation.

- Called-Station-ID: Specifies the DNN for the session
- Calling-Station-ID: Specifies the MSISDN of the UE
- RAT Type: RAT type for the current session (NR or EUTRAN)
- ULI: User location for the current session

The UPF receives preceding data in the "Subscriber Parameters" IE in the PFCP Session Establishment Request message. The RAT type and ULI can change during the lifetime of session (for events, such as 5G to 4G handover). The UPF receives the changed values of these parameters in the PFCP Session Modification Request message.

Note

- All the parameters are always sent from the SMF to the UPF irrespective of EDR configuration being available. These parameters ensure that any change in configuration after the session creation is immediately applied on the UPF.
- The SMF supports EDR related configurations. However, the SMF does not require these configurations for its functionality. These configurations are sent to the UPF.

For more information on the UPF EDRs, see the *UCC 5G UPF Configuration and Administration Guide*.

Dynamic Configuration Update

Feature Description

The SMF allows you to dynamically change the configuration of SMF profile and SMF service profile.

It is mandatory to perform following maintenance operational procedure for changes to certain SMF profile or service profile configuration parameters. This maintenance operational procedure operation helps to keep the SMF system in maintenance mode so that it doesn't impact the system by rejecting the new sessions. Also, this maintenance procedure provides flexibility to operators to clear the subscribers manually by executing **clear subscriber all** command.

The SMF updates configuration parameters change to NRF by sending "NFUPdate" using PUT Method.

How it Works

This section describes the maintenance operational procedure and how dynamic change in configuration works for the supported SMF configurations.

Maintenance Operational Procedure

For a change in the configuration parameters that require mandatory operational maintenance, perform the following steps:

1. Shutdown (offline) SMF by executing **mode offline** CLI command under SMF profile.

   The SMF sends NFUpdate with Method PUT and NFStatus as "UNDISCOVERABLE".

Note During the online to offline transition period, the SMF does not accept any new request.

2. Clean up the sessions using **clear subscriber sess all** CLI command.
3. Change the configurations and remove **mode offline** CLI command.

   SMF sends NFUpdate with Method PUT and NFStatus as "Registered".

SMF Profile and SMF Service Profile

The following table describes how dynamic change in configuration works for the supported SMF configurations.

Table 360: Dynamic Change in SMF Profile and SMF Service Profile

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
locality	Allowed	Sessions will start using the newer values.	Not Required	Required
node-id	Not applicable	No impact	Not applicable	Not applicable
fqdn	Allowed	SMF always fetches the latest FQDN value for sessions while interacting with UDM.	Required	Required
allowed-nssai	Allowed	Sessions will start using the newer values.	Required	Required
plmn-id	Allowed	Sessions will start using the newer values.	Required	Required

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
service name, schema, service-id, version	Allowed	Sessions will start using the newer values.	Required	Required
http-endpoint	Allowed	Sessions will start using the newer values.	Required	Required
icmpv6-profile	Allowed	Sessions will start using the newer values.	Not required	Not required
compliance-profile	Allowed	SMF might perform parse-failure because of incompatibility issues between SMF and other NFs for various SBI interfaces.	Not required	Not required
access-profile	Allowed	Sessions will start using the newer values.	Not required	Not required
subscriber-policy	Allowed	Sessions will start using the newer values.	Not required	Not required

Configuring Dynamic Configuration Change Support

To enable the offline mode of operation under SMF profile, use the following sample configuration.

```
config
  profile smf profile_name
    mode offline
    exit
```

NOTES:

- **mode**: Specify the mode of operation.
- **offline**: Specify the mode is offline and new sessions are rejected.

Verifying Dynamic Configuration Change Support Configuration

Use the **show running-config profile smf** CLI command to verify if the feature is enabled. When enabled, the following field will be displayed as part of the show command output:

- mode offline

Dynamic PCC Rules Enforcement

Feature Description

SMF uses either the Policy and Charging Control (PCC) rules from Policy Control Function (PCF) or the locally configured policy rules to control the policy management. The PCF sends the PCC rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define the QoS flows and apply the QoS enforcement (via UPF) and charging towards CHF.

The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

The following sections provide information on the features that are implemented for the dynamic policy management.

Supported Features Negotiation

The SMF and the PCF negotiate the supported features during Policy Context Creation and during PDU session establishment. Based on the negotiated features, the PCF provides the relevant information.

The following table lists the features that can be negotiated as defined in the 3GPP specification 29.512.

Table 361: Supported Negotiated Features

Feature Number	Feature Name	Description
1	TSC	This feature indicates support for traffic steering control in the (S)Gi-LAN or routing of the user traffic to a local Data Network identified by the DNAI per Application Function (AF) request. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.6.2.20.
2	ResShare	This feature indicates the support of service data flows that share resources. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.7.4.
4	ADC	This feature indicates the support of application detection and control.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network.
8	EPSFallbackReport	Indicates EPS Fallback has occurred and resource corresponding to rules in rule report were setup successfully post EPS Fallback. SMF performs the function as described in 3GPP Specification Release 16.10.0, 23.502/29.512.

The SMF sends supportedFeatures attribute in the Npcf_SMPolicyControl_Create message, and further includes a bitmap representing the supported features. The PCF also sends the supportedFeatures attribute in the response message. The response should either match or be a subset of the request.

The string contains a bitmask indicating supported features in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents the support of the features as described in the preceding table. The most significant character representing the highest-numbered features appears first in the string, and the character representing features 1–4 appears last in the string. The list of features and their numbering (starting with 1) are defined separately for each API.

Provisioning and Management of Session AMBR and Default QoS

For the N4 interface, the SMF sends the QoS information in the form of:

- Packet Detection Rule (PDR)
- Forwarding Action Rule (FAR)
- QoS Enforcement Rule (QER)

The SessionAMBR includes the maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session. The SMF sends the session level QER for non-GBR flows along with existing QER to the UPF.

The SMF receives sessionRule from PCF in SmPolicyDecision during PDU session creation. The sessionRule consists of authSessAmbr and authDefQos. The authorized AMBR consists of the Uplink (UL) and Downlink (DL) MBR at a session level and authDefQos contains the 5Qi, ARP, and other QoS binding parameters for the default QoS flow.

The SMF performs the following actions:

- Any PCC rules received from the PCF that have an associated QoS Desc with the same binding parameters as received in authDefQos are tagged with the default QoS flow.
- On the N4 interface, the UL and DL Packet Detection Rules (PDRs) are created for each PCC rule that is associated with the default QoS flow. For session AMBR enforcement, the SMF creates a QoS Enforcement Rule (QER) with appropriate AMBR and associates it with all PDRs for non-GBR rules.
- On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR and 5Qi values. The Session AMBR is also sent in this message.
- On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the AMBR and the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFI.
- The SMF supports the UDM-initiated Session AMBR modification. In this case:
    - The SMF sends Npcf_SMPolicyControl_Update to the PCF along with the new subscribed session AMBR within the "subsSessAmbr" attribute and the SE_AMBR_CH policy control request trigger within the "repPolicyCtrlReqTriggers". On receiving the change of session AMBR, the PCF provisions the new authorized session AMBR to the SMF in the response.
    - Update the QERs on N4 interface for Session AMBR enforcement.
    - Initiate N1N2MessageTransfer towards the AMF with Sess AMBR in PDU SESSION MODIFICATION COMMAND message in N1 interface and PDU Session Resource Modify Request transfer IE in N2 container having the new AMBR.

Provisioning of Policy Revalidation Time

Feature Description

The PCF instructs the SMF to trigger PCF interaction to request PCC rule from the PCF if not provided yet. The PCF performs this operation by providing revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute in SmPolicyDecision. The PCF can change the revalidation time by including a new value for the "revalidationTime" attribute. The PCF can also disable the revalidation function by removing RE_TIMEOUT policy control request trigger if it has been provided.

If the SMF receives the existing revalidation time or the new revalidation time, the SMF stores the received value and starts the timer based on it. Then, the SMF sends the PCC rule request before the indicated revalidation time. If the RE_TIMEOUT policy control request trigger is removed, the SMF stops the timer for revalidation.

Note When the RE_TIMEOUT is removed, the revalidation time value previously provided to the SMF is no longer applicable.

How it Works

Revalidation time is a string of the format "date-time" as defined in OpenAPI specification. The SMF, on receiving the revalidation time in "revalidationTime" attribute and RE_TIMEOUT trigger in "policyCtrlReqTriggers" attribute, starts a timer for the difference duration (revalidationTime – currentTime – 5 seconds buffer). Once the timer expires, the SMF initiates the PCF interaction to request PCC rules.

Standard Compliance

The Policy Revalidation Time feature complies with *3GPP TS 29.512, v15.2.0*.

Provisioning and Management of Additional QoS Flows

The PCF can create, modify, or delete multiple GBR and non-GBR PCC rules.

The following scenarios are possible:

1. Multiple non-GBR and GBR PCC rules are activated during PDU session establishment. In this case:
   a. The SMF creates the QoS flow according to the QoS flow binding principle as described in the QoS Management section.
   b. On the N4 interface, the UL and DL PDRs are created for each PCC rule that is associated with all the flows. For flow-level QoS enforcement, the SMF creates QERs with the MFBR and GFBR (for GBR flows) values and associates it with each PDR of a flow.
   c. On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR, GFBR, and 5Qi values. The packet filters associated with each QoS rule are sent on the N1 interface in the "Authorized QoS Rules" attribute.
   d. Different types of packet filters are supported on both the N4 and the N1 interfaces. This list includes:

```
Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
```

```
0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
```

e. On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFIs for each of the flows. The "GBR QoS Flow Information" field of the IE contains the MFBR and GFBR of the GBR flows.

2. Modification of PCC rules after PDU session establishment. In this case, the following scenarios are observed:

a. Modification, addition, and removal of packet filters of one or more PCC rules:

1. In this case, the SDF filters of the PDR on the N4 interface are changed by invoking N4 session modification.

2. The SMF initiates N1N2MessageTransfer towards the AMF with "Authorized QoS Rules" attribute in PDU SESSION MODIFICATION COMMAND message in N1 interface. The rule operation code in this attribute is one of the following:

```
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filter
```

b. Change in QoS associated with one or more PCC rules:

1. The SMF performs QoS flow binding evaluation which in turn results in the following operations:

1. Addition of a new QoS flow results in change of QFI on the N4 interface for some of the PDRs.

2. Movement of a PCC rule from one QoS flow to another QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

3. Removal of a QoS flow when the last PCC rule in that flow is moved to a different QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.

2. In the preceding cases, on the N1 interface the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description
```

3. On the N2 interface, QoS Flow Level QoS parameters of the PDU Session Resource Modify Request transfer IE carry the modified GFBR, MFBR, 5Qi and so on. For any flow removal, the QoS Flow to re-lease List is included in this IE.

c. PCC rule removal:

1. In this case, the SMF removes all the PDRs associated with a QoS flow on the N4 interface.

2. On the N1 interface, the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

   ```
   0 1 0 Delete existing QoS flow description
   ```

3. On the N2 interface, the PDU Session Resource Modify Request transfer IE carries the QoS Flow to release List.

QoS Enforcement

The SMF enforces QoS at PCC rule (SDF) level, QoS flow level, and session level by creating one QER:

- per PCC rule level to enforce MBR/GBR as per the associated QoS Desc supplied by PCF and associated to the given PCC rule.
- at QoS flow level which has aggregated MBR/GBR of all the PCC rules associated with a QFI.
- at session level to enforce the Session AMBR for all non-GBR QoS flows.

Once these QERs are created, the SMF associates:

- the session level QER to all PDRs belonging to the non-GBR QoS category.
- the SDF level QER to each individual PCC rule.

For any QoS modification including movement of the PCC rules from one flow to another and QoS modification within flow, the SMF modifies the GFBR/MFBR (or Session AMBR) and updates the QERs accordingly on the N4 interface.

Policy Control Request Triggers

The PCF provides one or more policy control request trigger(s) by including the triggers in the "policyCtrlReqTriggers" attribute(s) in the SmPolicyDecision data structure.

During the lifetime of the PDU session, the PCF updates or removes the policy control request triggers. To update the trigger, the PCF provides a new complete list of applicable policy control request triggers by including the trigger(s) in the "policyCtrlReqTriggers" attribute.

The PCF removes all previously provided triggers by providing a "policyCtrlReqTriggers" attribute set to NULL value. Upon reception of a policy control request trigger with this value, the SMF does not inform PCF of any trigger except for those triggers that are always reported and does not require provisioning from the PCF.

Whenever the PCF provisions the trigger, unless otherwise specified in the trigger's value definition, the SMF sends the corresponding currently applicable values (for example, access type, RAT type, user location information, and so on) to the PCF within the UeCampingRep data structure in the response of the HTTP POST message. In this case, the "repPolicyCtrlReqTriggers" attribute is not included.

The list of supported triggers is as follows:

Trigger	Description

RES_MO_RE	A request for resource modification has been received by the SMF. This is a mandatory trigger. **Note** This request is sent from SMF to PCF when UE/AMF requested QoS modification is triggered.
UE_IP_CH	UE IP address change. This is a mandatory trigger.
DEF_QOS_CH	Default QoS Change. This is a mandatory trigger.
SE_AMBR_CH	Session AMBR Change. This is a mandatory trigger.
SAREA_CH	Location Change about the Serving Area in N11 update.
SCNN_CH	Location Change about the Serving CN node. See the following section for details on how the SMF supports this trigger during the different handover scenarios.
RE_TIMEOUT	Indicates that the SMF has generated the request because there has been a PCC revalidation timeout (that is, Enforced PCC rule request as defined in Table 6.1.3.5.-1 of *3GPP TS 29.503*).
EPS_FALLBACK	Indicates that SMF supports EPS Fallback Report functionality for pccRules for which the EPS_FALLBACK trigger was sent by PCF.

Support SCNN_CH Trigger in Handovers

The SMF supports the serving network change trigger in the following handovers:

- **Inter AMF Handover**: If the "SCNN_CH" is provisioned, when the SMF detects a change of serving Network Function (for example, the AMF), the SMF includes the "SCNN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving Network Function in the "servNfId" attribute. When the serving Network Function is an AMF, the SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to 4G handover**: When the UE handed over from the 5GS to EPC/E-UTRAN, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute.
- **4G to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **WiFi to 5G handover**: The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to WiFi handover**: When the UE handed over from the 5GS to EPC non-3GPP access, the SMF includes, if the "SCNN_CH" policy control request trigger is provisioned and met, the ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

Gating Control

Feature Description

Gating control is the capability to block or allow IP packets belonging to a certain IP flow, based on the decisions by the PCF. The PCF could, for example, make gating decisions based on session events (start and stop of service) reported by the AF.

The AF instructs the PCF to temporarily block the user traffic corresponding to a specific PCC rule on uplink or downlink direction, or both the directions.

To enable the PCF gating control decisions, the AF reports session events (for example, session termination, modification) to the PCF. For example, session termination, in gating control, triggers the blocking of packets or "closing the gate".

Note Gating Control applies only for service data flows of IP type.

How it Works

The Gating Control feature works in the following manner:

1. PCF sends flowStatus attribute in TrafficControlData referenced by the PCC rule. The value of this attribute is set to "enabled", "disabled", "enable_uplink", or "enable_downlink" based on the PCF decision.
2. On receiving this attribute, the SMF instructs the UPF to open or close the GATE for the UL or DL Packet Detection Rule (PDR), or both UL and DL PDRs for the associated PCC rule. The Gate Status Information Element (IE) in Create QoS Enhancement Rule (QER) or Update QER associated with the PDR is set to OPEN or CLOSED.
3. If there is any subsequent change, the PCF triggers a N4 modification request to change the GATE status.

Standards Compliance

The Gating Control feature complies with the following standards:

- *3GPP TS 29.512, version 15.2.0*

How it Works

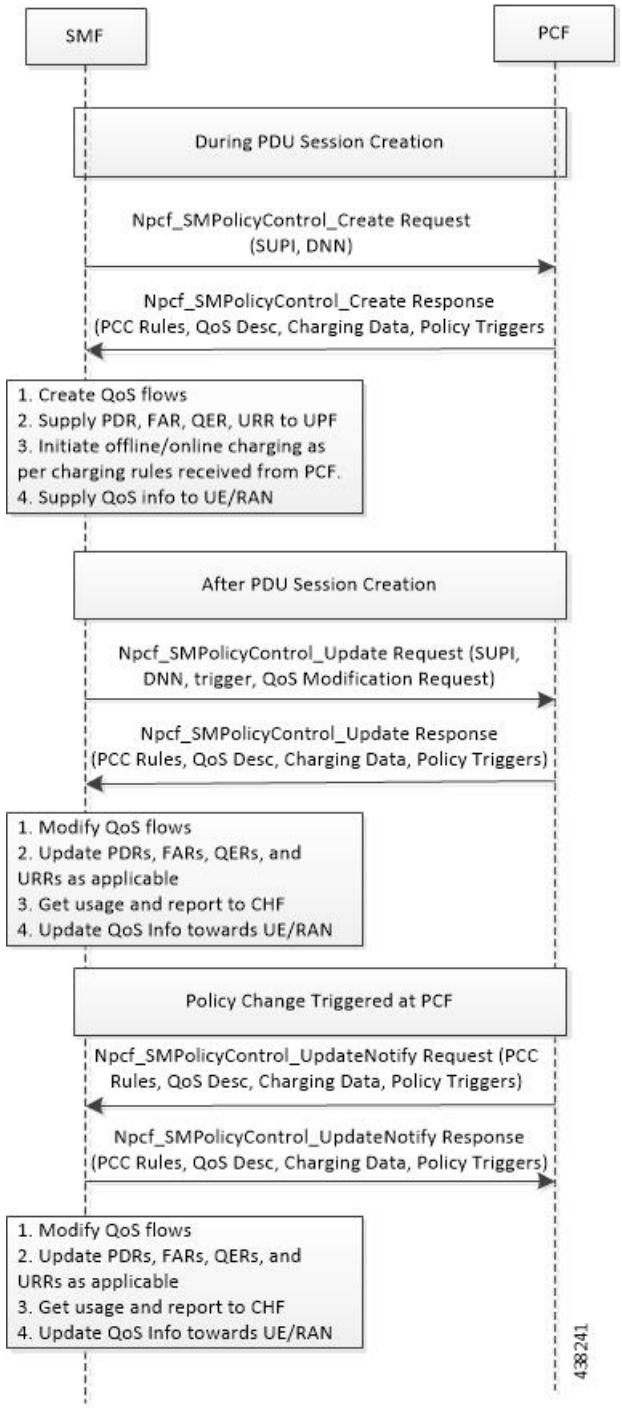
The SMF requests the policy information from PCF. The PCF in turn provides the policy rules during and after PDU session creation to enable the dynamic policy application. Dynamic policy management involves the following operations:

- Policy Context Creation: This operation is performed at the time of PDU session create and the PCF sends the PCC rules and the associated QoS, Charging and other policy data in the response message.
- Policy Context Update: For any RAN-initiated or UE-initiated policy updates and for notification of trigger events, the SMF initiates a policy context update. In response, the PCF sends the changed policy data that impacts the QoS and charging.

- Policy Context Update Notification: During the lifecycle of a PDU session, the PCF can initiate a policy update based on interaction with the AF or local configuration changes at PCF. The SMF handles the updated policy rules when received in a notification from the PCF.
- Policy Context Delete: At the end of a PDU session, the SMF terminates the Policy Context with PCF.

The following figure illustrates the dynamic policy management procedure for a PDU session.

Figure 208: Dynamic Policy Management Call Flow



Standards Compliance

The Dynamic PCC Rules Enforcement feature complies with the following standard:

- *3GPP TS 29.512 Version 15.4.0 – 5G; 5G System; Session Management Policy Control Service; Stage 3*

Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes

Configuring the Dynamic PCC Rules Enforcement Feature

This section describes how to configure the Dynamic PCC Rules Enforcement feature.

Configuring the Dynamic PCC Rules Enforcement feature involves the following steps:

1. Creating QoS Profile, on page 1027
2. Configuring QoS Parameters, on page 1027
3. Defining QoS Profile in DNN Profile Configuration, on page 1028

Creating QoS Profile

To create an instance of a quality of service (QoS) profile, use the following sample configuration.

```
config
  profile qos qos_profile_name
  exit
```

NOTES:

- **qos** *qos_profile_name*: Create a quality of service profile and provide access to the QoS Profile Configuration mode to configure the QoS parameters. *qos_profile_name* must be an alphanumeric string uniquely identifying the QoS profile.

Configuring QoS Parameters

To configure the QoS parameters, use the following sample configuration.

```
config
  profile qos qos_profile_name
     ambr { ul uplink_ambr | dl downlink_ambr }
     arp { preempt-cap preemption_capability |
     preempt-vuln preemption_vulnerability |
     priority-level priority_level }
```

```
max data-burst burst_volume
priority qos_priority
qi5 5qi_value
exit
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Define the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specify the preemption capability flag. The options are:
  - MAY_PREEMPT—Bearer may be preempted
  - NOT_PREEMPT—Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specify the preemption vulnerability flag. The options are:
  - PREEMPTABLE—Bearer may be preempted
  - NOT_PREEMPTABLE—Bearer cannot be preempted
- **arp priority-level** *priority_level*: Define the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Define the maximum data burst volume. *burst_volume* must be an integer in the range of 1–4095.
- **priority** *qos_priority*: Specify the 5QI priority level. *qos_priority* must be an integer in the range of 1–127.
- **qi5** *5qi_value*: Specify the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer in the range of 0–255.

Defining QoS Profile in DNN Profile Configuration

To configure the QoS profile in the existing DNN profile, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
    exit
```

NOTES:

- **qos-profile** *qos_profile_name*: Define the locally configured default QoS profile. This profile is configured under the existing DNN Profile configuration. *qos_profile_name* must be the name of the configured QoS profile.

Verifying the Dynamic PCC Rules Enforcement Feature Configuration

This section describes how to verify the Dynamic PCC Rules Enforcement feature configuration.

Use the following show command to verify the feature configuration details.

show full-configuration

The following is an example of this show command output.

```
show full-configuration
profile dnn dnn1
qos-profile qos1
!
profile qos qos1
ambr ul 1024
ambr dl 1024
qi5 128
arp priority-level 8
arp preempt-cap NOT_PREEMPT
arp preempt-vuln NOT_PREEMPTABLE
priority 9
max data-burst 2048
exit
```

Controlling PCF and SMF Interaction

PCF and SMF interaction for subscriber calls is enabled by default. To disable the PCF interaction with SMF, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    pcf-interaction { false | true }
    end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile name. *dnn_profile_name* must be an alphanumeric string.
- **pcf-interaction { false | true }**: Disable or enable the interaction with PCF.
  - **false**: SMF does not interact with PCF.
  - **true**: SMF interacts with PCF wherever applicable as part of all call flows. This is the default configuration.

Note The **pcf-interaction { false | true }** CLI command will be deprecated in the future releases.

Configuration Example

The following is an example configuration.

```
config
profile dnn intershat1
pcf-interaction false
end
```

Configuration Verification

Check the **pcf-interaction** configuration to determine if PCF interaction with SMF is enabled or disabled. To verify the configuration, use the following command at the Exec mode:

show running-config profile dnn intershat1

You can also verify the feature configuration using the following show command at the Global Configuration mode.

show full-configuration profile dnn intershat1

The following is an example output of the **show running-config profile dnn intershat1** command.

```
[smf] smf# show running-config profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

The following is an example output of the **show full-configuration profile dnn intershat1** command.

```
[smf] smf(config)# show full-configuration profile dnn intershat1
profile dnn intershat1
 dns primary ipv4 209.165.200.239
 dns primary ipv6 fd01:976a::9
 dns secondary ipv6 fd01:976a:c002:1:fd95:6218:825e:f867
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 charging-profile chgprf1
 virtual-mac      b6:6d:47:47:47:48
 pcscf-profile    PCSCF_Prof_2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat1
 pcf-interaction  false
exit
```

In the preceding examples, **pcf-interaction false** is displayed, indicating that SMF does not interact with PCF.

Handling Traffic Flow for Dedicated UE Services

Table 362: Feature History

Feature Name	Release Information	Description
Handling Traffic Flow for Dedicated UE Services	2024.01.2	This feature allows specific UEs, like PTTs, to connect on the 5G RAT using specific TFTs. To enable this functionality, PCF sets the value of the **PacketFilterUsage** IE attribute to **true** in the dynamic PCC rule. This rule causes the SMF to only send the PCC Rule TFTs instead of the IP "Any-Any". This feature is only applicable for default flow. **Default Setting:** Enabled - Always-on

Feature Description

When a specific UE with a limited-service accessibility (such as a PTT device) attaches to the 5G RAT, the PCF sends dynamic PCC rules associated with a default flow to the SMF. If PCF sends a **PacketFilterUsage** IE with value set to **true** in the dynamic PCC rule and if the PCC rule is associated to the default flow, SMF adds the QoS rule with the flow information and sends the TFT (Traffic Flow Template) to the UE.

If the **packetFilterUsage** IE is set to false, SMF adds the QoS rule with "**Any-Any**" filter and sends it to the UE. The packet filter "**Any-Any**" is a default filter that allows the UEs to communicate with any IP and avail any service. The purpose of this feature is to enable the prioritization of packets to support dedicated UE services such as PTT service.

This feature is supported only for dynamic rules and not for static or predefined rules. This feature is also not applicable for dedicated bearer.

Note As there is no impact on the N4 interface, all the rules and filters are sent to UPF as received from the PCF.

How It Works

Sending the TFT parameters associated to the default flow toward the UE happens through the following steps:

1. **PCC Rule Identification**: The following two conditions are used for identifying the PCC rule associated with the default flow:
   - If a PCC rule is associated to the QoS Data with the same binding parameters (5QI, arp) as the authDefQos (authDefQos contains the 5QI, ARP, and other QoS binding parameters for the default QoS flow) parameter.

Note For the PCC rules associated with default flow, only the **authDefQos** parameter is considered and all other QoS parameters are ignored.

   - If a PCC rule received from the PCF has **defQosFlowIndication** IE set to **true**.

2. **TFT Update**: SMF sends the corresponding TFT parameters to the UE based on the following conditions:

Conditions	Expected Behavior	Comments
PCC rules with **packetFilterUsage IE** set to **true**.	TFT associated to that PCC rule is sent to UE over the N1 interface.	
PCC rules with **packetFilterUsage IE** set to **false**.	"**Any-Any**" TFT is sent to the UE.	
Existing TFT with "**Any-Any**" filter + new rules with **packetFilterUsage** IE set to **true**.	SMF updates TFT with the new packet filter received from PCF.	Old QoS rule is deleted and new QoS rule is created toward UE.
Last rule with TFT **packetFilterUsage** = **true** is deleted.	SMF pushes updates TFT by deleting the current rule and adding a new rule with "**Any-Any**" filter.	
Multiple PCC rules for default flow with **packetFilterUsage**=**true**.	SMF randomly selects only one of the rules with **packetFilterUsage** IE as **true**.	SMF rejects all other rules with **packetFilterUsage** IE as **true**.
SMF is already having a PCC rule with **packetFilterUsage**=**true** and PCF sends a new rule with **packetFilterUsage**=**true**.	SMF rejects the new rule.	

Note

- SMF sends only one QoS rule for default flow with DQR (Default QoS Rule)=1 and packet filter as "**Any-Any**" or specific TFT over the N1 interface. The SMF does not send or add up the bit rates in QoS description of the PCC Rules in FBR IE. The MBR in UE should be derived from session AMBR.
- SMF does not send a CREATE_QER for the PCC rules QoS description over the N4 interface. The QER IDs in the PDRs for the PCC rules are set to the Session Rules QER IDs. SMF includes an additional QER in the PDR of the PCC rule, which contains only the gate status as enabled or disabled. The QER does not contain any MBR information.

Standards Compliance

This feature complies with the *3GPP TS 29.512 version 15.6.0; Session Management Policy Control Service; Stage 3* standard.

N7 Optimization

Table 363: Feature History

Feature Name	Release Information	Description
Minimizing SMF and PCF interactions on the N7 interface	2023.04	For the N7 optimization support, the SMF skips the N7 Update message by sending the UE IP address in the N7 Create message.

Feature Description

For the N7 optimization support, the SMF skips the N7 Update message by sending the UE IP address in the N7 Create message. After you enable this feature through the CLI command, the SMF allocates the IP address and performs the UPF selection before starting interaction with the PCF. If you have configured the SMF to select an alternate UPF that needs IP reallocation, then during the N4 failure, the SMF sends an N7 Update message after the N4 Success message to indicate the new IP address.

How it Works

Call Flows

This section describes the call flows that are associated with this feature.

- 5G Session Creation with N7 Optimization Call Flow, on page 1033
- 5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow, on page 1035

5G Session Creation with N7 Optimization Call Flow

The following call flow depicts the 5G session creation call flow with the N7 optimization enabled.

Figure 209: 5G Session Creation with N7 Optimization Call Flow

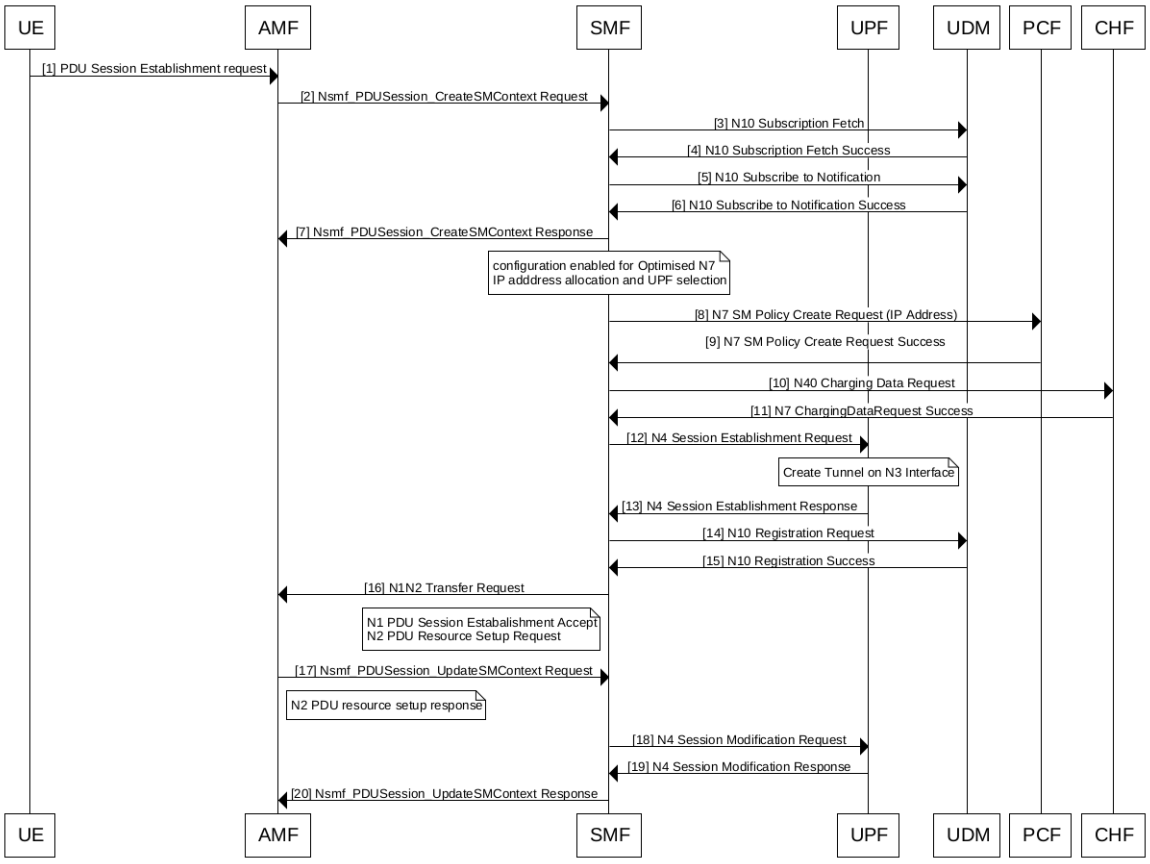


Table 364: Call Flow Description for 5G Session Creation with N7 Optimization

Step	Description
1	UE sends the PDU Session Establishment Request message to AMF.
2	AMF sends the Nsmf_PDUSession_CreateSMContext Request message to SMF.
3	SMF sends the N10 Subscription Fetch request to UDM.
4	UDM sends the N10 Subscription Fetch Success response to SMF.
5	SMF sends the N10 Subscribe to Notification message to UDM.
6	UDM sends the N10 Subscribe to Notification Success response to SMF.
7	SMF sends the Nsmf_PDUSession_CreateSMContext Response to AMF.
8	On SMF, the configuration is enabled for the optimised N7 IP adddress allocation and UPF selection. SMF sends the N7 SM Policy Create Request message along with the IP Address to PCF.
9	PCF sends the N7 SM Policy Create Request Success response to SMF.

Step	Description
10	SMF sends the N40 Charging Data Request message to CHF.
11	CHF sends the N7 Charging Data Request Success response to SMF.
12	SMF sends the N4 Session Establishment Request to UPF.
13	A tunnel is created on the N3 interface. Then, UPF sends the N4 Session Establishment Response to SMF.
14	SMF sends the N10 Registration Request message to UDM.
15	UDM sends the N10 Registration Success response to SMF.
16	SMF sends the N1N2 Transfer Request message to AMF.
17	The N1 PDU Session Establishment request is accepted and the N2 PDU Resource Setup Request is sent. AMF sends the Nsmf_PDUSession_UpdateSMContext Request message to SMF.
18	AMF sends the N2 PDU resource setup response. SMF sends the N4 Session Modification Request message to UPF.
19	UPF sends the N4 Session Modification Response to SMF.
20	SMF sends the Nsmf_PDUSession_UpdateSMContext Response to AMF.

5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow

The following call flow depicts the 5G session creation call flow during the message failure with the N7 optimization enabled.

Figure 210: 5G Session Creation During N4 Session Establishment Failure with N7 Optimization Call Flow

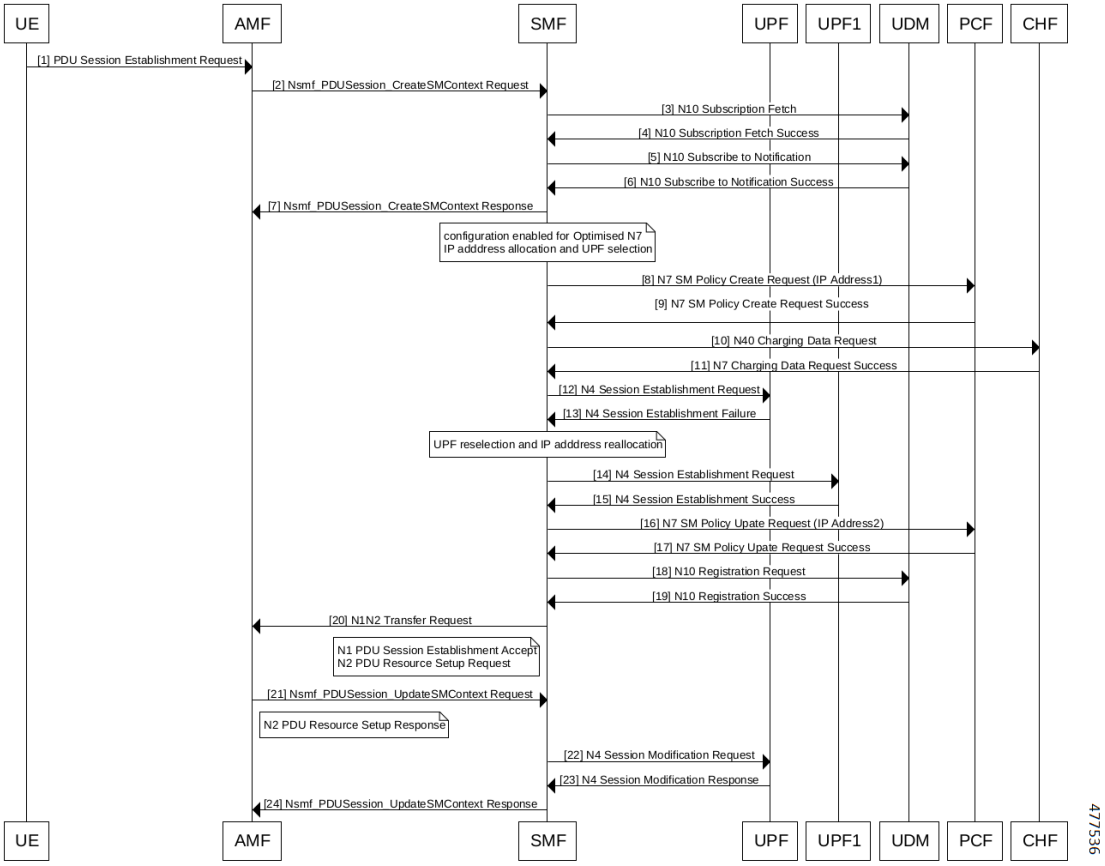


Table 365: Call Flow Description for 5G Session Creation During N4 Session Establishment Failure with N7 Optimization

Step	Description
1	UE sends the PDU Session Establishment Request message to AMF.
2	AMF sends the Nsmf_PDUSession_CreateSMContext Request message to SMF.
3	SMF sends the N10 Subscription Fetch request message to UDM.
4	UDM sends the N10 Subscription Fetch Success response to SMF.
5	SMF sends the N10 Subscribe to Notification message message to UDM.
6	UDM sends the N10 Subscribe to Notification Success response to SMF.
7	SMF sends the Nsmf_PDUSession_CreateSMContext Response to AMF.
8	On SMF, the configuration is enabled for the optimised N7 IP adddress allocation and UPF selection. SMF sends the N7 SM Policy Create Request message along with the IP Address to PCF.
9	PCF sends the N7 SM Policy Create Request Success message to SMF.

Step	Description
10	SMF sends the N40 Charging Data Request message to CHF.
11	CHF sends the N7 Charging Data Request Success message to SMF.
12	SMF sends the N4 Session Establishment Request message to UPF.
13	UPF sends the N4 Session Establishment Failure message to SMF.
14	The UPF reselection and IP adddress reallocation happens. SMF sends the N4 Session Establishment Request message to UPF1.
15	UPF1 sends the N4 Session Establishment Success message to SMF.
16	SMF sends the N7 SM Policy Upate Request, with another IP address to PCF.
17	PCF sends the N7 SM Policy Upate Request Success message to SMF.
18	SMF sends the N10 Registration Request message to UDM.
19	UDM sends the N10 Registration Success message to SMF.
20	SMF sends the N1N2 Transfer Request message to AMF.
21	The N1 PDU Session Establishment is accepted and the N2 PDU Resource Setup Request message is sent. AMF sends the Nsmf_PDUSession_UpdateSMContext Request message to SMF.
22	N2 PDU Resource Setup Response message is received. SMF sends the N4 Session Modification Request message to UPF.
23	UPF sends the N4 Session Modification Response message to SMF.
24	SMF sends the Nsmf_PDUSession_UpdateSMContext Response to AMF.

Configuring N7 Optimization

To configure the N7 optimization, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
    policy [ local | optimized ]
      rat-type [ nr | wlan | eutra ]
    end
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile name. *dnn_profile_name* must be an alphanumeric string.
- **policy [local | optimized]**: Disable or enable the interaction with PCF.
  - **local**: SMF does not interact with UPF.

Note

- This parameter is applied only during session creation and doesn't change during handover.
- If you configure **policy local**, then the configuration of PCF or PCRF is not mandatory.

- **optimized**: SMF skips the N7 update by sending the UE IP address in N7 Create message.

Note In case you configure both **policy local** and **policy optimized** together, then **policy local** takes the precendence.

- **rat-type [nr | wlan | eutra]**: This keyword is to reduce the number of messages being exchanged with PCF for the specified RAT type.

Note This keyword is optional. If **rat-type** is not configured then the **policy local** or **policy optimized** is valid for all the three RAT types, which are NR, WLAN, and EUTRA.

OAM Support

Bulk Statistics Support

The SMF maintains the following metrics as part of this feature.

- smf-service-stats

  Description: This statistics includes policy_type label to indicate the number of session setup with the optimized N7.

  Labels:

  - policy_type

- Values:
  - pcf
  - pcrf
  - local_policy
  - pcf_optimized

The smf-service-stats needs to be enabled as part of granular-labels configuration. If enabled, smf-service-stats indicates the number of session setup with the optimized N7 for the policy_type label.

To enable the smf-service-stats statistics, configure the granular-labels statistics for pcf_optimized using the following:

```
infra metrics verbose application
  metrics smf_service_stats
    granular-labels [ policy_type ]
  exit
```

Dynamic QoS Flow-based Application Detection and Control

Feature Description

To support the dedicated bearer on QCI 80 (QoS Class Identifier), SMF must support application detection and control (ADC) feature.

On receiving a PCC rule for application detection and control, with an application-Id and APP_STA/APP_STO provisioned in Policy-control-request-trigger, SMF instructs the UPF to detect the application traffic. When the application traffic is identified by an application identifier received from the UPF, SMF reports the start of the application to the PCF. Then, PCF makes the policy decisions based on the information received and installs a new dedicated PCC rule with QCI 80 to SMF.

SMF supports the following functionalities:

- Enable and disable ADC from PCF.
- Report APP_START and APP_STOP to PCF based on application traffic detection at UPF.
- Mute application detection.
- Process applications START, STOP from UPF in session report and triggering APP_STA/APP_STO toward the PCF.
- Detect application for L3, L4, and L7 rules.

Dynamic QoS Flow Based Application Detection and Control is applicable to both roaming and non-roaming scenarios.

How it Works

This section describes how Dynamic QoS Flow Based Application Detection and Control feature works.

Interface Details

PCF SMF interface – PCF enables ADC at SMF

ADC related IEs from PCF to SMF:

appId: application identifier provided by PCF within PCC-Rule.

APP_STA and APP_STO: PCF provisions these triggers in Policy control request trigger.

muteNotif : Mute Notification. PCF may mute a notification about a specific detected application by including IE in "traffContDecs" and including a "refTcData" attribute referring to the Traffic Control Data decision within the PCC rule.

Example:

```
{  'sessRules': {'SessRule-1': {…}}},
    'pccRules': {
         'PccRule-1': {…},
         'crn#rda1': {'pccRuleId': 'crn#rda1', 'appId': 'x', reftcdata:”TCD-2”}},
    'qosDecs': {'QoS-1': {…}}
    'traffContDecs':{'TCD-2':{'tcId':'TCD-2','flowStatus':'DISABLED',’muteNotif‘:true}},
    ‘policyCtrlReqTriggers’:[‘PLMN_CH’,’AC_TY_CH’,’APP_STA’,’APP_STO’] }
}
```

Important Unmuting a predefined rule is not supported.

Mute function is supported only during PolicyCreate and not during PolicyUpdate.

SMF PCF -Reporting Start or Stop Trigger to PCF

SMF sends a SMPolicyControl_Update including detected application information in "appDetectionInfo" and "APP_STA" / ”APP_STO” within the "repPolicyCtrlReqTriggers" attribute.

When UPF optimization enabled, SMF does not filter APP_STA or APP_STO trigger and it sends all APP_STA or APP_STO triggered to PCF which are triggered by UPF. UPF optimization enabled by setting environment variable UPF_ADC_OPTIMIZED = true in SMF setup.

Table 366: Definition of type AppDetectioninfo

Attribute Name	Data Type	P	Cardinality	Description
appId	String	M	1	Reference to the application detection filter configured at the UPF
InstanceId	String	O	1	Identifier dynamically assigned by SMF in order to allow correlation of the application Start and Stop events to the specific service data flow description, if service data flow descriptions are deducible.
sdfDescriptions	array(flow Information)	O	1...N	Contains the deducted service data flow descriptions if they are deducible.

Limitations

The Dynamic QoS Flow Based Application Detection and Control feature has the following limitations:

- In case both ADC start or stop and non-ADC Usage-report(vol/time threshold) come from UPF in same session-report, it is not deterministic weather first ADC report or Non-ADC report is processed. When both ADC and non-ADC report come in a session-report, smf-service pod posts two internal events ADC

event and non-ADC usage-report event. Infra creates two separate go-routines to process both events. But it is not deterministic which go-routine is going to be scheduled first, because of this limitation, some times Non-ADC usage-report is processed before ADC report or the other way around.

- When APP-Start and App-Stop event for two separate App-Id's are received from UPF in same session-report request, SMF informs both(Start and Stop) events in same SmPolicyUpdateReq to PCF. APP_STA and APP_STO are sent in repPolicyCtrlReqTriggers IE.\, this is a global IE. Since PCF has history of receiving APP_STA and APP_STO, it can link the APP_STO to the appId for which an APP_STA already received. APP_STA trigger is applicable to the appId for which PCF has not received a start indication.

Static PCC Rules Support

Feature Description

Static PCC rules are configured in the SMF. These rules can be activated immediately upon PDU session establishment. Static rule is identified by the ruledef configuration using the **action priority** CLI command.

The local configuration on SMF represents the rulebase which is sent to the UPF during session establishment. The SMF uses the configuration representing the PCC rules, QoS Desc, and Charging Data received from PCF to perform QoS flow binding. This configuration is present in the UPF as well. The SMF does not send the PDRs, QERs, and FARs, instead sends only the rulebase name in a default PDR (referred as rulebase PDR) over the N4 interface. The UPF generates the PDRs, FARs, QERs, and URRs for predefined rules based on the rulebase configuration.

Important The Static PCC Rules Support on SMF is applicable to both 4G and 5G calls.

Relationships

This feature utilizes the functionalities provided by PDU Session Lifecycle feature.

How it Works

PCF must send the rulebase name to enable the static PCC rule support on SMF.

When the PCF provides the rulebase name, the SMF performs the following steps during the PDU session creation:

1. The SMF sends Npcf_SMPolicycontrolCreate message to PCF. In response to this message, the PCF may send SMPolicyDecision with a PccRule. If the rule ID of the PccRule is in cbn# rulebase name format, the SMF assumes that the rule id is representing a rulebase name.
2. The SMF sends the rulebase name to the UPF in PFCP Session Establishment Request in a proprietary IE within Create PDR IE.

Note The SMF sends this name only in the default PDR which does not have any SDF filters. No other PDR, FAR, QER, and URR are sent to the UPF for the static rules. The UPF can derive the same from the rulebase name.

Pre-processing During Configuration

Once the Active Charging Service configuration is done (including rulebase, associated ruledefs, and charging actions), SMF processes the configured values and derives PCC Rules, QoSData, and ChargingData from the configured values. The following principles are used to create these entities:

1. QoSData:
   a. Each configured charging action results in a QoSDesc creation.
   b. The **flow-limit-bandwidth** configured under charging action provides the GBR/MBR for the QoSData.
   c. The QCI and ARP configured in charging action constitute the 5QI and ARP of the QoSData. If no QCI and ARP are configured, the 5QI and ARP of the default QoS flow are associated with this QoSData.
2. ChargingData:
   a. The **billing-action** configuration under charging action determines whether offline charging is enabled in the created ChargingData.
   b. The **cca charging credit** configuration under charging action determines whether online charging is enabled in the created ChargingData.
   c. The rating group and service ID of the ChargingData are provided by content-id and service-identifier configuration under charging action.
3. PCCRule:
   a. Each ruledef under a rulebase results in creation of a PCCRule.
   b. The **packet-filter** configured under charging action is used for the FlowInformation in the PCCRule.
   c. The QoSData and ChargingData associated with this ruledef in the rulebase configuration form the refQoS and refChg for this PCCRule.

All the created PCCRules, QoSData, and ChargingData are saved per rulebase.

During PDU Session Creation

1. During PDU session creation, PCF sends the rulebase name (value configured under upf-apn is selected if the PCF does not send it) as PCCRule with ID set to cbn# configured rulebase name. It may also send any predefined rule to be activated as another PCCRule with ID set to crn# configured ruledef name. All such PCC rules will have only the RuleId attribute present.
2. On receiving such a request, SMF selects the constructed PCCRules, QoSData, and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On the N4 interface, the SMF sends the rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase".

4. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
5. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create the corresponding QER and URR.
6. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
7. For all static and activated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
8. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

During PDU Session Modification

1. During PDU session modification, PCF sends the rulebase name as PCCRule with ID set to cbn#configured rulebase name. In case of predefined rule PCF can activate new rule crn#configured ruledef name or delete the existing rule (crn#"nil"). All such PCC Rules will have only the RuleId attribute present.
2. On receiving new rule addition request, SMF selects the constructed PCCRules, QoSData and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On receiving an existing rule deletion request, if the SMF received a ruledef name with nil value or a rulebase name different from the existing one, the SMF deletes the QoS flows which correspond to previous rulebase name or ruledef in QoSModel.
4. On N4 interface, SMF sends the new rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase" and RemovePDR with PDR ID which correspond to the old rulebase name.
5. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
6. For all deactivated predefined rules, SMF sends RemovePDR with PDR ID which corresponds to the predefined rule.
7. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create or delete the corresponding QER and URR.
8. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
9. For all static and activated/deactivated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
10. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated/deactivated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

Configuring the Static PCC Rules

This section describes how to configure the Static PCC Rules on SMF.

The configuration for static and predefined rules is based on the ECS configuration of the StarOS based PGW-C. This is to ensure that the UPF can work seamlessly with the SMF.

Make sure to first configure the Active Charging Service (ACS) before proceeding with the static PCC rules configuration. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

Note You can configure only one active charging service per system.

Configuring the Static PCC Rules Support involves the following steps:

1. Configuring Charging Action, on page 1044
2. Configuring Packet Filter, on page 1046
3. Configuring ACS Ruledef, on page 1047
4. Configuring ACS Group of Ruledefs, on page 1048
5. Configuring Rulebase and Predefined Rule Prefix, on page 1049
6. Configuring ACS Rulebase in ACS Configuration Mode, on page 1051
7. Configuring URR ID, on page 1050
8. Configuring GTPP Group, on page 1050
9. Configuring APN, on page 1050
10. Associating GTPP Group with APN, on page 1051
11. Configuring ACS Rulebase in APN Configuration Mode, on page 1049
12. Defining UPF APN Profile in DNN Profile Configuration, on page 1053
13. Configuring QoS Parameters, on page 1027

Configuring Charging Action

This section describes how to configure charging action. The charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, and so on. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3, L4, L7, and so on).

To define the QoS and charging related parameters associated with ruledefs, use the following sample configuration.

```
config
   active-charging service service_name
     charging-action charging_action
       allocation-retention-priority priority  [ pci pci_value
```

```
| pvi pvi_value billing-action egcdr cca
charging credit [ rating-group coupon_ id
] [ preemptively-request ]
content-id content_id
flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action
{ discard | lower-ip-precedence } [ committed-data-rate
bps committed-burst-size bytes
[ exceed-action { discard | lower-ip-precedence
} ] ] } | { id id } }
nexthop-forwarding-address ipv4_address/ipv6_address
qos-class-identifier qos_class_identifier
service-identifier service_id
tft packet-filter packet_filter_name
tft-notify-ue
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32
| af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value
} [ downlink | uplink ]
end
```

NOTES:

- **charging-action** *charging_action_name*: Specify the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
- If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
- **allocation-retention-priority** *priority* **[pci***pci_value* **| pvi** *pvi_value* : Configures the Allocation Retention Priority (ARP). *priority* must be an integer value in the range of 1-15.
  - **pci** *pci_value* : Specify the Preemption Capability Indication (PCI) value. The options are:
    - MAY_PREEMPT—Flow can be preempted. This is the default value.
    - NOT_PREEMPT—Flow cannot be preempted.
  - **pvi** *pvi_value*: Specify the Preemption Vulnerability Indication (PVI) value. The options are:
    - NOT_PREEMPTABLE—Flow cannot be preempted. This is the default value.
    - PREEMPTABLE—Flow can be preempted.
- **billing-action**: Configure the billing action for packets that match specific rule definitions.
- **cca charging credit**: Enable or disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.
- **content-id**: Configure the rating group.

- **flow action**: Specify the action to take on packets that match rule definitions.
- **flow limit-for-bandwidth**: Configure the QoS parameters, such as MBR and GBR.
  - peakdatarate(MBR): Default is 3000 bps
  - peakburstsize: Default is 3000 bytes
  - committedDataRate(GBR): Default is 144000 bps
  - committedBurstSize: Default is 3000 bytes
- **nexthop-forwarding-address** *ipv4_address/ipv6_address*: Configure the nexthop forwarding address.
- **qos-class-identifier** *qos_class_identifier*: Configure the QoS Class Identifier (QCI) for a charging action. *qos_class_identifier* must be an integer in the range of 1–9 or from 128–254 (operator specific).
- **service_identifier** *service_id*: Configure the service identifier to use in generated billing records. *service_id* must be an integer in the range of 1–2147483647.
- **tft packet-filter** *packet_filter_name*: Specify the packet filter to add or remove from the current charging action. *packet_filter_name* must be an alphanumeric string of 1 to 63 characters.
- **tft-notify-ue**: Control the TFT updates towards the UE based on certain trigger conditions.
- **tos**: Configure the Type of Service (ToS) octets.

Configuring Packet Filter

To configure the packet filter, use the following sample configuration.

```
config
  active-charging service service_name
    packet-filter packet_filter_name
      direction { bi-directional | downlink | uplink }
      ip local-port { = port_number | range start_port_number to
      end_port_number }
      ip protocol = protocol_number
      ip remote-port { = port_number | range start_port_number to
      end_port_number }
      ip tos-traffic-class = { type-of-service | traffic class }
      mask { = mask-value}
      priority priority
      end
```

NOTES:

- **packet-filter** *packet_filter_name*: Configure the packet filters to be sent to UE. *packet_filter_name* must be an alphanumeric string of 1 to 15 characters.
- **direction { bi-directional | downlink | uplink }**: Configure the direction in which the packet filter has to be applied. The default value is **bi-directional**.
- **ip local-port**: Configure the IP 5-tuple local port(s) for the current packet filter.
- **ip protocol**: Configure the IP protocol(s) for the current packet filter.
- **ip remote-address**: Configure the IP remote address(es) for the current packet filter.

- **ip remote-port**: Configure the IP remote port(s) for the current packet filter.
- **ip tos-traffic-class**: Configure the Type of Service (TOS)/Traffic class under charging action in the Packet filter mode.
- **priority** *priority*: Configure the priority of the current packet filter.

Configuring ACS Ruledef

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

To create, configure, or delete ACS rule definitions, use the following sample configuration.

```
config
  active-charging service service_name
    ruledef ruledef_name
      ip any-match [ = | != ] [ TRUE | FALSE ]
      ip dst-address { operator { { ipv4_address | ipv6_address
      } | { ipv4_address/mask | ipv6_address/mask} |
      address-group ipv6_address } | { !range | range }

      rule-application { charging | post-processing | routing }
      end
```

NOTES:

- **ruledef** *ruledef_name*: Specify the ruledef to add, configure, or delete. *ruledef_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
- If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
- If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef. The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).
- **ip any-match [= | !=] [TRUE | FALSE**: Define the rule expressions to match IPv4/IPv6 packets. The *operator* and *condition* in the command specifies the following:
  - *operator*
    - !=: Does not equal
    - < =: Equals
  - *condition*
    - FALSE
    - TRUE
- **ip dst-address {** *operator* **{ {** *ipv4_address* | *ipv6_address* **} | {** *ipv4_address/mask* |*ipv6_address/mask* **} | address-group** *ipv6_address* **} | { !range | range } host-pool** *host_pool_name* **}**: Define rule expressions to match IP destination address field within IP headers.

- *ipv4_address | ipv6_address*: Specify the IP address of the destination node for outgoing traffic. *ipv4_address | ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- *ipv4_address/mask | ipv6_address/mask*: Specify the IP address of the destination node for outgoing traffic. *ipv4_address/mask | ipv6_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.
- *address-group ipv6_address*: Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within a given IPv6 address.
- The *operator* in the command specifies the following:
  - !=: Does not equal
  - <: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **multi-line-or all-lines**: Allow a single ruledef to specify multiple URL expressions. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.
- **rule-application { charging | post-processing | routing }**: Specify the rule application for a rule definition.
  - **charging**: Specify that the current ruledef is for charging purposes.
  - **post-processing**: Specify that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
  - **routing**: Specify that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled.

Configuring ACS Group of Ruledefs

A group-of-ruledefs can contain optimizable ruledefs. Ruledef group optimization depends on the optimization ability of ruledefs in the group-of-ruledefs, and the optimization configuration of the group in a rulebase.

Upon adding a new ruledef, the following checks occur:

- Determines if the new ruledef is part of any existing group of ruledefs
- Identifies if the new ruledef requires optimization

To combine a set of ruledefs together to apply the same charging action on them, use the following sample configuration.

```
config
  active-charging service service_name
    group-of-ruledefs ruledef_group_name
```

```
add-ruledef priority ruledef_priority ruledef ruledef_name
exit
```

NOTES:

- **group-of-ruledefs** *ruledef_group_name* : Specify the ruledef group name to add, configure, or delete. This command allows up to a maximum of 128 group of ruledef configurations.
- **add-ruledef**: This command allows you to add or remove ruledefs from a group-of-ruledefs. This command allows up to a maximum of 128 ruledef configurations.
- **priority**: Specify the priority of the ruledef in the current group of ruledefs. *ruledef_priority* must be an integer in the range of 1–10000.
- **ruledef** *ruledef_name*: Specify the name of the ruledef to add to the current group-of-ruledefs. *ruledef_name* must be an alphanumeric string of 1 to 63 characters.

Configuring Rulebase and Predefined Rule Prefix

Rulebase and predefined rule prefix configuration is mandatory for static rule installation from PCF. The SMF supports the predefined rule installation with prefix and without prefix. The SMF also supports the group-of-ruledef installation for both predefined and static rules.

To configure the rulebase prefix and predefined rule prefix, use the following sample configuration.

```
config
  profile network-element pcf pcf_service_name
    predefined-rule-prefix predef_rule_prefix
    rulebase-prefix rulebase_prefix
    end
```

NOTES:

- **predefined-rule-prefix** *predef_rule_prefix*: Specify the predefined rule prefix to be added. For example, the prefix for predefined rule is **cbr**.
- This is an optional configuration for the predefined rule. When there is no prefix defined within the PCF network element profile, the predefined rule application behaves as defined in the *3GPP TS 29.244* specification.
- **rulebase-prefix** *rulebase_prefix*: Specify the rulebase prefix to be added. For example, the prefix for rulebase is **rbn**. This is a mandatory configuration for the static rule.

Configuring ACS Rulebase in APN Configuration Mode

To enable and configure an ACS rulebase to be used for subscribers who use the configured APN, use the following sample configuration.

```
config
  apn apn_name
    active-charging rulebase rulebase_name
    end
```

NOTES:

- **active-charging rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.

Configuring URR ID

This section describes how to configure the Usage Reporting Rules (URR) ID for the rating and service groups.

```
config
   active-charging service service_name
      urr-list list_name
         rating-group rating_id service-identifier service_id_value
         urr-id urr_id_value
         end
```

NOTES:

- **urr-list** *list_name*: Specify the name of the URR list. *list_name* must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *rating_id*: Specify the rating ID used in charging. *rating_id* must be an integer in the range of 0–2147483647.
- **service-identifier** *service_id_value*: Configure the service identifier value. *service_id_value* must be an integer in the range of 0–2147483647.
- **urr-id** *urr_id_value*: Configure URR identifier for rating/service group. *urr_id_value* must be an integer in the range of 1–8388607.
- The URR ID configuration is per rating group and service ID. For different rating group and service ID combinations, use the URR ID configuration as many times as needed.

Configuring GTPP Group

To configure the GTPP group, use the following sample configuration.

```
config
   gtpp group group_name
      gtpp trigger { time-limit | volume-limit }
      end
```

NOTES:

- **gtpp group** *group_name*: Specify the GTPP group name. *group_name* must be an alphanumeric string of 1 to 63 characters.
- **gtpp trigger { time-limit | volume-limit }**: Configure triggers for the CDR.
  - **time-limit**: Enable time-limit trigger for the CDR.
  - **volume-limit**: Enable volume-limit trigger for the CDR.

Configuring APN

This section describes how to create Access Point Name (APN) templates. This APN configuration represents the access point configuration in the UPF and further facilitates configuring a rulebase name within.

To configure the APN, use the following sample configuration.

```
config
   apn apn_name
   end
```

NOTES:

- **apn** *apn_name*: Specify a name for the APN template as an alphanumeric string of 1 to 62 characters. The name is case insensitive.

Associating GTPP Group with APN

To associate the GTTP group with the configured APN, use the following sample configuration.

```
config
   apn apn_name
      gtpp group group_name
      end
```

NOTES:

- **gtpp group** *group_name*: Associate the defined GTPP group with the already configured APN.

Configuring ACS Rulebase in ACS Configuration Mode

This section describes how to create, configure, or delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Rulebase configuration is the one that combines all the specified configurations together to construct the static and predefined PCC rules.

To configure the ACS rulebase, use the following sample configuration.

```
config
   active-charging service service_name
      rulebase rulebase_name
         action priority action_priority { [ dynamic-only ]
         | static-and-dynamic | timedef timedef_name ]
         { group-of-ruledefs ruledefs_group_name |
         ruledef ruledef_name } charging-action charging_action_name
         [ monitoring-key monitoring_key ] [ description description ] }
         cca quota { holding-time holding_time content-id content_id
         | retry-time retry_time [ max-retries retries ] }
         cca quota time-duration algorithm { consumed-time seconds
         [ plus-idle ] | continuous-time-periods seconds |
         parking-meter seconds} [ content-id content_id]
         credit-control-group cc_group_name
         dynamic-rule order { always-first | first-if-tied }
         egcdr threshold { interval interval
         [ regardless-of-other-triggers ] | volume { downlink | total |
         uplink } bytes }
         route priority route_priority ruledef ruledef_name
         analyzer { dns | file-transfer | ftp-control | ftp-data | h323
         | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp
        | rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced
```

```
]
| smtp | tftp | wsp-connection-less | wsp-connection-oriented }
[ description description ]
tcp check-window-size
tcp mss tcp_mss { add-if-not-present | limit-if-present }
tcp packets-out-of-order { timeout timeout_duration|
transmit [ after-reordering | immediately ] }
end
```

NOTES:

- **rulebase** *rulebase_name*: Specify the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.
- **action priority** *action_priority* **{ [dynamic-only] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**: Configure the priority order in which ruledefs are matched and the associated charging action.
  - *priority* must be an integer in the range of 1–65535.
  - *monitoring_key* must be an integer in the range of 100000–4000000000.

  Use the **no action priority** *action_priority* command to remove the configured ruledef, group-of-ruledefs, and charging action.

Important Currently, the SMF does not support individual removal of ruledef, group-of-ruledefs, and charging action.

- **cca quota { holding-time** *holding_time* **content-id** *content_id* **| retry-time** *retry_time* **[max-retries** *retries* **] }**: Configure the quota for online charging.
  - *holding_time* must be an integer in the range of 1–4000000000
  - *content_id* must be an integer in the range of 1–2147483647
  - *retry_time* must be an integer in the range of 0–86400
  - *retries* must be an integer in the range of 1–65535
- **cca quota time-duration algorithm { consumed-time** *consumed_time* **[plus-idle] | continuous-time-periods** *continuous_time* **| parking-meter** *parking_meter* **} [content-id** *content_id* **]**
  - *consumed_time* must be an integer in the range of 1–4294967295 seconds
  - *content-id* must be an integer in the range of 1–2147483647
  - *continuous_time* must be an integer in the range of 1–4294967295 seconds
  - *parking_meter* must be an integer in the range of 1–4294967295 seconds
- **credit-control-group** *cc_group_name*: Configure the online charging parameters used by this rulebase. *cc_group_name* must be an alphanumeric string of 1 to 63 characters.

- **dynamic-rule order**: Configure the order of dynamic rule matching against the static rules in a rulebase.
- **egcdr threshold { interval** *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink } bytes }**: Configure the threshold for offline charging.
  - *interval* must be an integer in the range of 60–40000000.
  - **downlink** must be an integer in the range of 100000–4000000000. Default: 4000000000.
  - **uplink** must be an integer in the range of 100000–4000000000. Default: 4000000000.
  - **total** must be an integer in the range of 100000–4000000000.
- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**: This command is used only on UPF.
  - *route_priority* must be an integer in the range of 0–65535.
  - *ruledef_name* must be an alphanumeric string of 1 to 63 characters.
- **tcp check-window-size**: This command is used only on UPF.
- **tcp mss** *tcp_mss*: This command is used only on UPF. *tcp_mss* must be an integer in the range of 496–65535.
- **tcp packets-out-of-order { timeout** *timeout_duration* **| transmit [after-reordering | immediately] }**: This command is used only on UPF.
  - *timeout_duration* must be an integer in the range of 100–30000. Default value is 5000.

Defining UPF APN Profile in DNN Profile Configuration

To configure the UPF APN profile in the existing DNN profile, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    upf apn apn_name
    end
```

NOTES:

- **upf apn** *apn_name*: Enable UPF APN profile configuration. This profile is configured under the existing DNN profile configuration. *apn_name* must be an alphanumeric string of 1 to 62 characters.

Configuring QoS Parameters

To configure the QoS parameters, use the following sample configuration.

```
config
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
    arp { preempt-cap preemption_capability |
    preempt-vuln preemption_vulnerability |
    priority-level priority_level }
```

```
max data-burst burst_volume
priority qos_priority
qi5 5qi_value
exit
```

NOTES:

- **ambr { ul** *uplink_ambr* **| dl** *downlink_ambr* **}**: Define the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption_capability*: Specify the preemption capability flag. The options are:
  - MAY_PREEMPT—Bearer may be preempted
  - NOT_PREEMPT—Bearer cannot be preempted
- **arp preempt-vuln** *preemption_vulnerability*: Specify the preemption vulnerability flag. The options are:
  - PREEMPTABLE—Bearer may be preempted
  - NOT_PREEMPTABLE—Bearer cannot be preempted
- **arp priority-level** *priority_level*: Define the Allocation and Retention Priority (ARP) for the service data. The default value of *priority_level* is 8.
- **max data-burst** *burst_volume*: Define the maximum data burst volume. *burst_volume* must be an integer in the range of 1–4095.
- **priority** *qos_priority*: Specify the 5QI priority level. *qos_priority* must be an integer in the range of 1–127.
- **qi5** *5qi_value*: Specify the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi_value* must be an integer in the range of 0–255.

Verifying the Static PCC Rules Support Feature Configuration

This section describes how to verify the Static PCC Rules Support configuration.

To verify the feature configuration details, use the following command.

show full-configuration

The following is an example of this show command output.

```
active-charging service acs
charging-action ca1
  arp priority-level 15 preempt-cap MAY_PREEMPT preempt-vuln PREEMPTABLE
  cca charging credit preemptively-request
  content-id 320001
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 1000000
 violate-action discard committedDataRate 2000000 committed-burst-size 2000000 exceed-action
 lower-ip-precedence
  nexthop-forwarding-address fa00:965a:c263:25::16/128
  qos-class-identifier 9
  service-identifier 32000
  tft packet-filter pf1
  tft-notify-ue
  tos af11 downlink
rulebase rb1
```

```
  cca quota time-duration algorithm parking-meter 1000 content-id 18000
  credit-control-group cg1
  dynamic-rule order first-if-tied
  egcdr threshold volume total 400000
  tcp packets-out-of-order transmit immediately
  action priority 95 timedef ruledef rd6 charging-action ca6 description ruledef
  action priority 96 ruledef rd3 charging-action ca5
  action priority 97 group-of-ruledefs grd3 charging-action ca4 monitoring-key 200000
  action priority 98 static-and-dynamic group-of-ruledefs grd2 charging-action ca2
  action priority 99 dynamic-only ruledef rd1 charging-action ca1 monitoring-key 100000
  action priority 100 dynamic-only group-of-ruledefs grd1 charging-action ca1 monitoring-key
 100000 description gruledefs
  route priority 1 ruledef rd1 analyzer dns description dns
exit
packet-filter pk1
  direction uplink
  ip local-port = 23
  ip protocol = 23
  ip remote-address = 209.165.201.0/27
  ip remote-port = 23
  ip tos-traffic-class = 23 mask = 10
  priority  4
exit
ruledef prepaidBgl
  multi-line-or all-lines
  rule-application charging
  ip any-match = TRUE
  ip server-ip-address range host-pool 12
  ip dst-address = 209.165.201.10
exit
urr-list urrlocal
  rating-group 1 service-identifier 1 urr-id 2
  rating-group 1 service-identifier 3 urr-id 2
exit
exit
```

To verify the group-of-ruledefs configuration details, use the following command.

show running-config

The following is an example of this show command output.

```
show running-config
profile network-element pcf pcf1
rulebase-prefix   rbn
predefined-rule-prefix cbr
!
active-charging service acs1
group-of-ruledefs IPV6-whtlst-https_2300
  add-ruledef priority 1 ruledef IPV6-whtlst-https_2300_01
  add-ruledef priority 2 ruledef IPV6-whtlst-https_2300_02
  add-ruledef priority 3 ruledef IPV6-whtlst-https_2300_03
  add-ruledef priority 4 ruledef IPV6-whtlst-https_2300_04
  add-ruledef priority 5 ruledef IPV6-whtlst-https_2300_05
  add-ruledef priority 6 ruledef IPV6-whtlst-https_2300_06
  add-ruledef priority 7 ruledef IPV6-whtlst-https_2300_07
  add-ruledef priority 8 ruledef IPV6-whtlst-https_2300_08
  add-ruledef priority 9 ruledef IPV6-whtlst-https_2300_09
  add-ruledef priority 10 ruledef IPV6-whtlst-https_2300_10
  add-ruledef priority 11 ruledef IPV6-2dns-whtlst-https_2300_01
  add-ruledef priority 12 ruledef IPV6-2dns-whtlst-https_2300_02
  add-ruledef priority 13 ruledef IPV6-2dns-whtlst-https_2300_03
exit
group-of-ruledefs rdg1
```

```
  add-ruledef priority 10 ruledef rd2
  add-ruledef priority 12 ruledef rd1
exit
exit
```

Predefined PCC Rules

Feature Description

Most of the concepts applicable for static rules also apply for predefined rules. The configuration set, mechanism for QoS binding and pre-constructed QoS model remain the same.

Important Predefined PCC Rules are applicable to both 4G and 5G calls.

Predefined Rules vs Static Rules

This section lists the differences between the predefined and static rules.

- Predefined rule is identified by the **dynamic-only** keyword in the action priority associated with a ruledef under rulebase configuration.
- Predefined rules are not activated automatically but are enabled or disabled by PCF on a per rule basis. The PCF sends a PCC rule with the ruledef name alone or ruledef and rulebase names together as the rule ID to activate the predefined rule and sends the PCC rule map with null entry for the ruledef previously activated to deactivate a predefined rule.
- The QoS binding and modelling is not done for predefined rules at the time of configuration unlike the static rule. Instead during PDU session activation/modification the ECS configuration of activated ruledefs are considered to create or change the QoS model applicable for the session.
- On N4 interface, one PDR and corresponding FAR per ruledef activated by the PCF is sent to the UPF with ruledef name in the Activate predefined Rule IE and rulebase name is sent in Rulebase IE in default PDR. On rule removal, the corresponding PDR is removed.

Note The PCF sends the predefined rules, and activates these rules only if the UPF APN is configured with "rulebase" name. Otherwise, the PCF must send the rule name along with the "rulebase" name.

Combined Application of Static, Predefined, and Dynamic Rules

All three static, predefined, and dynamic rules can coexist for a session. In such a case:

- Pre-constructed QoS model is prepared only for static rules. During PDU session activation/modification, any dynamic and predefined rules are evaluated to modify the QoS model and accordingly modifications are done on N1, N2, and N4 interfaces.
- If the rating-group and service ID for a dynamic rule are the same as that of a configured predefined and static rule, then the URR ID for the static and predefined rule is retained even for the dynamic rule.

Bearer QCI Support

Feature Description

The User Plane function (UPF) requires the Bearer level information (BLI) for each QoS flow like QFI for 5G and Bearer Id for 4G, 5G QoS Identifier (5QI) allocation and retention priority (ARP), and Charging ID, to support inline services. The Bearer QCI Support feature facilitates this requirement with the SMF.

Note The Bearer QCI Support feature also includes support for Bli_ID and QFI values in the "Create PDR" message.

The SMF sends the Bearer QoS Class Identifier (QCI) Information Element (IE), which is cisco proprietary IE, in the PFCP session establishment request and PFCP session modification request. The UPF implicitly derives the deletion indication. If a BLI ID is no longer associated with any PDR, the UPF removes it from the PFCP session context. The UPF adds the 5QI or QCI value in the EDR. Currently, the Bearer QCI field is used for 5G to add the 5QI.

The BLI is reported to the UPF as shown in the following table. The formats and encoding and decoding of these IEs are the same as other 3GPP IEs as described in *TS 29.244*.

Information Elements	**Mandatory or Optional**	**Data Type**	**Description**
valid		guint8	Validity of the Bearer level information IE
bli_id	Mandatory	PfcpBliId	QoS flow identifier (QFI) of 5G or Bearer ID (4G)
qci	Optional	PfcpQci	Used by PGW-C, not relevant for SMF
_5qi	Optional	Pfcp5qi	5QI associated with the QoS flow
arp	Mandatory	PfcpArp	ARP comprises of pre-emption capability, Pre-emption vulnerability, and priority level.
charging_id	Optional	PfcpChargingId	Charging ID associated with the QoS flow or Bearer (or both).

Bearer Level Information ID

The unique ID for each Bearer level information sent from SMF. The recommended value of this IE is QFI (in 5G) or Bearer-id (in 4G). The format of IE is as below:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 232 (decimal)							
3 to 4	Length = 1							
5	BLI_ID value							
6 to n+4	These octets are present only if explicitly specified							

QCI: This is not applicable for 5G. It is used in CUPS, if required.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 233 (decimal)							
3 to 4	Length = 1							
5	QCI value							
6 to n+4	These octets are present only if explicitly specified							

5QI: The SMF uses this IE to send the 5QI value.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 234 (decimal)							
3 to 4	Length = 1							
5	5QI value							
6 to n+4	These octets are present only if explicitly specified							

ARP: The ARP value is sent with this IE.

Note From SMF, the ARP value is encoded as arp->pci)<<4) | arp->pl)<<2)| arp->pvi)

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 235 (decimal)							
3 to 4	Length = 1							
5	ARP value							

6 to n+4	These octets are present only if explicitly specified

Charging ID: The Charging IE is sent with this IE.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 236 (decimal)							
3 to 4	Length = 1							
5	Charging Id value							
6 to n+4	These octets are present only if explicitly specified							

Triggers for Bearer Level Information IE

The following are the triggers for sending the BLI IE in PFCP messages:

PFCP Session Establishment Message

The Bearer level information IE is sent for each new QoS flow with the unique QFI ID. This IE is added in the policy decision in the N7 Policy Control Create Response message from the PCF. Therefore, SMF sends multiple instances of this IE, in a single PFCP message.

PFCP Session Modification Message:

Any new QoS flow addition or new PCC rule referring to an existing QoS flow that results in a new QER or PDR IE that has a new Bearer level information IE for each unique QFI ID.

The BLI IE is not included in the PFCP Session Modification Message if the modification is for IDFT tunnels.

Non-standard QCI Support for Dynamic PCC and Session Rules

Feature Description

The SMF supports non-standard QCI values in dynamic PCC and session rules along with the standard QCI values.

Non-standard QCIs are the values from 1 through 255 and that are not part of standard QCI values as defined in section 6.1.7.2 of 3GPP 23.203 specification.

The SMF supports non-standard QCI for DSCP marking of the data packets for the session.

Important SMF does not support CLI-based configuration of non-standard QCI values for static and predefined rules. When the PCF sends the session rule with a non-standard QCI, then the SMF reserves the non-standard QCI value for the static and predefined rules that belong to the default flow.

How it Works

The SMF receives the non-standard and standard QCIs in QoS from PCF through SmPolicyCreateResponse, SmPolicyUpdateResponse, or SmPolicyUpdateNotify message.

If the PCF does not send the session rule information or if the PCF sends an invalid QCI value, the SMF uses the UDM-provided non-standard QCI value and processes the QCI information in the same manner as sent by PCF. If neither PCF nor UDM sends the non-standard QCI information, the SMF uses the QCI information locally configured within QoS profile. For configuration details, see the Configuring QoS Parameters, on page 1027 section.

When the PCF sends a PCC rule with a non-standard QCI, the SMF creates a GBR flow if the (UL and DL) GBR QoS information is available in the associated QoS-Descriptor. Otherwise, the SMF creates a non-GBR flow.

For the default session rule, the SMF assumes it as a non-GBR flow irrespective of the non-standard QCI information it receives from PCF.

The SMF initiates the session establishment or modification procedure towards RAN or UE, and communicates the same QCI information on N1, N2, N4, and S5 interfaces.

Note The SMF does not handle the QoS Characteristics sent by PCF for a non-standard QCI.

If a discrepancy or an ambiguity arises in the QCI input from PCF, the SMF performs the following validations:

- The SMF checks if the QCI value is ranging from 1 through 255. The SMF does not handle any non-standard QCI value that does not fall within the specified range.
- When the PCF sends session rule and PCC rule with the same binding parameters and non-standard QCI along with GBR UL and DL information as shown in the following example, the SMF rejects the “PccRule1” PCC rule.

```
sessRule1=>AuthDefQos{arp1, qci128}+ authSessAmbr{UL=20mbps,DL=20mbps}

PccRule1=>QosDesc{arp1, qci128, gbrUL=10mbps, gbrDL=10mbps}
```

Limitations

The Non-standard QCI Support feature has the following limitations:

- The SMF assumes session rule flow as non-GBR flow for a non-standard QCI.
- The SMF does not handle the QoS Characteristics sent by PCF for a non-standard QCI.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF uses the existing policy statistics for non-standard QCIs. The QCI label which displays standard QCI value displays the non-standard QCI value too.

Troubleshooting Information

To view the flow information associated with the non-standard QCI values, use the same **show subscriber 5qi** CLI command as used for the standard QCI values.

Use the existing **clear subscriber 5qi** CLI command to delete the flows with non-standard QCI values as well.

Support for Configuring the Bandwidth ID

Feature Description

The SMF expects the user to configure the bandwidth limitation, for both downlink and uplink packets, in all charging actions, even if the bandwidth limitation configuration is the same for all the charging actions.

To optimise these configurations, the SMF allows the user to define a bandwidth ID to include all bandwidth related configurations and associate the bandwidth ID under the charging actions.

If the bandwidth value is changed, the new subscribers use the configured bandwidth values while the existing subscribers continue to use the old values.

Limitations

The SMF imposes the following limitations related to the configuration of bandwidth-policy.

- Allows up to 64 k flow ID configurations within the bandwidth-policy
- Allows configuring up to a maximum of 64 bandwidth policies
- The maximum number of groups that can be configured per bandwidth policy is 1000.
- The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

Configuring Bandwidth ID

To define the bandwidth ID within the charging action, use the following sample configuration.

```
config
  active-charging service service_name
    bandwidth-policy policy_name
    flow limit-for-bandwidth id bandwidth_id group-id group_id
    group-id group_id direction { downlink | uplink }
    peak-data-rate peak_data_rate peak-burst-size
    peak_burst_size violate-action { discard | lower-ip-precedence }
    [ committed-data-rate committed_data_rate committed-burst-size
    committed_burst_size [ exceed-action { discard | lower-ip-precedence
    } ] ]
    exit
  active-charging service service_name
  charging-action charging_action_name
```

```
flow limit-for-bandwidth bandwidth_id
end
```

- **bandwidth-policy** *policy_name*: Specify the name of the bandwidth policy. This CLI option allows configuring up to a maximum of 64 bandwidth policies.
- **flow limit-for-bandwidth id** *bandwidth_id*: Define a bandwidth ID to include all the bandwidth related configurations within the charging action for predefined and static rules.

  bandwidth_id must be an integer in the range of 1–65535.

Note The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

- If the bandwidth ID is configured and the individual uplink and downlink limit-for-bandwidth are also configured in the charging actions, then the bandwidth ID configuration takes the precedence.
- **group-id** *group_id*: Specify the group ID. *group_id* must be an integer in the range of 1– 65535.

  The group ID identifies the QoS parameters, such as MBR and GBR. Each group ID is mapped to a particular bandwidth ID.
- The maximum number of groups that can be configured per bandwidth policy is 1000.

Verifying Bandwidth ID Configuration

To verify the bandwidth ID configuration, use the following show command:

```
show config
```

This show command helps in identifying any invalid configurations such as the configured bandwidth ID being removed but still defined in the charging action. For such invalid configurations, this show command displays appropriate errors as shown in the following example output:

```
ERROR COMPONENT      ERROR DESCRIPTION
-------------------------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

Generating UE Camping Report for PCF

Feature Description

PCF needs to be aware of UE location, RAT type, access type, and other details to provision relevant policies during the PDU session life cycle. To facilitate this, during PCF initiated policy update procedure, the SMF sends "UeCampingRep" attribute in the response message based on the triggers enabled by PCF.

The SMF sends the UeCampingRep to PCF as per the Table 5.5.2.2-2 defined in 3GPP specification 29.512. When validation of all the PCF provided rules succeed, the SMF sends the UeCampingRep in the update response message to the PCF.

If validation of any of the rules fail, then the SMF sends the ueCampingRep in “PartialSuccessReport” as defined in 4.2.3.2 section of 3GPP specification 29.512.

The fields in the "UeCampingRep" IE are populated based on the following triggers set by PCF.

- Access type (AC_TY_CH)
- RAT change (RAT_TY_CH)
- User location change (SAREA_CH)
- PLMN Change (PLMN_CH)

The SMF supports the following attributes:

- accessType
- ratType
- servingNetwork
- userLocationInfo

Important The SMF currently does not support the ueTimeZone attribute.

UPF Node Selection

The UPF Selection feature enables the 5GS and EPS core networks to select an UPF for reduced latency on user plane and priority-based serviceability.

The SMF selects an appropriate UPF during the setup of a PDU session. The UPF selection depends on the following query parameters:

- DNN
- Subscriber location
- Network slice information

- PDU session type
- PDU subscription type
- Priority
- Load
- Dual Connectivity with New Radio (DCNR)

When multiple UPFs meet the UPF selection criteria, UPF selection is based on priority and load. For the load metric information, the SMF fetches the Packet Forwarding Control Protocol (PFCP) IE from UPF over N4 interface. If the failure handling support exists and N4 Session Establishment fails, the SMF selects the next least-loaded UPF.

The network operator leverages this functionality for efficient handling of the user plane traffic based on priority, PDU session type, and so on. This functionality is also used for effective load balancing of the user plane connections across multiple UPFs.

In scenarios where multiple UPFs are available for a particular Subscription Permanent Identifier (SUPI), SMF provides the capability to configure multiple UP addresses for each SUPI. The SMF performs UPF selection for a particular PDU session based on the SUPI preferred configuration. For configuration details, see the Configuring UPF Address, on page 1077 section.

That is, the SMF checks if any of the configured SUPI values match the current SUPI. If the match is successful, SMF uses information on the available user plane nodes and checks if the IP address matches with any of the values configured for the SUPI. The SMF performs the following validations for UPF selection:

- Check if the UP node is valid and active
- Check if the location-based DNN or the DNN received from service is available in the list of supported DNNs in UP node
- Check if the PDU session type is supported for the configured user plane. For this validation, SMF fetches the UP profile name and UPF group configured within network profile UPF. Then, SMF checks if the UPF group is empty or if the group has the PDU session type that is available in the supported PDU session types.

When all the validations are successful, the SMF skips the existing UPF selection logic involving the query parameters and uses the UPF selected by SUPI. In cases where UPF address is not configured for the SUPI or if the preceding validation checks fail, the SMF uses the default UPF selection mechanism. For co-located UPF selection, the cnSGW-C configuration remains the same as on the SMF.

UPF Selection Based on Query Parameters

This section describes how the SMF selects the UPF based on certain selection parameters.

Feature Description

The SMF selects UPF from a list of all active UPFs based on the predefined query parameters.

The 5GS and EPS core networks apply the selection mechanism to select a UPF node during the creation of a subscriber session.

When the UPF selection is based on the load of the UPFs, the SMF distributes calls among active UPFs associated with SMF. 3GPP specifies Load Control feature as optional feature over N4 reference points. This functionality enables UPF to send its load information to CP functions.

To support load-based UPF selection, the SMF uses UPF-provided Load Control information in the following Packet Forwarding Control Protocol (PFCP) messages:

- Session Establishment Response
- Session Modification Response
- Session Deletion Response
- Session Report Request

Load Control procedure details are available in *section 6.2.3* of *3GPP TS 29.244, Release 14*. The SMF adheres to the CP functionality.

How it Works

The UPF initiates an N4 Association Setup request to set up an association with SMF.

The following is a high-level summary of how SMF selects the UPF node for the core network:

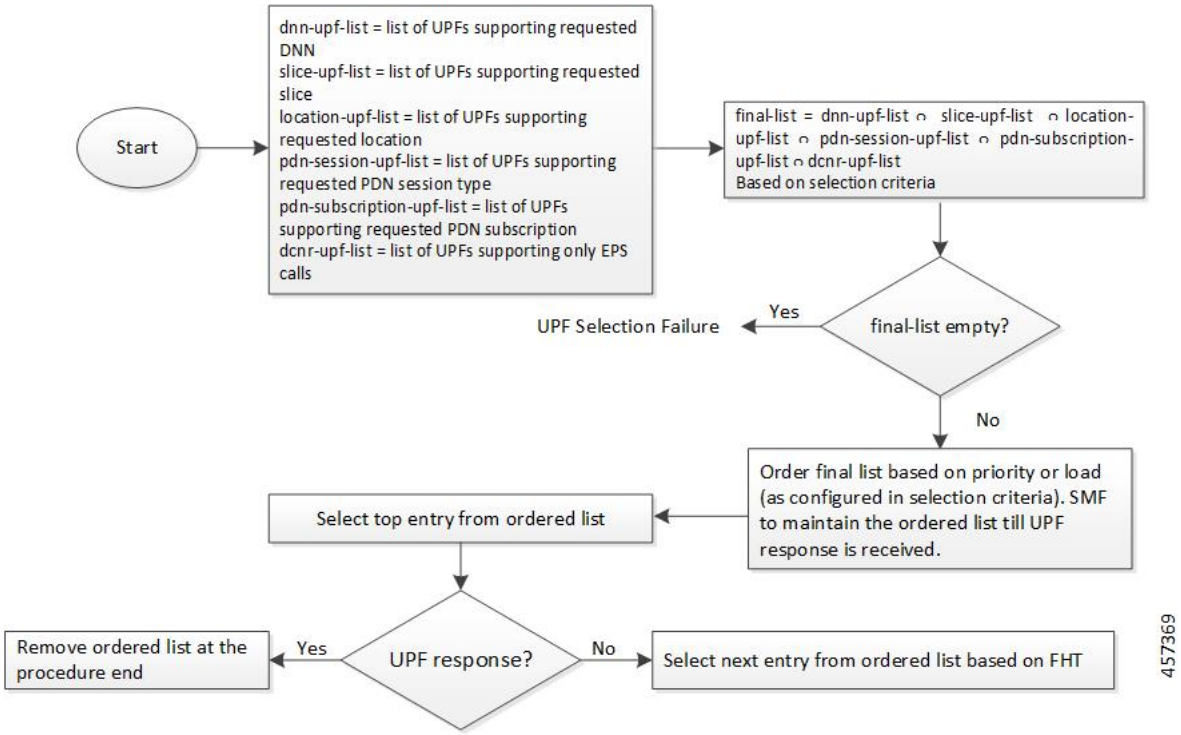
- The SMF selects the UPF node for EPS and 5GS sessions based on the UPF selection policy configured under DNN profile configuration. The UPF selection policy defines a combination of the following parameters:
  - DNN
  - Network slice
  - Subscriber location
  - DCNR (only for EPS calls)
  - PDN/PDU subscription type
  - PDN/PDU session type
- If the UPF selection policy is not defined under DNN profile configuration, then SMF selects the UPF based on the derived location DNN or requested DNN
- The SMF enables you to define the UPF selection criteria which it uses to query the appropriate node.
- If multiple UPFs match the selection criteria, then SMF selects the active UPFs and sorts them based on their priority and load information. The SMF then attempts to access the UPF one by one until the N4 Session Establishment is successful.
- The SMF stores the load information provided by UPF and uses it in selecting the UPF for the new sessions. The SMF selects the less loaded UPF among the candidate (DNN-based) active UPFs.
- The SMF considers priority and capacity configured statically against each UPF. In cases where UPF does not send the load information statically, the SMF uses the configured capacity to select the UPFs.
- The SMF selects the UPF which is given more priority in a particular location. Both the UPF priority and UPF group priority are used to determine the final priority of UPF. For information on configuring the UPF group priority, see the Assign Priority for UPF Group, on page 1075 section.

UPF Selection Algorithm

The SMF determines the UPF node based on an algorithm.

The following figure depicts the UPF node selection workflow.

Figure 211: UPF Node Selection Workflow



The SMF lists the UPF nodes based on the priority assigned to the node. When there are multiple nodes with the same priority value, then the SMF selects a UPF experiencing the lowest level of load. The load parameter is applied only for UPFs that have the same priority.

When load is not available as a selection criteria, then SMF selects a random UPF when there are multiple UPFs with the same priority.

The SMF stores UPF order list based on priority. When a failure occurs, the SMF selects the next entry in the list based on failure handling template (FHT) configuration.

If priority is not available as a selection criteria and load is available as a selection criteria, then SMF selects least loaded UPF from the list of selected UPFs.

Important The SMF performs UPF selection during initial call establishment and handover procedure.

When the subscriber location is used as the UPF selection parameter, the SMF uses the priorities that are set for the UPF and the UPF group to choose the best suitable UPF.

The following is an example to understand the UPF selection logic.

Assume two UPF groups and two UPFs with the following configurations.

- UPF groups:

- UpfGrp1:
  - Location Area Group List:TAI1
  - Slice list
  - PDN type list
- UpfGrp2:
  - Location Area Group List:TAI2
  - Slice list
  - PDN type list

- UPFs
  - Upf1:
    - Priority: 500
    - Capacity: 1000
    - Upf Grp List: ((UpfGrp1, priority: 10), (UpfGrp2, priority: 30))
  - Upf2:
    - Priority: 500
    - Capacity: 1000
    - Upf Grp List: ((UpfGrp1, priority: 20), (UpfGrp2, priority: 5))

A combination of UPF group priority and UPF priority is used for selecting the UPF having more preference (less priority) in a particular location.

The SMF selects upf1 for location TAI1 as upf1 is with less priority. Similarly, upf2 is selected for TAI2 based on the UPF priority and UPF group priority.

The SMF also provides the capability to configure DNN profile based on UE location, that is, TAI or ECGI. The location-based DNN profile allows mapping of location area group with DNN profile where location area group specifies the TAI or ECGI group.

For TAI-based UPF selection, it is mandatory to first select the DNN profile based on the UE location through location-dnn-profile configuration. Then, use the UPF selection policy (for example, DNN and slice selection criteria) defined in the selected DNN profile.

For configuration details, see the Select Location-based DNN Profile, on page 1075 section.

Standards Compliance

The Load-based UPF Selection feature complies with the following standard:

- *3GPP TS 29.244 Release 14 – LTE; Interface between the Control plane Plane and the User Plane of EPC Nodes*

Limitations

The Load-based UPF Selection feature has the following limitation:

- Post nodemgr POD restart, UPF association must be re-established for subsequent PDU session establishments to be successful.

Configuring the UPF Selection Feature

This section describes how to configure the UPF Selection feature.

The UPF selection depends on the query parameter. Use the following configurations based on the selected query parameter.

- Creating the ECGI Group Profile for EPS Session, on page 1068
- Creating the NCGI Group Profile for 5GS Session, on page 1069
- Configuring Tracking Area Identity Group, on page 1070
- Creating the Location-Area-Group Profile, on page 1071
- Defining the UPF Group, on page 1071
- Associating the UPF Group with UPF Network Element, on page 1072
- Defining UPF Selection Query Parameters, on page 1073
- Associating UPF Selection Query Parameters with DNN Profile, on page 1074
- Configuring UPF Address, on page 1077

Creating the ECGI Group Profile for EPS Session

This section describes how to create an instance of the ECGI Group Profile.

The ECGI Group Profile allows you to configure the list of individual ECGI values and ranges.

To create an ECGI-Group, use the following sample configuration.

```
config
  profile ecgi-group profile_name
    mcc mcc_value mnc mnc_value
    ecgi list [ ecgi_value1 ecgi_value2 ecgi_valueN ]
    ecgi range start start_value end end_value
    end
```

NOTES:

- **profile ecgi-group** *profile_name*: Specify the name of the ECGI Group Profile to enter the profile configuration. The ECGI Group Profile supports a maximum number of 16 PLMNs.
- **mcc** *mcc_value* **mnc** *mnc_value*: Specify the MCC and MNC values.
- **ecgi list [** *ecgi_value1 ecgi_value2 ecgi_valueN* **]**: Specify the list of ECGI values to be configured. The accepted value is the 7-digit hex string E-UTRAN Cell ID. The SMF supports a maximum number of 64 ECGI values under a PLMN.
- **ecgi range start** *start_value* **end** *end_value*: Specify the start and end range values of ECGI. The accepted start and end range of ECGI is the 7-digit hex string E-UTRAN Cell ID. **ecgi range** is an optional

attribute. You can configure multiple ECGI range values. The SMF supports a maximum number of 64 ECGI ranges under a PLMN.

Important The SMF ignores the ECGI range values if the start range value is greater than the end range value.

Verifying the ECGI-Group Profile Creation

This section describes how to verify if the ECGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ecgi-group** command:

```
profile ecgi-group e1
mcc 123 mnc 45
  ecgi list [ 1234567 abcdef0 ]
  ecgi range start 1111111 end fffffff
  exit
exit
exit
```

Creating the NCGI Group Profile for 5GS Session

This section describes how to create an instance of the NCGI Group Profile.

The NCGI Group Profile allows you to configure the list of individual NCGI values and range.

To create an NCGI group, use the following sample configuration.

```
config
  profile ncgi-group profile_name
    mcc mcc_value mnc mnc_value
    ncgi list [ ncgi_value1 ncgi_value2 ncgi_valueN ]
    ncgi range start start_value end end_value
    end
```

NOTES:

- **profile ncgi-group** *profile_name*: Specify the name of the NCGI Group Profile to enter the profile configuration. The NCGI Group Profile supports a maximum number of 16 PLMNs.
- **mcc** *mcc_value* **mnc** *mnc_value*: Specify the MCC and MNC values.
- **ncgi list [** *ncgi_value1 ncgi_value2 ncgi_valueN* **]**: Configure the list of NCGI values to be configured. The accepted value is the 9-digit hex string NR Cell ID. The SMF supports a maximum number of 64 NCGI values under a PLMN.
- **ncgi range start** *start_value* **end** *end_value*: Configure a specific NCGI range or multiple NCGI range lists. The accepted start and end range is the 9-digit hex string NR Cell ID. **ncgi range** is an optional attribute. You can configure multiple NCGI range values. The SMF supports a maximum number of 64 NCGI ranges under a PLMN.

Important The SMF ignores the NCGI range values if the start range value is greater than the end range value.

Verifying the NCGI-Group Profile Creation

This section describes how to verify if the NCGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ncgi-group** command:

```
profile ncgi-group n1
mcc 123 mnc 45
  ncgi list [ 123456789 12ab34CD9 ]
  ncgi range start 111111111 end FFFFFFFFF
  exit
exit
exit
```

Configuring Tracking Area Identity Group

The SMF provides configuration to define the supported list of Tracking Areas and Tracking Area Ranges for a PLMN. Upon enabling this configuration, the SMF sends the configured Tracking Area Identity (TAI) to the NRF during the SMF Service Registration.

To define multiple TAI groups with different names, use the following sample configuration.

```
config
  profile tai-group tai_group_name
    mcc mcc mnc mnc
    tac list [ tac_value1 tac_value2 tac_valueN ]
    tac range start tac_start_value end tac_end_value
    end
```

NOTES:

- **profile tai-group** *tai_group_name*: Specify the name of the TAI Group to enter the profile configuration.
- **mcc** *mcc_value*: Specify the mobile country code.
- **mnc** *mnc_value*: Specify the mobile network code.
- **tac list [** *tac_value1 tac_value2 tac_valueN* **]**: This keyword allows you to configure—
  - multiple PLMNs and TAC values within the specified TAI group
  - a maximum number of 16 PLMNs within the specified TAI group
  - a maximum number of 64 TAC values under a PLMN
- **tac range start** *tac_start_value* **end** *tac_end_value*: This keyword allows you to configure—
  - multiple TAC range values
  - a maximum number of 64 TAC ranges under a PLMN

Important The SMF ignores TAC range values if the start range value is greater than the end range value.

- The SMF derives TAC list and TAC range from TAI group or NCGI group configuration. If the NCGI list already includes a TAC, you can skip the TAC configuration under TAI group. However, if the TAC is associated to a different UPF, this behavior is not applicable.

Creating the Location-Area-Group Profile

The SMF associates one or more serving location details to a peer UPF. Location details include individual tracking areas and/or a range of tracking areas along with optional supported cells details.

To create an instance of the location area group profile which is added under the ecgi-group and ncgi-group, use the following sample configuration.

```
config
   profile location-area-group profile_name
      tai-group tai_group_name
      ecgi-group ecgi_group_name
      ncgi-group ncgi_group_name
      end
```

NOTES:

- **profile location-area-group** *profile_name* : Specify the name of the location area group to enter the profile configuration.
- **tai-group** *group_name*: Specify the name of the TAI group.
- **ecgi-group** *group_name*: Specify the name of the ECGI group. This configuration is optional.
- **ncgi-group** *group_name*: Specify the name of the NCGI group. This configuration is optional.

Verifying the Location-Area-Group Profile Creation

This section describes how to verify if the Location-Area-Group Profile is created.

The following configuration is a sample output of the **show running-config profile location-area-group** command:

```
profile location-area-group la1
tai-group  t1
ecgi-group e1
ncgi-group n1
exit
```

Defining the UPF Group

This section describes how to configure the UPF group, and define pdn-session-type, slice-group and other parameters for the UPF group profile.

To define the UPF group profile, use the following sample configuration.

```
config
  profile upf-group upfgroup_name
     pdn-session-type [ ipv4 | ipv4v6 | ipv6 ]
     dcnr { false | true }
     slice-group-list [ slice1 slice2 sliceN ]
     location-area-group-list [ la1 la2 laN ]
     end
```

NOTES:

- **profile upf-group** *upfgroup_name*: Specify a name for the UPF group that must be associated to the specified UPF network configuration.

- **pdn-session-type [ipv4 | ipv4v6 | ipv4v6]**: Configure the PDN session type that is supported by UPF. The query parameters for pdn-session-type accept the "pdn-type-subscription" and "pdn-type-session". This parameter selects the pdn-type from UDM returned subscription or UE session, respectively.

Note If both "pdn-type-subscription" and "pdn-type-session" parameters are configured, SMF considers "pdn-type-subscription".

The SMF provides this CLI option to associate the UPF to servicing different PDN session types, such as IPv4, IPv6, and IPv4v6. An UPF serves more than one PDN session type.

- **slice-group-list [** *slice1 slice2 sliceN* **]**: Specify the configured Network Slice Selection Assistance Information (NSSAI) list. The slice value must be the same as the allowedNssai under smf-profiles. The slice group contains both the NSSAI and DNN information. When fetching the NSSAI UPF list, consider the DNN list that is configured under the slice group. The existing dnn-list under the network-element is not moved to the upf-profile group.
- **dcnr { true | false }**: Configure the Dual Connectivity with New Radio (DCNR) capability. The default configuration is false.

Note The DCNR capability is applicable only for 4G calls.

- **location-area-group-list [** *la1 la2 laN* **]**: Configure the list of location area groups with different names.

Verifying the UPF Group Profile Configuration

This section describes how to verify if the UPF Group Profile is configured.

The following configuration is a sample output of the **show running-config profile upf-group** *upfgroup_name* command:

```
profile upf-group ug1
pdn-session-type ipv4v6
slice-group-list [ slice1 ]
location-area-group-list [ loc1 ]
dcnr true
exit
```

Associating the UPF Group with UPF Network Element

To associate the defined UPF group with the UPF network element, use the following sample configuration.

The UPF profile contains a list of UPFs configured in the SMF.

```
config
  profile network-element upf upf_name
    upf-group-profile upfgroup_name
    capacity service_capacity
    priority priority_value
    dnn-list dnn_list
    end
```

NOTES:

- **profile network-element upf** *upf_name*: Configure the UPF network configuration to which the defined UPF group is associated.
- **upf-group-profile** *upf_group*: Configure the UPF group name that must be associated to the specified UPF network configuration.
- **capacity** *service_capacity*: Configure the static weight relative to other UPFs of the same type. *server_capacity* must be an integer in the range of 0–65535. Default: 10.
- **priority** *priority_value*: Configure the static priority relative to other UPFs of the same type. *priority_value* must be an integer in the range of 0–65535. Default: 1.
- **dnn-list** *dnn_list*: Specify the list of location DNNs or DNNs supported by the UPF node.

Verifying the UPF Configuration

This section describes how to verify the UPF configuration and the association of UPF group with UPF network element.

The following configuration is a sample output of the **show configuration** command:

```
profile network-element nrf nrf1
http-endpoint base-url http://209.165.200.253:8082
…
profile network-element upf upf2
upf-group-profile ug1
capacity 10
priority 1
n4-peer-address ipv4 209.165.200.234
n4-peer-port 8805
keepalive 60
dnn-list [ dnn1 intershat cisco.com ]
…
```

Defining UPF Selection Query Parameters

This section describes how to configure parameters that enable SMF to select the UPF using the selection query.

To define the UPF selection policy-specific configuration, use the following sample configuration.

```
config
  policy upf-selection upfpolicy_name
    precedence priority_value [ dcnr | dnn | location | pdn-type-session |
 pdn-type-subscription | slice ]
    end
```

NOTES:

- **policy upf-selection** *upfpolicy_name*: Specify the UPF policy name that must be associated with the DNN profile.

  The SMF selects the UPF node with the lowest precedence value. The SMF selects the node with the highest precedence selection-criteria when the previous lower precedence criteria did not return any UPF. If the configured criteria are exhausted, and nodes are not selected, then the UPF selection policy fails.

  Within the precedence value, the intersection of UPFs from each criterion is performed to retrieve the UPF list.

- **precedence** *priority_value* **[dcnr | dnn | location | pdn-type-subscription | pdn-type-session | slice]**: Assign the precedence value to the UPF policy. Specify the DNN and other parameters for the UPF selection.

  The **precedence** keyword allows a maximum of four precedence values to be configured under the UPF selection policy.

  If the DNN profile does not have any UPF selection policy associated with it, then the SMF performs UPF selection using location DNN or DNN, priority, and load information.

Verifying the UPF Selection Policy Configuration

This section describes how to verify if the UPF selection policy is configured.

The following configuration is a sample output of the **show running-config policy upf-selection** command:

```
#show running-config policy upf-selection
policy upf-selection polUpf1
   precedence 1
         [dnn location pdn-type-subscription]
   exit
   precedence 2
         [dnn pdn-type-session slice]
   exit
   precedence 3
          [dnn]
   exit
exit
```

Associating UPF Selection Query Parameters with DNN Profile

This section describes how to associate UPF selection query parameters with DNN profile.

To associate the UPF selection policy with DNN profile, use the following configuration:

```
config
   profile dnn profile_name
      upf-selection-policy upfpolicy_name
      end
```

NOTES:

- **profile dnn** *profile_name*: Specifies the DNN profile name. *profile_name* must be an alphanumeric string.
- **upf-selection-policy** *upfpolicy_name*: Specifies the name of UPF selection policy that must be associated to the DNN profile.

Verifying the Association of UPF Selection Policy and DNN Profile

This section describes how to verify if the UPF selection policy association with the DNN profile is established.

The following configuration is a sample output of the **show running-config profile dnn** *profile_name* command:

```
profile dnn intershat
upf-selection-policy upfPol1
end
```

Assign Priority for UPF Group

This section describes how to configure the UPF group list and assign priority for the UPF group.

The UPF group lists the set of locations, slices, and so on. Each UPF present in the group is given a priority which decides the final priority of that UPF.

To assign the UPF group priority, use the following sample configuration.

```
config
  profile network-element upf upf_profile_name
    upf-group-profile-list upf_group_name
      priority priority_value
      end
```

NOTES:

- **upf-group-profile-list** *group_name*: Specify the UPF group profile name.
- **priority** *priority_value*: Assign priority to the UPF group.

  The UPF group priority is used in scenarios where there are two or more UPFs with the same location (TAI).

Configuration Verification

To verify the feature configuration, use the **show running-config profile network-element upf** command.

The following is an example output of the **show running-config profile network-element upf** command.

```
[smf] smf# show running-config profile network-element upf
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.231
 n4-peer-port 8805
 dnn-list     [ intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
 intershat7 intershat_hrt intershatipex ]
 capacity     65535
 priority     65535
 upf-group-profile-list group1 priority 10
 upf-group-profile-list group2 priority 20
exit
```

In the preceding output, check the lines **upf-group-profile-list group1 priority 10** and **upf-group-profile-list group2 priority 20** to view the UPF group configurations and the UPF group priorities.

To view all the configured UPF groups, use the **show running-config profile upf-group** command.

The following is an example output of the **show running-config profile upf-group** command.

```
[smf] smf# show running-config profile upf-group
profile upf-group group1
 failure-profile FH1
exit
profile upf-group group2
 failure-profile FH2
exit
```

Select Location-based DNN Profile

The DNN policy can have a DNN profile configuration based on UE location for each UE-requested DNN. The DNN profile has a virtual or mapped DNN with its list of interfaces.

To configure location-based DNN profile, use the following sample configuration:

```
config
  policy dnn dnn_policy_name
    dnn dnn_name location-dnn-profile location_dnn_profile_name
    end
```

NOTES:

- **dnn** *dnn_name* **location-dnn-profile** *location_dnn_profile_name*: Specify the name of DNN profile that is defined based on the UE location.

  This configuration maps the UE-requested DNN with the location-based DNN profile in DNN policy.

Associate Location Area Group and DNN Profile

To associate location area group and location-based DNN profile, use the following sample configuration:

```
config
  profile location-dnn location_dnn_profile_name
    location-area-group lag_name profile dnn_profile_name
    end
```

NOTES:

- **profile location-dnn** *location_dnn_profile_name*: Specify the name of the configured DNN profile.
- **location-area-group** *lag_name* **profile** *dnn_profile_name*: Specify the name of a location area group and DNN profile.

  This configuration maps the location area group with the DNN profile.

Configuration Example

The following is an example configuration.

```
config
 policy dnn polDnn
  profile default-profile
  dnn ims location-dnn-profile loc1
  exit
  profile location-dnn loc1
   location-area-group lag1 profile dnnprof-imslag1
   location-area-group lag2 profile dnnprof-imslag2
   exit
  profile location-area-group lag1
   tai-group tai1
   ecgi-group ecgi1
   exit
  profile location-area-group lag2
   tai-group tai2
   ecgi-group ecgi2
   exit
  profile tai-group tai1
   mcc 123 mnc 456
   tac range start 4455 end 5566
   exit
  profile tai-group tai2
   mcc 123 mnc 456
   tac range start 3355 end 3366
   exit
  exit
```

```
  profile ecgi-group ecgi1
   mcc 123 mnc 456
   ecgi range start A123451 end A234567
   exit
  exit
  profile ecgi-group ecgi2
   mcc 123 mnc 456
   ecgi range start B123451 end B234567
   exit
  exit
  profile location-dnn loc1
   location-area-group lag1 profile dnnprof-imslag1
   location-area-group lag2 profile dnnprof-imslag2
   exit
  profile dnn dnnprof-imslag1
   dns primary ipv4 209.165.201.10
   dns primary ipv6 fd00:976a::9
   dns secondary ipv4 209.165.201.12
   dns secondary ipv6 fd00:976a::10
   dnn imslag1 network-function-list [ upf ]
   dnn rmgr imslag1
   upf-selection-policy       upfsecpol1
   timeout up-idle 3600 cp-idle 7320
   pcscf-profile pcscf1
   session type IPV4V6
   upf apn ims
   dcnr true
   userplane-inactivity-timer 3600
   exit
  profile dnn dnnprof-imslag2
   dns primary ipv4 209.165.201.13
   dns primary ipv6 fd00:976a::9
   dns secondary ipv4 209.165.201.14
   dns secondary ipv6 fd00:976a::10
   dnn imslag2 network-function-list [ upf ]
   dnn rmgr imslag2
   upf-selection-policy       upfsecpol2
   timeout up-idle 3600 cp-idle 7320
   pcscf-profile pcscf1
   session type IPV4V6
   upf apn ims
   dcnr true
   userplane-inactivity-timer 3600
   exit
  exit
 exit
exit
```

In the preceding example, the name of the configured DNN is "ims", location-dnn-profile is “loc1”, location-area-group is "lag1" and "lag2", and the dnn-profile is "dnnprof-imslag1" and "dnnprof-imslag2".

SMF selects location-dnn-profile “loc1” for the “ims” DNN received in PDU session request. The loc1 profile maps location-area-group to the dnn-profile. The SMF uses TAI and ECGI information from PDU session request to find the configured location-area-group "lag1". Then, the corresponding dnn-profile "dnnprof-imslag1" is selected.

After the "dnnprof-imslag1" dnn profile is selected, the SMF selects a suitable UPF based on the selection criteria that are specified in the UPF selection policy.

Configuring UPF Address

This section describes how to configure SUPI and UPF node information.

To configure the SUPI value and UPF addresses, use the following sample configuration:

```
config
   system-diagnostics supi supi_value
     preferred-up node-id upf_address
     end
```

NOTES:

- **system-diagnostics supi** *supi_value*: Specify the SUPI value or a list of SUPI values separated by comma. *supi_value* must be a string of 15 digits.
- **preferred-up node-id** *upf_address*: Specify the UPF addresses, separated by comma, for the configured SUPI. *upf_address* must be a string in the IPv4 address pattern.

  When multiple UPFs are configured for a SUPI, the SMF performs UPF selection for a particular PDU session based on the SUPI preferred configuration.

Configuration Verification

To verify the configuration, use the **show running-config system-diagnostics supi** command.

The following is an example output of the show command.

```
[smf] smf# show running-config system-diagnostics supi
system-diagnostics supi [ 123456789012345 ]
 preferred-up node-id [ 209.165.200.230 209.165.200.236 ]
exit
```

UPF Selection OA&M Support

This section describes operations, administration, and maintenance information for this feature.

Statistics

The following statistics are added in support of UPF node selection based on DNN, pdn-type-session, network slice, priority, and load.

- upf-selector

  req_type="upf-selector",

  status="Precedence:2 Dnn-Upf-List:3 Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"

  status="upf_selector_empty_upf_list"

  status="upf_selector_invalid_upf_selection_policy"

  Example:

  ```
  smf_service_resource_mgmt_stats{app_name="SMF",cluster="Local",
  data_center="DC",dnn="intershat",emergency_call="",instance_id="0",ip_req_type
  ="upf-selector",pdu_type="ipv4",procedure_type="PDU Session Establishment",
  rat_type="NR", service_name="smf-service", status="Precedence:2 Dnn-Upf-List:3
   Pdn-Type-Upf-List:2 Slice-Upf-List:2 Dcnr-Upf-List:0"} 1
  ```

IP Threshold-based UPF Selection

Feature Description

This feature addresses the load balancing across overloaded UPFs. Each IP pool has existing usable threshold configuration. This configuration allows to mention percentage of IP addresses to be considered as a threshold hit for a given UPF. IPAM informs SMF when a threshold is hit for a particular DNN for a UPF, SMF gives lower priority to such UPF until UPF hits threshold condition.

Use Cases

UPFs serving same DNN and have different priority consume IP addresses unevenly, in such cases particular UPF may run out of IP addresses quickly and hit a threshold. In such cases SMF will first give preference to UPFs which have't hit the threshold while assigning new sessions.

Due to nonlinear activities in field, it is possible that initial session distribution by SMF to UPF is uniform. In the subsequent sessions, one particular UPF may stay longer and another UPF cleared, in such cases new sessions continue to distribute based on priority the UPF. On the calls which stay longer may hit a threshold and it may happen that UPF may run out of IP addresses. To cater such situation the UPF's threshold is given less priority.

How it Works

This section describes how IP Threshold SMF and IPAM Integration works.

Intimation of a threshold hit condition from IPAM to SMF: When IP addresses in a DNN for a UPF left with a “threshold” configured number of IP addresses in a IPAM module gives information to SMF using resource management response.

SMF behaviour when a threshold hit received: SMF marks a usable threshold hit for a given UPF. Since IPAM pool distribution is per node manager separately, SMF marks a threshold separately for primary and secondary node manager.

SMF behaviour choosing UPF for new session when a threshold marked: SMF performs the following checks.

- If a threshold hit for a primary node manager and secondary node manager is not hit, IP allocation request is sent for a secondary node manager.
- If a threshold hits both primary and secondary node manager, then current UPF selects the lower priority node manager, if any other UPF configured and threshold not hit is selected first.
- If all the UPFs are threshold hit, then the behaviour falls back to priority and load based which is existing behaviour. This is similar to that of a non-existence threshold hit behaviour.

Important Refer IP Address Management, on page 737 chapter for configuration details.

Recovery behaviour from a threshold hit: IPAM to periodically if UPF has come out of threshold hit condition. When UPF has enough free addresses to come out of threshold hit (for each DNN, and each UPF) IPAM gives information of SMF (through a callback). SMF unmarks UPF as threshold hit.

When IP addresses in a pool (for each DNN, and each UPF) left with a “threshold” configured number of IP addresses in a IPAM module gives information to SMF using resource management response.

OAM Support for IP Threshold-based UPF Selection

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

New statistics introduced to capture the following stats information:

Lables:

- Label: up_ep_key

  Label Description: When a particular IP address pools threshold is hit for usage of IP addresses, this stats will be recorded

  Example: 209.165.200.241:209.165.200.242

- Label: dnn

  Label Description: DNN of the IP pool which reached the configured threshold usgae

  Example: sampleDNN

- Label: threshold_hit

  Label Description: Indicates if the threhold hit is yes or no

  Example: yes

- Label: threshold_clear

  Label Description: Indicates if the threhold hit is cleared or not

  Example: yes

- Label: nodemgr_id

  Label Description: Indicates the instance of the nod manager which hit the threshold

  Example: 1

show userplane all

This section describes show commands that help in debugging issues.

show userplane all

- Node IP and end point
- Capacity and priority
- Serving DNN list
- Primary and peer node manager instance
- Load seq and load metrics
- Connected time
- Usable threshold hit for primary and secondary node manager

The following is an example of the show command output

```
[smf] smf# show userplane all
result
{
  "209.165.200.230:209.165.200.244": {
    "NodeIdType": 1,
    "NodeId": "209.165.200.228",
    "NodePort": 8805,
    "NodeStatus": 2,
    "Capacity": 65535,
    "Priority": 65535,
    "DnnList": [
      "intershat",
      "intershat1",
      "intershat2",
      "intershat3"
    ],
    "PrimaryNodeMgrInst": {
      "InstanceId": 1,
      "IsActive": true
    },
    "PeerNodeMgrInst": {
      "IsActive": true
    },
    "EpIp": "209.165.200.244",
    "EpPort": 8805,
    "UpEpKey": "209.165.200.230:209.165.200.244",
    "recoveryInfo": {
      "SvcRecoveryTime": 3820194022,
      "PeerRecoveryTime": 3817503651
    },
    "ConnectedTime": 3820194461,
    "IntfType": 1,
    "UpProfName": "upf1",
    "OverloadTimer": {},
    "NegotiatedCPFeatures": 2147483648
  }
}
```

Co-located UPF Selection During Initial EPS Attach

This section describes how the SMF performs UPF selection during the initial EPS Attach procedure.

Feature Description

The converged core gateway with the cnSGWc and SMF supports selection of a converged UP node to realize convergence. With this functionality, it is possible to create an optimized data path for the UE.

The SMF performs co-located UPF selection based on the SGW-U node name received in the Create Session Request (CSR) message.

How it Works

This section describes how the SMF handles the co-located UPF selection during PDN Session Establishment in 4G network.

When the SGW-U node name is available in the CSR, SMF derives the UPF from the configuration based on the node name.

Then, SMF uses the existing UPF selection logic and derives the list of UPFs accordingly. The SMF checks if the SGW-C selected UPF exists in the derived UPF list.

If the SGW-C selected UPF is present in the derived UPF list and if its priority matches with the highest priority in the derived UPF list, then SGW-C selection UPF is selected. Otherwise, priority UPF in the derived list is selected.

In the absence of the SGW-U node name, the SMF follows the existing UPF selection algorithm.

Configuring Node ID

To select the co-located UPF, use the following sample configuration.

```
config
  profile network-element upf upf_name
    node-id value
    end
```

NOTES:

- **profile network-element upf** *upf_name*: Specify a profile name for the UPF.
- **node-id** *value*: This keyword aids in configuring the node ID of UPF. The SMF compares this node name with SGW-U node name to select the co-located UPF. *value* is an alphanumeric string.

Statistics Support

The SMF maintains the following statistics in support of this feature.

upf_selection_stats

Description: Displays the total number of times the same co-located UPF is selected by SMF.

Metrics-Type: Counter

Labels:

- upf_selection_type
- upf_fqdn
- preferred
- upf_not_associated
- upf_profile_not_found
- upf_not_active
- n4_failed
- pdu_session_type
- pdu_subscription_type
- snssai

Status:

- attempted
- failure

Reason: If the status is failure, the value can be one of the following:

- upf_not_associated
- upf_profile_not_found
- upf_not_active
- n4_failed

Co-located UPF Selection During Handover

This section describes how the SMF performs UPF selection during 5G to 4G handover and EPS fallback scenarios.

Feature Description

During the UE session establishment in 5G core network, the SMF uses the existing UPF selection logic and records the index of the selected UPF in PGW-C Control Tunnel Endpoint Identifier (TEID).

Upon receiving Create Session Request (CSR) from MME, cnSGWc checks whether or not the TEID value is zero. If it is zero, then cnSGWc sends Remote Procedure Call (gRPC) message to SMF and fetches UP ID and UPF IP.

If the TEID is non-zero, the SMF checks the bits from 21 through 30 of control TEID value, and extracts the UPF index. The SMF uses the extracted UPF index to select the preferred UPF.

The SGW-C uses this as the preferred UPF when the UE session is handed over to EPS network. If the preferred UPF is present in the list returned by the UPF selection algorithm, then the cnSGWc selects the UPF with highest priority. That is, the cnSGWc selects the same UPF that was chosen by SMF. This operation enables creating an optimized data path for the UE.

If the preferred UPF does not exist in the returned list, cnSGWc selects a different UPF.

Configuring Parameters for Co-located UPF Selection

This section describes how to perform co-located UPF selection during handover scenario.

Configuring the parameters for co-located UPF selection involves the following steps:

- Enabling Co-located UPF Selection, on page 1083
- Configuring Index and Session Count for UPF Selection, on page 1084

Enabling Co-located UPF Selection

To enable or disable co-located UPF selection, use the following sample configuration.

```
config
  profile converged-core cc_profile_name
    up-selection { disable | enable }
    end
```

NOTES:

- **profile converged-core** *cc_profile_name*: Specify the name of the converged core profile. This keyword allows you to enter the converged core profile configuration mode.

- **up-selection { disable | enable }**: Enable or disable the co-located UPF selection. By default, this configuration is enabled.

Configuring Index and Session Count for UPF Selection

To define the UPF index value and maximum session count for co-located UPF selection, use the following sample configuration.

```
config
  profile converged-core cc_profile_name
    max-upf-index upf_index_value
    max-session-count up_session_count
    end
```

NOTES:

- **profile converged-core** *cc_profile_name*: Specify the name of the converged core profile. This keyword allows you to enter the converged core profile configuration mode.
- **max-upf-index** *upf_index_value*: Specify the maximum number of supported UPF index values for UPF selection.

  upf_index_value must be an integer in the range of 0–1023.

  The SMF validates the configured UPF index value against the UP ID received in the N4 Association Setup request from UPF. If the validation fails, the SMF rejects the corresponding request. If the validation is successful, the SMF acknowledges the request and stores the UP ID along with other UPF details.
- **max-session-count** *up_session_count*: Specify the maximum number of UP sessions supported.

  up_session_count must be an integer in the range of 1000000–12000000. Default value is 1000000.

  The SMF uses the configured session count to associate the UP session with IdMgr context. Note that IdMgr maintains a separate context per million UP sessions.

Support for UPF Node Reports and Proprietary Session Reports

Feature Description

The SMF triggers the Packet Forwarding Control Protocol (PFCP) Node Report procedure as per the *3GPP TS 29.244, section 6.2.9*. The UPF sends this report to indicate a user plane path failure affecting all the PFCP sessions towards a remote GTP-U peer. The UPF notifies this failure to the SMF through User Plane Path Failure Report (UPFR). When the UPF detects a GTP-U path failure, the SMF clears the PDU sessions belonging to the GTP-U peer and UPF node ID.

In addition to the existing UPF session report, the SMF supports the following proprietary report types:

- Graceful Termination Report (GTER)—This type of report is sent when the UPF is unable to recover a PDU session during Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).
- Session Replacement Report (SRIR)—This type of report is sent to replace a session due to identical GTP-U tunnel endpoint identifier (TEID) allocated by gNB. This is possible with the restart of gNB. In this case, the old session with the same TEID is deleted.

- Self-protection Termination Report (SPTER)—This type of report is sent to terminate a PFCP session during overload scenarios.

How it Works

This section describes how the SMF supports the UPF node report and the proprietary session reports.

PFCP Node Report Handling

For proper handling of PFCP node report, the GTP-U peer address must include a non-unique secondary session key. The Common Data Layer (CDL) stores the peer address and the UPF IP address along with the session details. If the GTP-U peer address changes during idle to active transition procedure, N2 handover (HO), 5G to 4G HO, or 4G to 5G HO, the CDL database deletes the old key and adds the new one.

1. The UPF sends PFCP Node Report Request to the SMF along with the IP address of the failed GTP-U peer.
2. The SMF protocol checks the node ID, that is, the UPF IP address included in the request. If the node ID is not found or if the node ID is not in associated state, the SMF protocol sends a failure response.
3. If the node ID is found, the node manager queries the CDL for EPS session with the GTP-U peer IP address and node ID. The node manager sends bulk notification to the CDL to clear the corresponding sessions.
4. The CDL sends the notification to rest endpoint (REST-EP) pod to clear the sessions.
5. The REST-EP pod sends the subscriber clear notification to the SMF service based on the affinity. The SMF service clears the sessions on all interfaces.

PFCP Session Report Handling

The UPF sends PFCP session report along with GTER, SRIR, and SPTER to the SMF. If the session is found, the SMF sends a successful PFCP session report response. Then, the SMF triggers the PDU session release procedure and deletes the sessions on all interfaces.

Collision Handling

For the newly supported messages (node report and session report), the SMF triggers the PDU session release procedure. If the PDU session release procedure collides with the HO procedure, the SMF does not abort the HO procedure as the GTP-U peer IP changes during the HO. To achieve this, the PDU release procedure involves comparing the GTP-U peer IP address received in release request with the one present in the PDU session. If the two addresses are different, then the SMF aborts the release procedure.

Important The collision handling depends on the arrival time of the incoming HO message and **clear subscriber** command triggered by node report.

Resiliency Handling

The SMF uses a retry timer to check and report any pending session deletions for a GTP-U peer. After the restart of SMF node manager, if any sessions are not deleted, then these sessions remain as is.

Standards Compliance

The UPF Node Report and Session Report Support feature complies with the following standard:

- *3GPP TS 29.244 Version 15.6.0 – LTE; Interface between the Control Plane and the User Plane nodes*

Limitations

This feature has the following limitations:

- If the CDL notifications are lost and the sessions are not cleared, the SMF node manager retries the bulk deletion operation only once after 10 minutes.
- If the node report request arrives and the system is in overload state, some CDL notifications are dropped. In this case, the SMF performs the session clean-up based on error indication report request from the UPF.
- The UPF currently sends only one Remote GTP-U peer in the Node Report request. So, the SMF can validate only one remote GTP-U peer.

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Monitoring Support

An alarm is added when the following configuration is performed on CEE Ops-Center. This alarm indicates that a GTP-U peer for a particular UPF has gone down. The alarm data includes GTP-U peer IP and UPF IP addresses.

The following is a sample configuration performed on the CEE Ops-Center to configure alert rules related to the UPF Node Report Request.

```
config
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      severity severity_level
      type alert-type
      annotationannotation_name
      value annotation_value
      exit
   exit
```

NOTES:

- **alerts rules**: Specify the Prometheus alerting rules.
- **group** *alert_group_name*: Specify the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The *alert-group-name* must be a string in the range of 0–64 characters.
- **interval-seconds** *seconds*: Specify the evaluation interval of the rule group in seconds.

- **rule** *rule_name*: Specify the alerting rule definition. *rule_name* is the name of the rule.

The following is an example configuration of the alert.

```
config
   alerts rules group NodeReportGTPURemotePeer
   interval-seconds 300
   rule NodeReportGTPURemotePeerDown
      expression smf_protocol_udp_res_msg_total{message_name=\"n4_node_report_req\",
message_direction= \"inbound\", status=\"accepted\"}"
      severity major
      type "Communications Alarm"
      annotation summary
      value "This alert is fired when the UPF Sends Node Report Request to SMF"
      exit
   exit
```

Show Command Support

Use the **show subscriber all** command to view the configuration related to GTP-U peer IP address and GTP-U peer endpoint key. This configuration data helps to identify the failed sessions or collision of procedures.

The following is an example output.

```
[unknown] smf# show subscriber all nf-service smf
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-223310101010101",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "udm-sdm:10.84.17.111",
      "pcfGroupId:PCF-dnn=;",
      "policy:2",
      "pcf:10.84.17.111",
      "upf:10.84.17.111",
      "upfEpKey:10.84.17.111:10.84.17.112",
      "ipv4-addr:poolv4/209.165.202.129",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/209.165.202.129",
      "ipv4-startrange:poolv4/209.165.202.129",
      "gtp-peer:10.84.17.112",
      "peerGtpuEpKey:10.84.17.111:10.84.17.111",
      "namespace:smf"
    ]
  ]
}
```

Use the **show subscriber count peerGtpuEpKey** command to view the number of sessions associated with the specified GTP-U peer and the UPF node.

Important Use the **show subscriber count peerGtpuEpKey** command carefully and sensibly as it might impact the system performance.

The following is an example output of **show subscriber count peerGtpuEpKey** command.

```
smf# show subscriber count peerGtpuEpKey 30.30.30.63:50.50.0.58
  subscriber-details
  {
    "sessionCount": 12568
  }
```

Statistics Support

The SMF maintains the following statistics to track the total number of attempted, successful, and failed node-level and session-level requests.

- SMF_SERVICE_STATS for the following procedure types:
  - upf_node_report_pdu_sess_rel

    attempted: Total number of attempted PDU session release requests triggered due to the node report.

    successful: Total number of successful PDU session release requests triggered due to the node report.

    failure: Total number of failed PDU session release requests triggered due to the node report.
  - upf_sess_report_gter_pdu_sess_rel

    attempted: Total number of attempted PDU session release requests triggered due to the session report “GTER”.

    successful: Total number of successful PDU session release requests triggered due to the session report “GTER”.

    failure: Total number of failed PDU session release requests triggered due to the session report “GTER”.

- SMF_PROTOCOL_UDP_REQ_MSG_TOTAL for the following message types:
  - n4_node_report_req

    attempted: Total number of attempted N4 requests triggered due to the node report.

    successful: Total number of successful N4 requests triggered due to the node report.

    failure: Total number of failed N4 requests triggered due to the node report.
  - n4_session_report_req

    attempted: Total number of attempted N4 requests triggered due to the session report.

    successful: Total number of successful N4 requests triggered due to the session report.

    failure: Total number of failed N4 requests triggered due to the session report.

- SMF_PROTOCOL_UDP_RES_MSG_TOTAL for the following message types:
  - n4_node_report_res

    attempted: Total number of attempted N4 responses triggered due to the node report.

successful: Total number of successful N4 responses triggered due to the node report.

failure: Total number of failed N4 responses due to the node report.

- n4_session_report_res

  attempted: Total number of attempted N4 responses triggered due to the session report.

  successful: Total number of successful N4 responses triggered due to the session report.

  failure: Total number of failed N4 responses due to the session report.

- SMF_DISCONNECT_STATS triggered for the following disconnect reasons:

  gtpu_peer_path_failure : This statistic is triggered when the session is deleted due to the node report.

  upf_sess_report_gter_pdu_sess_rel: This statistic is triggered when the session is deleted due to the session report.

The following is an example of the statistics:

Node Report SMF-service stats:

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""}

smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

Session Report SMF-service stats:

```
smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""} 1

smf_service_stats{always_on="",app_name="smf",cluster="smf",data_center="unknown",
dcnr="",dnn="intershat",emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="success",up_state=""} 1
```

Node Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="0",message_direction="inbound",message_name="n4_node_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 15

smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="0",message_direction="outbound",
message_name="n4_node_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin"} 15
```

Session Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf",cluster="smf",data_center="unknown",
instance_id="1",message_direction="inbound",message_name="n4_session_report_req",
msgpriority="",service_name="smf-protocol",status="accepted",
transport_type="origin"} 43

smf_proto_udp_res_msg_total{app_name="smf",cause="1",cluster="smf",
data_center="unknown",instance_id="1",message_direction="outbound",
```

```
message_name="n4_session_report_res",msgpriority="",service_name="smf-protocol",
status="accepted",transport_type="origin"}
```

The SMF also maintains labels to track the number of session deletions due to the node report and session report types – GTER, SRIR, and SPTER.

For example, the label "LABEL_DISC_PDNREL_GTER_SESSION_REP" is added to track the session deletion due to the presence of GTER.

Outer Header Format

Table 367: Feature History

Feature Name	Release Information	Description
Dual Stack Support on N3	2024.01	SMF enables the dual stack transport for N3 tunnel using the **dual-stack-transport { false | true }** CLI command in the UPF network profile. **Default Setting:** Disabled – Configuration Required

SMF sends the Outer Header IE to UPF in the Packet Detection Rule (PDR) of the PFCP session. The Outer Header IE is available in the N4 Session Establishment Request message sent over the Sx interface. The version 16.4.0 of 3GPP TS 29.244 specification defines the format of this IE.

The following table identifies the encoding format of the Outer Header Creation (OHC) Description field. It takes the form of a bitmask where each bit indicates the outer header to be added to the outgoing packet. SMF ignores the spare bits.

Table 368: Header Encoding Format

Octet / Bit	Outer Header Created in the Outgoing Packet
5/1	GTP-U/UDP/IPv4
5/2	GTP-U/UDP/IPv6
5/3	UDP/IPv4
5/4	UDP/IPv6
5/5	IPv4
5/6	IPv6
5/7	C-TAG
5/8	S-TAG
6/1	N19 Indication
6/2	N6 Indication
6/3	TCP/IPv4

Octet / Bit	Outer Header Created in the Outgoing Packet
6/4	TCP/IPv6

NOTES:

- Currently, UPF doesn't support the following values of Outer Header Creation Description:
  - IPv4
  - IPv6
  - C-TAG
  - S-TAG
  - N19 Indication
  - N6 Indication
- The third and fourth bits of the sixth octet (that is, 6/3 and 6/4) are spare bits (that is, not part of 3GPP TS 29.244, version 16.4.0) used for LI over TCP.

Important SMF and UPF must support the same format of Outer Header IE for a successful session establishment.

Feature Configuration for Outer Header IE

SMF enables dual stack connection in the UPF profile. When the dual stack is configured, the Outer Header Removal (OHR) Description field in the OHR IE is set to 6 to remove the GTP-U or UDP or IP header for the IPv4 and IPv6 addresses.

To enable dual stack on the N3 interface, use the following sample configuration:

```
config
   profile network-element upf upf_profile_name
        dual-stack-transport { true | false }
        end
```

NOTES:

- **dual-stack-transport { true | false }**: Enable or disable dual stack transport on the N3 interface.
  - When the **dual-stack-transport true** command is configured, SMF sends the OHR IE with the value 6 for the IPv6 address on the supported interfaces.
  - SMF saves the configured dual stack value during session establishment. SMF uses the same dual stack value in the subsequent N4 messages until the session gets disconnected.

Note This CLI configuration is applicable for the SMF with legacy interfaces as well.

Usage Monitoring over PCF

Feature Description

SMF supports usage monitoring functionality over the PCF N7 interface for 4G and 5G PDU sessions. After SMF reports the usage data to PCF, SMF supports the modification of usage monitoring parameters, such as Total Volume, Uplink Volume or Downlink Volume thresholds and the disabling of usage monitoring based on non-reception of usage monitoring threshold or related triggers from PCF.

How it Works

This section describes how the SMF usage monitoring over PCF N7 interface works.

Usage Reporting

UPF measures the volume and the time usage of all traffic for the PDU session or the corresponding service data flows. UPF sends the accumulated usage report in either the PFCP Session Report Request or the PFCP Session Modification Response to SMF. Then, SMF includes one or multiple accumulated usage reports in the "accuUsageReports" attribute in one of the following messages towards PCF.

- HTTP POST message

Note This message also includes the "US_RE" value in the "repPolicyCtrlReqTriggers" attribute.

- Message to include the SM Policy Delete Data data structure during the terminate procedure.

Each AccuUsageReport data structure includes the accumulated usage within one or two usage report information elements. These elements are corresponding to a usage monitoring control instance that PCF requested. If the PCF provides both volume and time thresholds and the threshold for one of the measurements reaches, then the UPF communicates this event to the SMF along with the accumulated volume and time measurements. Then, SMF sends the accumulated usage since the last report to PCF for both the measurements.

The SMF receives the accumulated usage report from UPF in the PFCP Session Report Request. After receiving this report, the SMF identifies the list of usage report corresponding to the usage monitoring control instance. Then, SMF posts a PDU Modify or PDU Dedicated bearer procedure. This procedure includes new event type, list of usage reports, and the list of URRs to process them.

Accumulated Usage Report

The following table lists the information available in the accumulated usage report.

Table 369: Accumulated Usage Report

Attribute Name	Data Type	P	Cardinality	Description
refUmIds	String	M	1	Indicate the reference ID for the UsageMonitoringData objects that is associated with the usage report.
volUsage	Volume	O	0.1	Indicate the total accumulated volume usage.
volUsageUplink	Volume	O	0.1	Indicate an accumulated volume usage in the uplink.
volUsageDownlink	Volume	O	0.1	Indicate an accumulated volume usage in the downlink.
timeUsage	DurationSec	O	0.1	Indicate an accumulated time usage.
nextVolUsage	Volume	C	0.1	Indicate an accumulated volume usage after the monitoring time.
nextVolUsageUplink	Volume	O	0.1	Indicate an accumulated volume usage in the uplink after the monitoring time.
nextVolUsageDownlink	Volume	O	0.1	Indicate an accumulated volume usage in the downlink after the monitoring time.
nextTimeUsage	DurationSec	C	0.1	Indicate an accumulated time usage after monitoring.

Usage Monitoring Data Modification

Following are the available data modification scenarios for the usage monitoring over PCF.

- If the PCF needs to remove the threshold level for one or multiple monitoring keys, the PCF provides the corresponding attribute with the NULL value to the corresponding usage monitoring control instance.
- When the PCF receives the accumulated usage in the HTTP POST message, the PCF communicates to SMF whether the usage monitoring continues for the following usage monitoring control instance:
  - If the monitoring continues for the specific levels, the PCF provides the new thresholds for the levels in the response of the HTTP POST message. This message includes the existing attributes, such as "volumeThreshold", "volumeThresholdUplink", and "volumeThresholdDownlink".
  - If the PCF stops monitoring for the specific levels, the PCF doesn't include an updated threshold in the response of the HTTP POST message for the stopped levels. It implies that PCF doesn't include the corresponding attributes in the entry of the "umDecs" attribute. These attributes are "volumeThreshold", "volumeThresholdUplink", "volumeThresholdDownlink", "timeThreshold", "nextVolThreshold", "nextVolThresholdUplink", "nextVolThresholdDownlink", and "nextTimeThreshold".

If the PCF stops the monitoring for the usage monitoring control instance, the PCF doesn't include any thresholds of the usage monitoring control instance in the response of the HTTP POST message. In addition, the PCF doesn't remove the reference of the usage monitoring control instance from the dynamic PCC rule or session rule.

Based on the following scenarios, SMF sends the PFCP Session Modification Request to PCF:

- In case of modification in the existing thresholds, SMF updates the URR with the new thresholds and initiates Update URR towards UPF in the PFCP Session Modification Request.
- In case of stopped monitoring for the usage monitoring control instance, SMF removes the URR and initiates Remove URR toward UPF in the PFCP Session Modification Request.
- In case of new usage monitoring control instance, SMF creates a new URR with the thresholds. SMF also associates the URR to the corresponding PDRs and initiates Create URR along with Update PDR toward UPF in the PFCP Session Modification Request.

Error Handling

While provisioning the usage monitoring on SMF and its actions, following errors can occur:

- If PCF has defined invalid thresholds, the SMF marks the PCC rule as failed or invalid when the Session rule or PCC rule has the reference of monitoring key (UmId) with the invalid thresholds.
- If PCF removes or doesn't configure the US_RE flag between the message exchanges where usage monitoring is active in the SMF, the SMF sends the Remove URR request to UPF in the Modification Request with the available URRs that are created for the N7 interface.

Call Flows

This section describes the following call flows.

- Usage Monitoring Activation call flow
- Usage Reporting call flow

Usage Monitoring Activation Call Flow

This section describes the Usage Monitoring Activation call flow.

Figure 212: Usage Monitoring Activation Call Flow

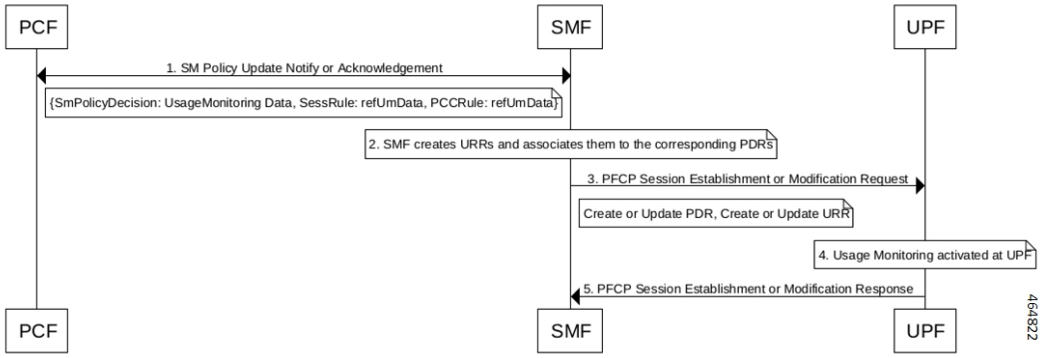


Table 370: Usage Monitoring Activation Call Flow Description

Step	Description
1	PCF sends the list of Usage Monitoring data with thresholds to be monitored and association of the thresholds to either Session or PCC rule level.
2	SMF creates the URR for each monitoring data and associates it to the corresponding PDRs.
3	SMF sends Create or Update URR and links the URR with the corresponding PDR in PFCP Session Establishment or Modification request.
4	UPF activates the monitoring on the received URR.
5	UPF sends the response to SMF with the corresponding cause code.

Usage Reporting Call Flow

This section describes the Usage Reporting call flow.

Figure 213: Usage Reporting Call Flow

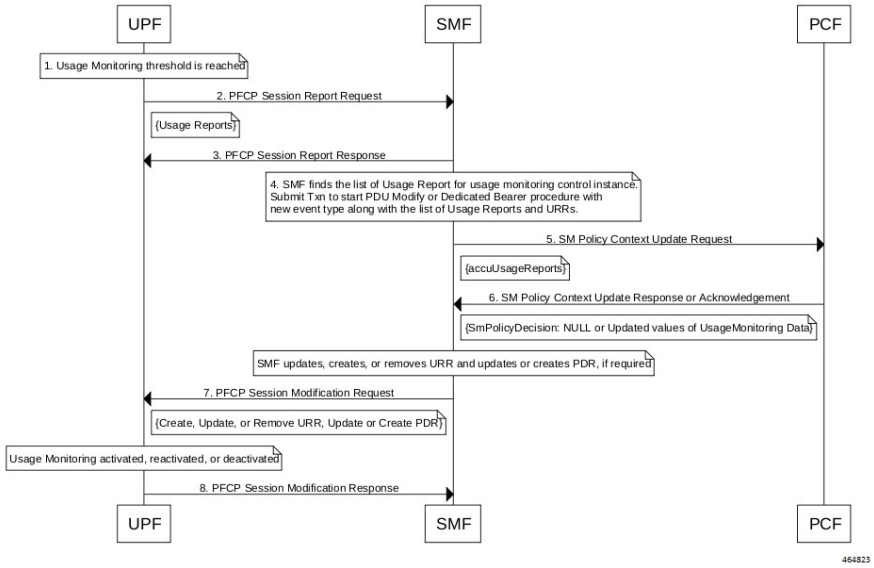


Table 371: Usage Reporting Call Flow Description

Step	Description
1	On UPF, the configured usage monitoring threshold limit reaches.
2	UPF sends the PFCP Session Report Request along with the usage information for the URR to SMF.
3	SMF sends PFCP Session Report Response with Cause: PFCP Cause Request Accepted.
4	SMF sends the received usage information to PCF in the Policy Update Request.

Step	Description
5	PCF acknowledges with either updated threshold for monitoring or none to SMF. In case of none, monitoring to SMF is disabled.
6	SMF removes or updates the corresponding URR and sends the modification request to UPF.
7	UPF deactivates or reactivates the monitoring based on the received information.
8	UPF sends the acknowledgment response with the corresponding cause code to SMF.

Standards Compliance

The usage monitoring over PCF feature complies with the following standards.

- *3GPP TS 29.512 version 16.5.0 Release 16—5G; 5G System; Session Management Policy Control Service*

Limitations

This feature has the following limitations:

- If you have enabled the PCC Rule level monitoring, then by default this monitoring gets linked with the URR of the refUmData that is associated with the PCC rule and Session level URR, if exists. The linking exists until PCF excludes it from the session level monitoring in "exUsagePccRuleId".
- While the usage monitoring is in progress, any update of parameters from PCF for a Session or PCC rule without refUmData implies disabling or removal of usage monitoring for that rule. This rule must always include the refUmData even if no change exists.
- SMF doesn't honor the usage report received from UPF after SMF notifies the usage report to PCF and PCF responds with 204—No Content (PCF disables the usage monitoring). In this case, SMF notifies only the UPF with the remove URR for the disabled UmId and locally discards any received usage report.
- By default, SMF links the URR, if it exists, of the Session level to all the active static rules as part of the session. As no URR information exchange happens for static rules between SMF and UPF, the UPF is responsible to monitor the static rules data usage as part of the PDU and Session level monitoring. Then, UPF sends the response to SMF through the Usage report.

Configuring Usage Monitoring Key for Pre-defined Rules

To configure the usage monitoring key for pre-defined rules, use the following sample configuration:

```
config
   active-charging service  service_name
      rulebase  rulebase_name
         action priority  priority_name dynamic-only ruledef  ruledef_name
charging-action  charging-action_name umid  usage-monitoring_identifier
         end
```

NOTES:

- **umid** *usage-monitoring_identifier*: Specify the usage monitoring identifier. The *usage-monitoring_identifier* must be a string.

Note You can associate the usage monitoring identifier for pre-defined rules by local configuration in the **action priority** *priority_name* **dynamic-only ruledef** *ruledef_name* command. After PCF activates this rule, the SMF fetches usage monitoring thresholds that SMF receives from PCF. SMF creates the URR and associates it with the created PDRs of the pre-defined rules and then sends them to UPF. Then, UPF honors these URR and reports the usage back to SMF.

Configuration Verification

To verify the configuration, use the following command:

show running-config active-charging service *active-charging_service_name* **rulebase** *rulebase_name* **action priority** *action_priority* **dynamic-only ruledef**

If the usage monitoring key is configured, then the value appears as part of the **umid** configuration in the following output.

```
show running-config active-charging service acs1 rulebase rba1
   active-charging service acs1
      rulebase rba1
        action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1

        action priority 2 dynamic-only ruledef rda1 charging-action ca1 description myrule2
 umid 54
        action priority 3 dynamic-only ruledef rda3 charging-action ca3 description myrule3

      exit
     exit
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Usage Monitoring Statistics

The SMF-Service (smf-service) pod supports the following statistics:

PolicyPcfUpdatesTotal

- Description: Display the number of times Usage Report sent towards PCF.
- Metrics-Type: Statistics
- Labels:
  - Label: **smf_current_procedure**
    - Description: Display the current running procedure.
    - Value: PDU Session Modify – PCF-initiated or PDN Session Modify—Bearer Add, Delete, or Modify

  - Labels:

- Label: **trigger**
  - Description: Displays the trigger for the procedure initiated at SMF
  - Value: usage_report

QoS Group of Ruledefs Support over N7

Feature Description

The QoS Group of Ruledef feature enables the PCF to define and enforce Fair-Usage-Policy (FUP) per subscriber. This feature enables changing certain charging-action parameters and all QoS-of-ruledefs parameters per individual subscriber session.

QoS Group of Ruledefs is also called as QGR.

The following attributes of QoS-group-of-ruledefs are supported:

- Precedence or Priority: Priority of a QoS-group-of-ruledefs implies priority of applying QoS-parameters of a QoS-group-of-ruledefs to an incoming data packet. If a packet matches a ruledef which is part of multiple QoS-groups activated for the session, then QoS parameters of the QoS-group-of-ruledefs with highest priority (precedence) is applied to the packet. A lower priority number indicates higher priority of application of QoS parameters of that group. Priority of a QoS-group-of-ruledefs is set by PCF for each subscriber session.
- Flow-Status: Describes whether the IP flows are enabled or disabled. Possible values are:
  - Enabled uplink
  - Enabled downlink
  - Enabled
  - Disabled
  - Removed

  Default value is Enabled.

Note Attributes of QosGroupRuleDefs IE cannot be defined using CLI commands. These attributes can only be set and changed by PCF.

Individual ruledefs cannot be dynamically added or removed from a predefined QoS-group-of-ruledefs received over the N7 interface.

How it Works

This section describes how the QoS Group of Ruledef feature is implemented.

UPF provisions the configuration of QoS-group-of-ruledefs under the Active Charging Service (ACS). The CLI allows addition and removal of charging and dynamic ruledefs to a named QoS-group-of-ruledefs. A single ruledef can be part of multiple QoS-group-of-ruledefs. In this scenario, a QGR with higher priority is enforced or considered, where priority is communicated through Precedence IE by PCF over N7 interface.

PCF is aware of the names of all QoS-group-of-ruledefs and their related ruledefs configured on SMF. The PCF activates and removes QoS-group-of-ruledefs for a subscriber session using proprietary AVP in N7 message. This AVP specifies the name of the QoS-group-of-ruledefs to activate or to remove.

A subscriber may not have any QoS-group-of-ruledefs activated. Incoming traffic may match a ruledef, which has no associated QoS-group-of-ruledef for that subscriber session. In that case, action is taken based only on the configuration for that ruledef.

QGR Processing Flow

The following is the QGR processing logic at UPF.

- On receiving a IE ‘Qos-Group-Of-Ruledef', search for the QGR in static configuration. For each ruledef or group-of-ruledef in QGR, look up for its corresponding PDR and update the FAR and QER list with the received QGR FAR and QER IDs.
- For each ruledef or group-of-ruledef PDR on UPF, associate high priority QGR’s FAR-ID and QER-ID.
- Maintain QGR map at both SMF and UPF. It consists of QGR name, precedence, QER-ID, and FAR-ID. Use QGR map for recovery and lookup whenever required.

QGR Parameters

The SMF sends the QGR parameters in Session Establishment or Modification Request to UPF through N4 interface.

QGR Name and Precedence is sent in a custom IE "QGR-INFO-LIST". Flow-action and bandwidth parameters create a new FAR and QER respectively.

Any changes to QGR dynamic parameters trigger an update to FAR and QER.

This IE is sent in Session Establishment or Modification Request.

QGR IE

```
Qos-Group-Of-Ruledef:
Name:
Operation:  (0 – Add  1 - Modify 2 - Delete)
Precedence:
FAR ID:
QER ID:
```

Custom IEs at UPF

This section lists the custom IEs that are available at UPF.

Extended Apply Action

The Extended Apply Action IE indicates the action(s) the UPF is required to apply to packets. It is coded as shown in the following figure.

Figure 214: Extended Apply Action IE

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **200** (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	TERMFLOW	DL DROP	UL DROP

523029

The octet 5 is encoded as follows:

- Bit 1 – UL DROP (Drop Uplink): when set to 1, this indicates a request to drop uplink packets.
- Bit 2 – DL DROP (Drop Downlink): when set to 1, this indicates a request to drop downlink packets.
- Bit 3 – TERMFLOW (Terminate/Kill Flow) : when set to 1, this indicates a request to terminate the flow.
- Bit 4 to 8 – Spare, for future use and set to 0.

QGR-INFO List

The QGR-INFO List IE indicates the information about the QoS Group received from the PCF to UPF which identifies the flow and applies the received parameters. It is coded as shown in the following figure.

Figure 215: QGR-INFO List IE

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **241** (decimal)							
3 to 4	Length - n							
5 to 6	Number of QGR							
7	Spare	Spare	Spare	Spare	QER	FAR	QGRN	PRECED
8	QGR Operation (ADD = 0/MODIFY = 1/REMOVE = 2)							
9 to 12	QGR Precedence							
13	Length of QGR Name							
14 to n	QGR Name							
n+1 to n+4	FAR ID							
n+5 to n+8	QER ID							
Same as 7 to n+8	Next QGR Details (if any)							

523030

The octet 7 (bit vector for the QGR Information) is encoded as follows:

- Bit 1 – PRECED (Precedence): when set to 1, this indicates precedence is present.
- Bit 2 – QGRN (QGR Name): when set to 1, this indicates QGR Name is present.
- Bit 3 – FAR : when set to 1, this indicates FAR ID is present.
- Bit 4 – QER: when set to 1, this indicates QER ID is present.
- Bit 5 to 8 – Spare, for future use and set to 0.

SMF encodes the QGR information based on this bit vector field.

Burst Size

The Burst Size IE indicates the information about the UL and DL burst size for MBR to UPF. It is coded as shown in the following figure.

Figure 216: Burst Size IE

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **176** (decimal)							
3 to 4	Length - n							
5 to 8	UL Burst Size							
9 to 12	DL Burst Size							

523031

Conform Action

The Conform Action IE indicates the action(s) the UPF is required to apply to packets for both UL and DL. It is coded as shown in the following figure.

Figure 217: Conform Action IE

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **177** (decimal)							
3 to 4	Length - n							
5	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
6	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
7	UL Tos							
8	DL Tos							

523032

Exceed Action

The Exceed Action IE indicates the action(s) the UPF is required to apply to packets for both UL and DL. It is coded as shown in the following figure.

Figure 218: Exceed Action IE

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = **178** (decimal)							
3 to 4	Length - n							
5	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
6	Spare	Spare	Spare	Spare	Spare	MARK-DSCP	DROP	ALLOW
7	UL Tos							
8	DL Tos							

523033

The following tables provide information on the custom IEs included in the N4 messages.

Table 372: FAR Format

FAR ID	Unique ID
Extended Apply Action	Private IE to include Flow-Action Allow as well Discard Uplink, Discard Downlink, and Terminate Flow. The value of Extended Apply Action is derived from FlowStatus IE value received in QosGroupOfRuledef IE from PCF.

Table 373: QER Format

QER ID	Unique ID
Maximum Bitrate	MBR of QGR in Kbps. • UL MBR • DL MBR
Burst Size	Private IE to include the burst size. • UL Burst • DL Burst
Conform Action	Private IE to configure the conform action. • Uplink Action • Uplink ToS • Downlink Action • Downlink ToS
Exceed Action	Private IE to configure the exceed action. • Uplink Action • Uplink ToS • Downlink Action • Downlink ToS

Custom IEs at PCF

The PCF sends the custom IE "QosGroupRuleDefinition" in SmPolicyDecision attribute to the SMF. This IE comprises QosGroupRuleName, refQosGroupQosData, FlowStatus, and Precedence attributes.

PCF triggers “Add/Update QGR” by sending QosGroupRuleName as key and QosGroupRuleDefinition as value (with all attributes) in QGRDefs map.

For QGR removal, PCF triggers “Remove QGR” by sending QosGroupRuleName as key and the value is set to NULL.

The following tables list the custom IEs that are sent by the PCF.

Table 374: SmPolicyDecision Attribute

Attribute name	Data type	P	Cardinality	Description	Applicability
qosGroupQosData	Map(QosGroupQosData)	O	1..N	A map of qosGroupQosInfo with the content being the QosGroupQosData.	qosGroupQosInfo
qosGroupRuleDefs	Map(QosGroupRuleDef)	O	1..N	A map of QosGroupOfRuledefs with the content being the QosGroupRule Definition.	

Table 375: QosGroupRuleDef Attribute

Attribute name	Data type	P	Cardinality	Description	Applicability
qosGroupRuleId	string	M	1	Uniquely identifies the Qos Group of Ruledef (QGR) configured at SMF	
refQosGroupQosData	string	M	1	A reference to QosGroupQosData	
flowStatus	FlowStatus	O	0..1	Describes whether the IP Flows are enabled or disabled. Possible values: Enabled uplink, Enabled downlink, Enabled, Disabled, Removed Default value "Enabled" is applied.	
precedence	Uinteger	M	0..1	Describes the priority of the Qos Group of Ruledef identified with QosGroupRuleName.	

Table 376: QosGroupQoSData Attribute

Attribute Name	Data type	P	Cardinality	Description	Applica
qosId	String	M	1	Univocally identifies the QoSGroupQosData	

maxbrDL	BitRateRm	M		Indicates the maximum bandwidth in downlink.	
maxbrUL	BitRateRm	M		Indicates the maximum bandwidth in uplink.	
mbrBurstSizeUL	MaxDataBurstVol	O		Describes the amount of data that can be sent at peak rate in uplink	
mbrBurstSizeDL	MaxDataBurstVol	O		Describes the amount of data that can be sent at peak rate in downlink	
mbrConformActionUL	RateLimitAction	O		Describes the ratelimiting action to be taken as long as traffic stays within maxbitrate in uplink.	
mbrConformActionDL	RateLimitAction	O		Describes the ratelimiting action to be taken as long as traffic stays within maxbitrate in downlink.	
mbrExceedActionUL	RateLimitAction	O		Describes the ratelimiting action to be taken if traffic exceeds maxbitrate in uplink.	
mbrExceedActionDL	RateLimitAction	O		Describes the ratelimiting action to be taken if traffic exceeds maxbitrate in downlink.	

Table 377: RateLimitAction Attribute

Attribute Name	Data type	P	Cardinality	Description	Applicability
action	Action	M		Describes the ratelimiting action. Enum Action with possible values: ALLOW, DROP,MARK_DSCP	
tosTrafficClass	string	C		Contains the IPv4 Type-of-Service and mask field or the IPv6 Traffic-Class field and mask field. tosTrafficClass IE is present only in case action IE has value MARK_DSCP.	

Data Path Enforcement

The following is the sequence for the data traffic enforcement performed at UPF.

1. Verify whether the incoming data traffic matches the http ruledef.
2. Check if there is a QGR with the matched ruledef or group of ruledefs. If a match is found, the highest priority QGR is returned.

Note The ruledef or group of ruledefs can be either static or predefined.

3. If the QGR matches, then Flow-Action enforcement is first performed at Charging-Action level and then at QGR level assuming Charging-Action has allowed the packet. If the packet is dropped, then QGR-level Flow-Action enforcement is skipped.
4. If Flow-Action at QGR allows the packet to pass, then the Bandwidth Limiting or QoS Enforcement Rule (QER) Limiting is enforced on the data packet. If it is dropped at QGR, QER Limiting is skipped.
5. Unlike the Flow-Action enforcement, the QER Limiting is also performed first at Charging-Action Level and then at the QGR subject to packet being allowed at Charging-Action.

Call Flows

This section describes the key call flows for this feature.

QoS Group of Ruledef Activation Call Flow

This section describes the call flow associated with the activation of QoS Group of Ruledefs.

Figure 219: Qos-Group-of-Ruledef Activation Call Flow

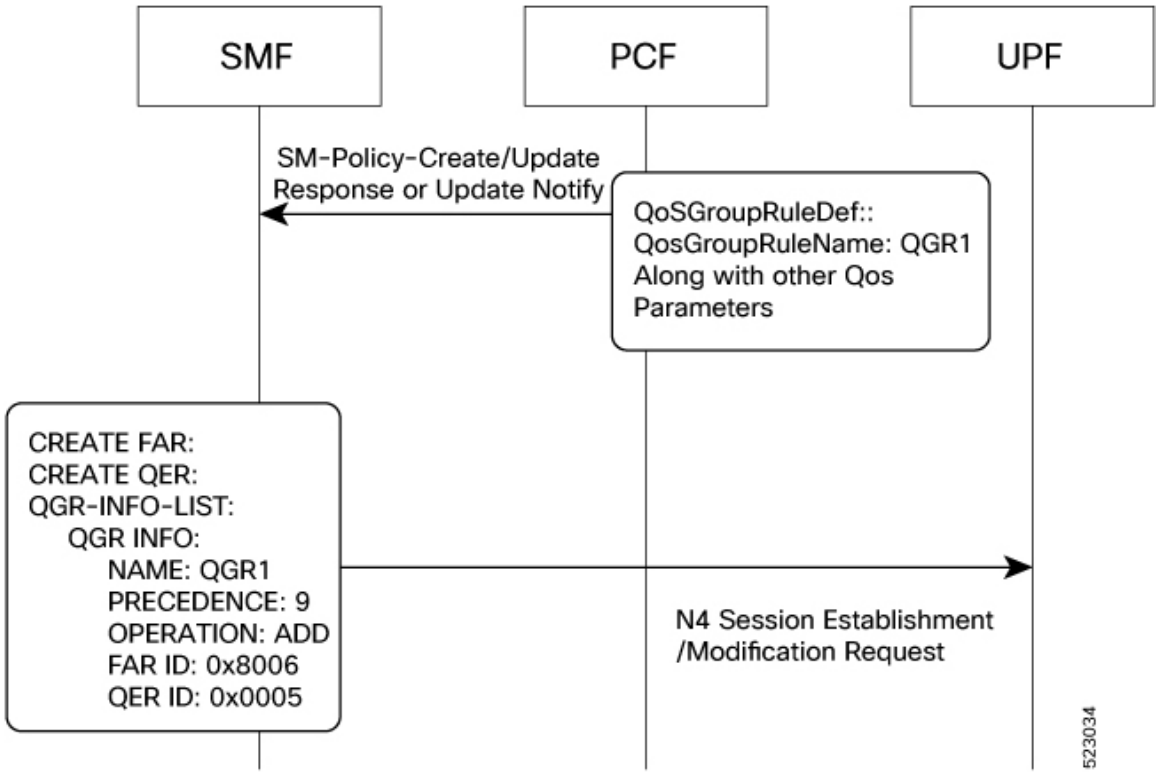


Table 378: Call Flow Description for Activation of QoS Group of Ruledefs

Step	Description
1	PCF activates the qos-group-of-ruledefs through the custom IE 'QosGroupRuleDefs' received in N7 messages. The QosGroupRuleDefs IE comprises QosGroupRuleName, refQosGroupQosData, FlowStatus, and Precedence. PCF triggers "Add QGR" by sending QosGroupRuleName as key and QosGroupRuleDef as value (with all attributes) in QGRDefs map. PCF sends the QosGroupRuleDefs IE to the SMF through N7 Policy association establishment response or policy association update request message.
2	The SMF prepares Create FAR and QER for each QGR received from PCF and encodes QoS group names along with the corresponding FAR IDs and QER IDs in QGR-INFO-LIST IE to be sent on N4 interface session establishment or modification request.

QoS Group of Ruledef Modification Call Flow

This section describes the call flow associated with the modification of QoS Group of Ruledefs.

Figure 220: Qos-Group-of-Ruledef Modification Call Flow

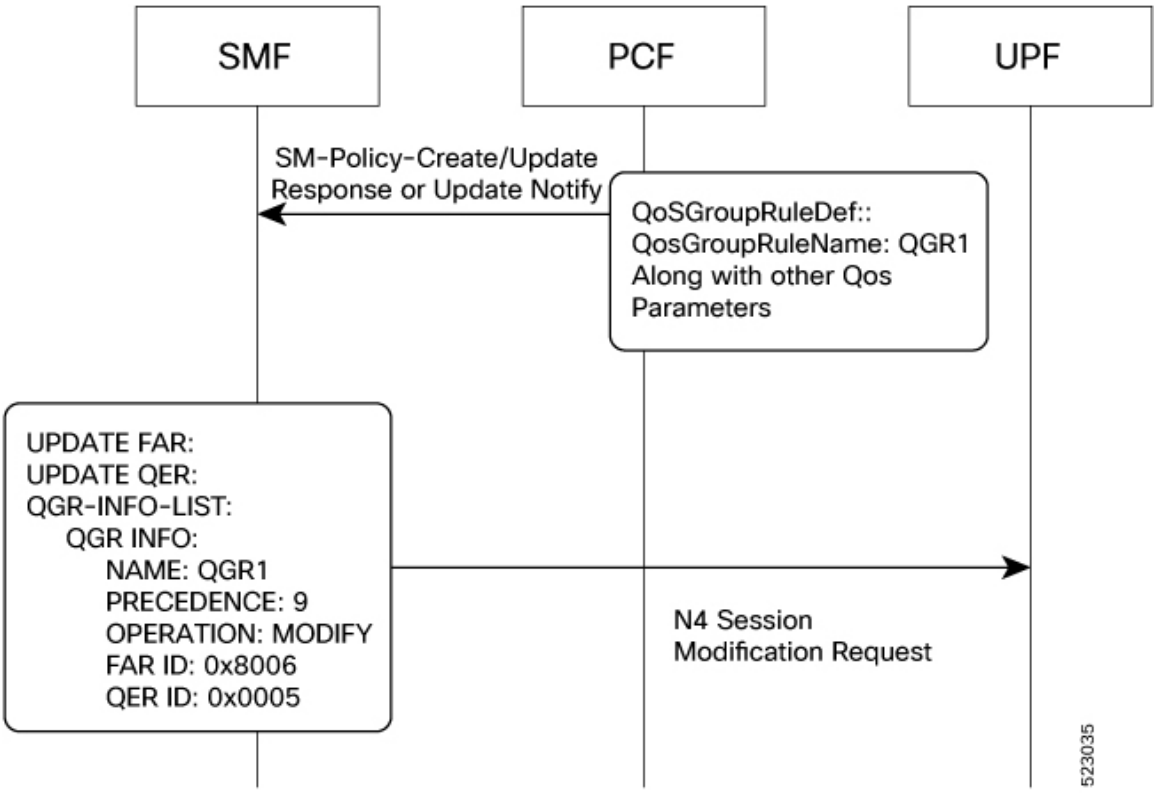


Table 379: Call Flow Description for Modification of QoS Group of Ruledefs

Step	Description
1	Once qos-group-of-ruledefs is activated, PCF modifies the QoS parameters through 'QoSGroupRuleName' IE sent in SM policy association establishment response and SM policy association update request from N7 messages. PCF triggers "Modify QGR" by sending QosGroupRuleName as key and QosGroupRuleDef as value (with all attributes) in QGRDefs map. PCF sends the QosGroupRuleDefs IE to the SMF through N7 policy association establishment response or policy association update request message.
2	SMF prepares Update FAR and QER for each QGR received for modification and encodes the activated QoS group names along with the corresponding FAR IDs and QER IDs in QGR-INFO-LIST to be sent on N4 session establishment or modification request.

QoS Group of Ruledef Deactivation Call Flow

This section describes the call flow associated with the deactivation of QoS Group of Ruledefs.

Figure 221: Qos-Group-of-Ruledef Deactivation Call Flow

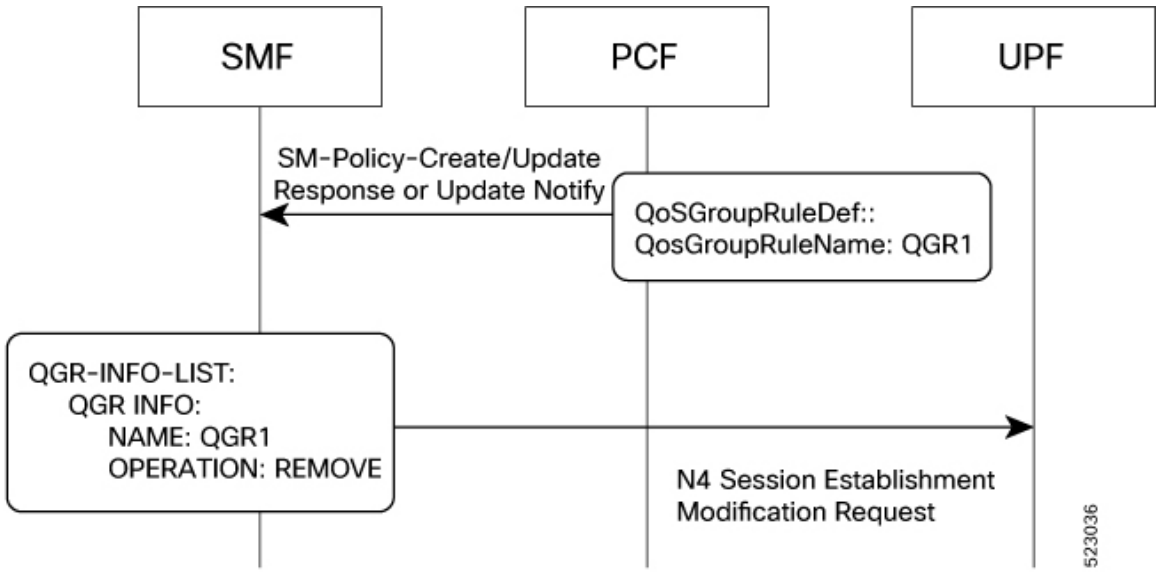


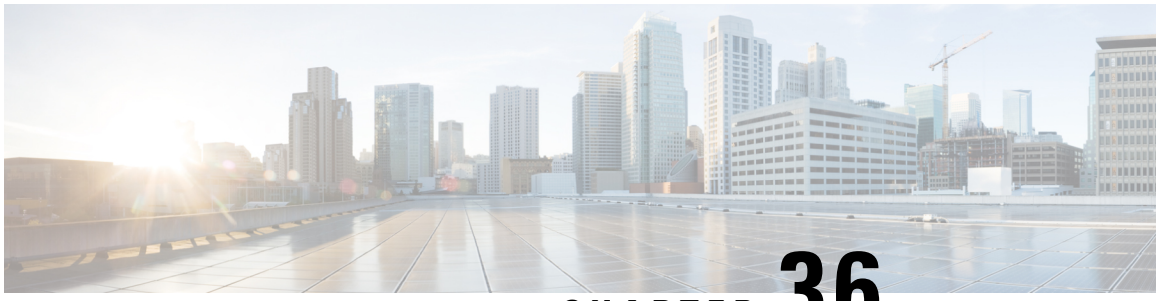
Table 380: Call Flow Description for Deactivation of QoS Group of Ruledefs

Step	Description
1	PCF deactivates qos-group-of-ruledefs through 'QosGroupRuleDefs' IE by sending only the map key which is QosGroupRuledefName with a value as NULL.
2	SMF encodes the deactivated QoS group of ruledef names along with the operation "Remove" in QGR-INFO-LIST to be sent in N4 session modification request.

Limitations

The QoS Group of Ruledefs support feature has the following limitations:

- Monitoring-Key associated with the QGR will not be usage monitored. That is, URR creation and enforcement are not supported.
- PCF will not send the QosGroupRuleDef IE separately. It will be sent along with the PCC rules.
- SMF supports up to a maximum 20 QosGroupRuleDefs. That is, SMF accepts only initial 20 QosGroupRuleDefs from PCF.
- QosGroupRuleDef attribute from PCF will not be ignored if invalid value is received for FlowStatus attribute. FlowStatus will be considered as ENABLED which is the default value of the attribute.



CHAPTER 36

RADIUS Authentication and Accounting

- Feature Summary and Revision History, on page 1109
- Feature Description, on page 1110
- How it Works, on page 1116
- Configuring the RADIUS Client, on page 1138
- RADIUS Client OA&M Support, on page 1157
- Troubleshooting Information, on page 1163

Feature Summary and Revision History

Summary Data

Table 381: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 382: Revision History

Revision Details	Release
Added dynamic configuration change support for the RADIUS endpoint.	2023.03.0
Added the Secure Group Tag support for RADIUS access response attributes.	2023.01.4

Revision Details	Release
Added the support for: • 3GPP dictionary • Allow-auth • Consecutive failure • Max-transmissions	2023.03.0
Added support for interworking with ISE.	2021.02.2.t1.0
Introduced new CLI option in charging profile to generate the RADIUS accounting trigger on TFT change.	2021.02.0
To support instance awareness on RADIUS, the SMF allows: • Instance-level configuration under RADIUS profile • NAS-IP-Address and NAS-Identifier attribute configuration per instance-id in RADIUS profile configuration • RADIUS Disconnect-Request VIP configuration per instance-id in RADIUS endpoint configuration	2021.02.0
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

Remote Authentication Dial-In User Service (RADIUS) is a client and server protocol. The RADIUS client is typically a Network Access Server (NAS) and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts

on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user.

RADIUS provides Authentication and Accounting services to the users. The SMF supports the following configurations:

- Add RADIUS server details.
- Enable RADIUS accounting and authentication.
- Add RADIUS interface as an option for virtual APN configuration within DNN profile.
- Enable CC trigger reporting.
- Define volume and time limits.

The RADIUS client supports the following functions:

- **Server Selection**

  RADIUS servers are configured with IP: Port as the key. The **algorithm** CLI specifies the failover or load-balancing algorithm to select the RADIUS server to which the authentication or accounting request must be sent. Servers that are marked "dead" aren't considered for selection until they are marked "alive". The supported algorithms are first-server and round-robin.

  - First-server—Specifies that the request must be sent to the RADIUS server with the highest priority. If the server becomes unreachable, the request is sent to the server with the next highest configured priority. This is the default algorithm.
  - Round-robin—Specifies that the request must be sent based on load balancing in a circular queue manner. The server that is last used is stored to maintain the round-robin selection. The order of the list is purely based on the configuration sequence.

- **Monitor Server and Dead Server Detection**

  The Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead. The two different parameters that you can set up to identify a dead server are as follows.

  - **Response-timeout**: Monitor Server revisits the server database and marks the server which hasn't received response beyond the configured "response-timeout" value after the first request is sent. The server is marked "dead" and remains in dead-state for minutes configured as "deadtime". After the "deadtime" elapses, the server's dead-variable is reset again to mark it as ready to process requests. If the server is still not reachable, it's marked "dead" as part of the next request response timeout.
  - **Consecutive failures**: Consecutive failure helps to configure the number of consecutive timeouts that must occur on the server before the RADIUS server is marked as dead. Whether a request is a retry request or a regular request, the failure count increments when server doesn't return any response (i.e request timeout). When the failure count of the server reaches the threshold for consecutive failures, the server is declared as dead server.

- **Timeout and Retry**

  After a server is selected and a request is sent to the server, an entry is maintained in the request queue until response is received from the RADIUS server or until timeout occurs. Monitor Requests is called to check on the requests queue for response timeouts and retry. It walks through all the entries and checks if any request timeout value configured as "timeout" is hit. For such requests, if the number of retries is less than the configured "max-retries" value, the request is resent to the RADIUS server. Else, if the

"max-retries" count is reached, the request is deleted from the request queue. After a request is deleted, even if response comes for such requests, the response is discarded and not sent to the user.

- **Max transmission**

  Max transmission helps to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available, or if the maxtransimissions limit is reached, then the timeout response is sent.

  Example: If max-transmissions value is set to 5, max retry value is 2, and there are two servers available. So there are three attempts (one actual attempt and two retries) on the first server, and the remaining 2 (1 actual and one retry) on the second server.

RADIUS Authentication

Authentication and key management are fundamental to the security of mobile networks because they provide mutual authentication between users and the network.

5G defines various authentication methods to authenticate a user. In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI), and key agreement between the UE and the network using the primary authentication mechanism.

For information on enabling the RADIUS Client feature, see Configuring the RADIUS Client, on page 1138.

Identity Services Engine

Identity Services Engine (ISE) is a common point of policy definition for 5G and other enterprise devices. In 5G as a Service (5GaaS) architecture, ISE conducts only the authorization and accounting. The Control Center handles the 5G authentication. You can implement the 5G authorization with the RADIUS Authorize-Only flow.

SMF supports communication with ISE for Cisco private 5G. Based on the policies that SMF receives from ISE, Cisco private 5G supports various behaviors on the enterprise side. ISE provides a mechanism for the enterprise customers to perform tasks, such as identifying the subscriber, define groups for the subscribers, and assign policy.

Allow-auth

If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

Throughput Limiting

If you have configured a secondary authentication on the SMF, then the SMF sends the RADIUS access request to ISE based on the configured RADIUS server address. SMF includes PEI in the access request, if available. The configured IMEI-based ISE includes the name of the rule that is to be applied on the private 5G network to achieve the throughput limiting.

Note Throughput limiting can use either IMEI or IMSI.

ISE populates the rule name in the 3GPP-Policy-Reference attribute in the access accept request. You can configure this rulebase in SMF. SMF derives the ASCII value from the octet string included in the 3GPP-Policy-Reference attribute. Then, SMF matches this value with the configured rulebase.

Following table lists the octet values for the 3GPP-Policy-Reference AVP.

Table 383: 3GPP-Policy-Reference AVP

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP Type = 113							
2	3GPP Length = m							
3-m	Policy Data Reference (octet string) **Note** DN AAA sends the policy data reference value. SMF uses this value to retrieve the SM and QoS policy data in the PCF.							

The ISE sends the rulebase to SMF. If the SMF receives the rulebase that is not configured, then the SMF ignores it. If you have not configured the default bandwidth policy on SMF, then the bandwidth policy is ignored.

You can configure the bandwidth limit on SMF when a UE attaches through the 4G RAT or 5G RAT. Based on the bandwidth limit configured through the 4G RAT, the SMF populates the BearerQoS value in the Create Session response. Based on the bandwidth limit configured through the 5G RAT, the SMF populates the QosFlowDescription value in the N1 PDU Establishment Accept request.

Bandwidth limiting is configured locally on UPF based on the predefined rule that SMF sends.

RADIUS Accounting

Accounting collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities the start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access and the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

The SMF implements the RADIUS Accounting functionality through the use of CLI configuration. For more details on the configuration, see Configuring the RADIUS Client, on page 1138.

If the RADIUS accounting is enabled and server-group is configured within the DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment request. When the SMF sends AAA group which is not present on UPF, then it does not account the traffic for static and predefined rules in RADIUS URR and fails to report. In this scenario, the SMF considers only the dynamic rules traffic for accounting in the RADIUS URR.

Handling RADIUS Disconnect Request Messages

Dynamic Authorization Client (DAC) sends Disconnect-Request packet to RADIUS endpoint (radius-ep) through UDP port. DAC sends this packet to terminate the user session(s) on Network Access Server (NAS). It also discards all the associated session contexts.

The Disconnect-Request packet contains the following session identification attributes to identify the sessions to be terminated.

- 3GPP-IMSI + 3GPP-NSAPI
- ACCT-SESSION-ID
- CALLED-STATION-ID (DNN) + FRAMED-IP-ADDR
- CALLED-STATION-ID (DNN) + FRAMED-IPV6-PREFIX

The RADIUS endpoint validates the Disconnect-Request packet. If the validation fails, the endpoint rejects the packet and sends Disconnect-NAK message with appropriate cause code to DAC. If the validation is successful, the endpoint performs affinity lookup based on the session identification keys or attributes. Then, the endpoint forwards the Disconnect-Request packet to the particular SMF service instance. The SMF processes the packet and triggers pdu-release or pdn-disconnect procedure. The SMF sends the Disconnect ACK response with the appropriate cause code if the session is identified, removed, and no longer valid. The SMF sends a Disconnect-NAK message with appropriate cause code if the session context is not found. The SMF does not wait for the completion of release procedure to send the Disconnect ACK or NAK response.

In the roaming scenario, the RADIUS Disconnect-Request is supported for home-routed subscribers when the roaming status is roamer. The hSMF acts as the SMF service and initiates the session release procedure.

Note Roaming with 4G and EpsInterworkingIndication is not supported. Hence, a combination of IMSI and NSAPI keys is not supported.

This feature uses a combination of the session identification keys or attributes to identify the sessions for termination.

Important If multiple key combination is provided for the same session, it is accepted. However, if the multiple key combination leads to multiple session contexts or non-existing session context, the behavior is non-deterministic.

The SMF supports only one session context per Disconnect-Message (DM) request. The SMF supports the following attributes in the DM request to identify the NAS and the user sessions to be terminated.

Attribute	Reference Specification	Encoding Type
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10 3GPP 29.561 – 11.3	String
Accounting-Session-Id	RFC 2866	String
FRAMED-IP	RFC 2865 - 5.1	IPv4 Address

Attribute	Reference Specification	Encoding Type
FRAMED-IPV6-PREFIX	RFC 3162	PrefixLen and String
CALLED-STATION-ID (DNN)	RFC 2865 - 5.30	String
NAS-IP-Address	RFC 2865 – 5.4 (optional)	String
NAS-Identifier	RFC 2864 – 5.32 (optional)	String

The SMF silently discards other attributes present in the DM request if the packet decoding is successful.

The SMF supports the following attributes in the DM ACK or NAK response.

Attribute	Reference Specification	Encoding Type
ERROR-CAUSE	RFC 5176 – 3.5	Integer
REPLY-MESSAGE	RFC 2865 – 5.18	String

The RADIUS endpoint pod supports the following error codes if the Disconnect Request is rejected by radius-ep:

- 402 (Missing Attribute) - Triggered due to invalid key combination
- 403 (NAS Identification Mismatch) - Triggered if NAS-IP attribute in DM request does not match the endpoint COA-NAS VIP-IP or if NAS-Identifier attribute in the request does NAS identifier configuration within RADIUS Dynamic Authorization or CoA configuration
- 407 (Invalid Attribute) - Triggered due to format error, encode error, and so on
- 405 (Unsupported Service) - Triggered if the request is not a disconnect request
- 503 (Session Context Not Found) - Triggered if the session cannot be located

For more information on configuring this feature, see the Configuring the Session Disconnect Feature, on page 1155 section.

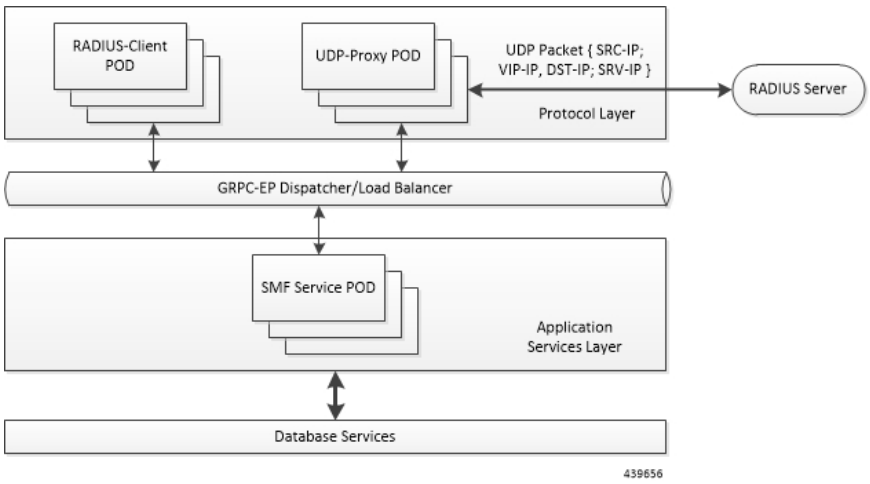
Architecture

RADIUS Client Integration in SMF

The RADIUS client pod resides in the protocol layer of the 5G architecture.

The following figure illustrates the integration of RADIUS Client in SMF.

Figure 222: RADIUS Client Integration



Radius-EP App (RADIUS-Client Pod)—The RADIUS Client functionality is added in a new pod. It handles RADIUS protocol-specific functions, such as authentication and accounting.

SMF Service App (SMF Service Pod)—The SMF Service App provides PDU session service. During session establishment, the SMF service decides if the secondary authentication is required or not, and acts accordingly.

UDP-Proxy App (UDP-Proxy Pod)—The UDP-Proxy App is enabled with host-networking and, communicates the packets using external Virtual-IPs. All RADIUS packets are transmitted and received from an outside cluster using this application.

How it Works

This section describes how the SMF supports RADIUS authentication and accounting functionality.

RADIUS Interaction for Authentication

The RADIUS server supports various methods to authenticate the user. When the server is provided with the username and original password of the user, it can support Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MSCHAP), UNIX login, and other authentication methods.

The SMF supports user authentication using PAP, CHAP, or MSCHAP protocol. The SMF configuration aids in the protocol selection for the user authentication. If the secondary authentication is enabled in DNN profile, the SMF interacts with the RADIUS server to perform RADIUS authentication. To implement the authentication, the RADIUS client residing within the SMF sends the User-Name and User-Password attributes in Access-Request message to the RADIUS server.

The SMF uses more attributes to facilitate the RADIUS authentication function. For the complete list of attributes supported, see the RADIUS Attribute Definition, on page 1129 section.

The RADIUS server validates the user with the authentication information. If the validation is successful, the server sends the Access-Accept response to the SMF.

PAP, CHAP, MSCHAP-based Authentication

The SMF decodes the Protocol Configuration Options (PCO), Extended PCO (ePCO), or Additional PCO (APCO) IE received from UE. Then, the SMF retrieves the values related to PAP (User Name and Password), CHAP (Challenge and Response), or MSCHAP (Challenge and Response) from the IE. If any of the protocols have higher precedence in configured priority under DNN, the SMF sends the received values in RADIUS Access-Request message to the RADIUS server.

Note The SMF does not include the authentication information received from the UE in the RADIUS Access-Request message if the priority is not configured.

By default, the SMF uses the configured host password under DNN for authentication until additional configuration is enabled to use the password received in PCO, ePCO, or APCO. The SMF allows the operator to configure the host password at DNN profile either in plain-text or encrypted form and always displays the same in encrypted format only wherever applicable.

The SMF sends MSISDN as the User Name if the UE does not provide the username explicitly in PCO IE for PAP-based authentication.

For CHAP-based authentication, the SMF converts the received CHAP Challenge and Response to MSCHAP if the **convert-to-mschap** command option is enabled, CHAP is enabled, and the received CHAP Response length is 49 bytes. By default, the SMF uses MSCHAPv1 as the authentication algorithm.

For MSCHAP-based authentication, the SMF sends User Name, Challenge, and Response received in PCO to the RADIUS server if Protocol ID is LCP and LCP container specifies the algorithm as CHAP/MSCHAPv1 (128) as per RFC 2433 or CHAP/MSCHAPv2 (129) as per RFC 2795.

The SMF forwards the authentication information from RADIUS server to UE in Create-Session-Response PCO/EPCO/APCO IE for a 4G/Wi-Fi session, and in N1 Container EPCO IE for a 5G session.

Consider the following important points while implementing the RADIUS authentication functionality.

- Perform the length validation of different AVPs applicable for this feature based on RFC 2865. Also, reject the authentication if any violation is identified.
  - The minimum length of CHAP Challenge is 5 bytes (even though it is 1 byte as per RFC 1334 and RFC 1994).
- The SMF sends the received authentication information from UE to RADIUS server based on the configured authentication algorithm at DNN level. The SMF does not manipulate any data received from UE and it only applies the configurations related to authentication before sending the information to RADIUS server.
- SMF assigns the IPv4 or IPv6 address to the session and sends FRAMED-IP or FRAMED-IPv6-PREFIX attribute to the RADIUS server through RADIUS accounting messages. RADIUS server uses this attribute information to correlate MSISDN with IP address.
- The SMF does not validate the use case of incrementing the Identifier value for every authentication as it does not allow multiple authentication during the PDU session lifetime.
- The SMF sends the encrypted NULL (empty) password in Access-Request when it receives empty password from UE and no host level password configured at SMF or **password-use-pco** option is enabled.
- The SMF falls back to the default authentication where Access-Request carries the configured server secret as User Password in the following scenarios:

- If none of the algorithm preference is enabled with priority
- If the UE provided information is not applicable for the configured algorithm preferences, if any
- When the UE sends the empty PAP or CHAP containers without any data (the container length is 0)

- The SMF rejects the authentication in the following scenarios:
  - When there is no other algorithm configured for authentication
  - Whenever there is a mismatch in CHAP identifier received in both CHAP Challenge and CHAP Response containers (the SMF currently copies the CHAP-ID from CHAP Challenge container)
    - CHAP-ID in CHAP Password must be taken from CHAP Response as per RFC 2865.
    - Response Identifier must be copied from the Identifier field of the Challenge Response as per RFC 1334.
    - Whenever the validation criteria of the current algorithm fails

- The SMF allows to configure the same priority through CLI for different algorithms because configuring 0 explicitly disables the configuration. In this scenario, any one of the algorithms is considered and the selection is purely implementation dependent. It is the responsibility of operator to ensure different algorithms have different priorities to resolve the conflicts whenever UE sends multiple authentication containers to the SMF.
- The SMF allows to configure the **password-use-pco** option without configuring PAP due to the limitation of Yang defined syntax format. The same is applicable for **convert-to-mschap** option. But the functionality will work only if the corresponding algorithm is enabled with the valid priority.
- By default, the SMF encrypts the operator given Host level password using AES-128-CFB encryption algorithm, if it's a plain-text. It ignores the encryption if the operator gives the already encrypted password which has to meet the AES-128-CFB encryption standard.
- By default, the SMF considers the authentication algorithm as MSCHAPv1(128) whenever the received CHAP Challenge and Response converted to MSCHAP if received CHAP-Response length is 49 bytes and **convert-to-mschap** option is enabled.
- The following are the list of MSCHAP specific AVPs supported at SMF and its RFC references:
  - MSCHAP-CHALLENGE (MSCHAP) RFC2548 Section 2.1.2
  - MSCHAP-RESPONSE RFC2548 Section 2.1.3
  - MSCHAP2-RESPONSE RFC2548 Section 2.3.2
  - MSCHAP-ERROR RFC2548 Section 2.1.5
  - MS-CHAP2-Success (RFC 2548, Section 2.3.3) is not supported as there is no clear information on MS-CHAP success AVP for v1 in RFC 2548.

- When the RADIUS server sends both MSCHAP-Error and Reply-Message AVPs in Access-Reject message, the preference is given to MSCHAP-ERROR while filling the CHAP container for NACK in PCO/APCO/EPCO. MSCHAP-Error is common for both MSCHAPv1 and MSCHAPv2 algorithm and it is encapsulated in the Message field of the CHAP Failure container.

- In MSCHAP, only the authentication functionality is supported.

Important The SMF uses the inbuilt encryption algorithm “AES-128-CFB” for encrypting the host level password (outbound password) provided by NETCONF-YANG data model. The SMF Ops Center creates a global key, for AES-128-CFB encryption, which is used for encrypting the operator given plain-text password. It shares the key with all the pods via SSH for decrypting the encrypted data in the respective pods. The key is exported as a ENV variable “CONFD_AES_KEY” in SMF-SERVICE pod. If the operator wishes to configure the already encrypted password, then the AES-CFB-128 encrypted string should be prefixed with “8” as follows, 8<encrypted-data> to indicate that the given input is already AES-128-CFB encrypted string to NETCONF-YANG model.

For CLI details associated with authentication, see the Configuring the RADIUS Client, on page 1138 section.

RADIUS Authentication Attributes

RADIUS Access Request Attributes

The following table lists the supported attributes in the RADIUS access request message.

Attribute	Reference Specification	Encoding Type
USER-NAME	RFC2865 - 5.1	String
PASSWORD	RFC2865 - 5.2	Encrypted String
CALLING-STATION-ID	RFC2865 - 5.31	String
CALLED-STATION-ID	RFC2865 - 5.30	String
NAS-IP-ADDRESS	RFC2865 - 5.4	IPv4 Address
NAS-IDENTIFIER	RFC2865 - 5.32	String
SERVICE-TYPE	RFC2865 - 5.6	Octets - 4 bytes
FRAMED-PROTOCOL	RFC2865 - 5.7	Octets - 4 bytes
NAS-PORT-TYPE	RFC2865 - 5.41	Octets - 4 bytes
NAS-PORT	RFC2865 - 5.5	Octets - 4 bytes
SERVING-NETWORK-NAME	3GPP TS 29.561 - 16.4.0, RFC2865	String
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String
3GPP-CHARGING-ID	3GPP 29.061 - 16.4.7.2-2	Octets - 4 bytes
3GPP-PDP-TYPE	3GPP 29.061 - 16.4.7.2-3	Octets - 4 bytes
3GPP-CHARGING-GATEWAY-ADDR	3GPP 29.061 - 16.4.7.2-4	IPv4 Address
3GPP-GPRS-NEG-QOS-PROFILE	3GPP 29.061 - 16.4.7.2-5	Special Encoded Octets
	3GPP 29.274 - 8.7	
3GPP-SGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-6	IPv4 Address
3GPP-GGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-7	IPv4 Address

Attribute	Reference Specification	Encoding Type
3GPP-IMSI-MCC-MNC	3GPP 29.061 - 16.4.7.2-8	String
3GPP-GGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-9	String
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10 3GPP 29.561 – 11.3	String
3GPP-SELECTION-MODE	3GPP 29.061 - 16.4.7.2-12	String
3GPP-CHARGING-CHARACTERISTICS	3GPP 29.061 - 16.4.7.2-13	String
3GPP-SGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-18	String
3GPP-IMEISV	3GPP 29.061 - 16.4.7.2-20	String
3GPP-RAT-TYPE	3GPP 29.061 - 16.4.7.2-21	Octet - 1 byte
3GPP-USER-LOCATION	3GPP 29.061 - 16.4.7.2-22 3GPP 29.274 - 8.21-4, 8.21-5 3GPP 38.413 – 9.3.1.7, 9.3.3.10	Special Encoded Octets
3GPP-MS-TIMEZONE	3GPP 29.061 - 16.4.7.2-23	Special Encoded Octets
	3GPP 29.274 - 8.44	
3GPP-NEGOTIATED-DSCP	3GPP 29.061 - 16.4.7.2-26	Octet - 1 byte
CHAP-PASSWORD (CHAP)	RFC2865 – 5.3	String
CHAP-CHALLENGE (CHAP)	RFC2865 – 5.40	String
MSCHAP-CHALLENGE (MSCHAP)	RFC2548 – 2.1.2	String
MSCHAP-RESPONSE	RFC2548 – 2.1.3	Octets
MSCHAP2-RESPONSE	RFC2548 – 2.3.2	Octets
MSCHAP-ERROR	RFC2548 – 2.1.5	String
REPLY-MESSAGE	RFC2865 – 5.18	String

Note The Wi-Fi call attributes are the same as the 4G call.

RADIUS Access Response Attributes

The following table lists the supported attributes in the RADIUS access response message.

Attribute	Reference Specification	Encoding Type
Class	RFC 2865	String
FRAMED-IP	RFC2865 - 5.1	IPv4 Address

Attribute	Reference Specification	Encoding Type
FRAMED-IPv6-PREFIX	RFC3162	PrefixLen and String
Framed-IP-Netmask	RFC 2865	Octet
IDLE-TIMEOUT	RFC2865 - 5.28	Integer
3GPP-POLICY-REFERENCE	3GPP TS 29.061	Octet
MS-Primary-DNS-Server	RFC 2548	Octet
MS-Secondary-DNS-Server	RFC 2548	Octet
SN-VIRTUAL-APN-NAME	Starent Dictionary	Opaque
SESSION-TIMEOUT	RFC2865 - 5.27	Integer
cts:security-group-tag	Cisco Dictionary	Opaque

Note The Wi-Fi call attributes are the same as the 4G call.

For complete description of the RADIUS authentication attributes, see the RADIUS Attribute Definition, on page 1129 section in this guide.

Call Flows

RADIUS Authentication Call Flow

The following figure illustrates the end to end call flow between the SMF server and RADIUS endpoint.

Figure 223: RADIUS Authentication Call Flow

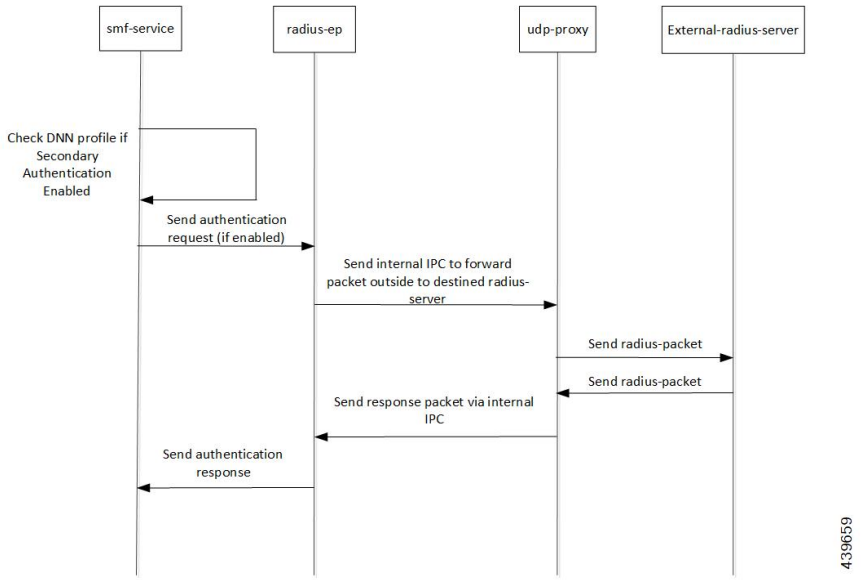


Table 384: RADIUS Authentication Call Flow Description

Step	Description
1	Bringing up RADIUS pod: Add the respective endpoint configuration, with VIP-IP similar to Protocol-EP VIP-IP. Add the RADIUS server information to the RADIUS profile configuration.
2	Add the secondary authentication configuration to the required DNN profiles.
3	During session bringup, the DNN profile checks if secondary authentication is enabled after successful UDM validation. • If authentication is not enabled, continue with PCF. • If authentication is enabled, send inter-process communication (IPC) message to RADIUS pod to authenticate the subscriber.
4	The RADIUS pod prepares the Access Request packet that is destined to a configured RADIUS server, sends the packet to UDP proxy pod to proxy the packet out.
6	The UPD proxy pod creates a socket (if not already present) and sends the packet to the RADIUS server.
7	The RADIUS server validates the Access Request. If accepted, it responds with the Access Accept message. Else, it responds with the Access Reject message.
8	The UDP proxy responds to the respective RADIUS-EP instance.
9	The RADIUS-EP instance validates the response, fetches the framed-IP (if present), and updates the SMF service.
10	The SMF service, upon successful response from RADIUS-EP, continues with the PCF flow. Else, the SMF service disconnects from the subscriber.

RADIUS Interaction for Accounting

The SMF exchanges the following messages with RADIUS server through the RADIUS-client RADIUS-EP.

- Accounting-Request: This message carries any of the following packets to relay the accounting information to the RADIUS server.
  - **Accounting Start packet:** This packet describes the type of service being delivered and the user it is being delivered to.

    The SMF sends accounting-start packet during the session establishment procedure. The RADIUS Accounting server returns an acknowledgement upon receiving the accounting-start packet.

    For details on configuring the RADIUS Accounting, see Configuring the RADIUS Client, on page 1138 section.
  - **Accounting Stop packet:** This packet describes the type of service that was delivered and optionally statistics, such as elapsed time, input and output octets, or input and output packets.

    At the end of service delivery, the SMF sends the accounting-stop packet for all session deletion scenarios and when the RADIUS accounting is enabled during the call setup.
  - **Accounting-Request Interim-Update:** During the session, the SMF sends the updated cumulative usage report to the RADIUS accounting server.

- Accounting-Response: For each successfully processed accounting request, the RADIUS server returns an accounting acknowledgment confirming the receipt of the information.

For CLI details associated with accounting, see the Configuring the RADIUS Client, on page 1138 section.

RADIUS Accounting Attributes

The following table lists the RADIUS accounting attributes supported in the accounting request message.

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
USER-NAME	RFC 2865 - 5.1	String	Start, Stop, Interim update
CALLING-STATION-ID	RFC 2865 - 5.31	String	Start, Stop, Interim update
CALLED-STATION-ID	RFC 2865 - 5.30	String	Start, Stop, Interim update
Class	RFC 2865 - 5.25	String	Start, Stop, Interim update
NAS-IP-ADDRESS	RFC 2865 - 5.4	IPV4 Address	Start, Stop, Interim update
NAS-IDENTIFIER	RFC 2865 - 5.32	String	Start, Stop, Interim update
SERVICE-TYPE	RFC 2865 - 5.6	Octets - 4 bytes	Start, Stop, Interim update
FRAMED-PROTOCOL	RFC 2865 - 5.7	Octets - 4 bytes	Start, Stop, Interim update
FRAMED-IP	RFC2865 - 5.1	IPv4 Address	Start, Stop, Interim update
FRAMED-IPv6-PREFIX	RFC3162	PrefixLen and String	Start, Stop, Interim update
Framed-IP-Netmask	RFC 2865 - 5.9	Octets - 4 bytes	Start, Stop, Interim update
NAS-PORT-TYPE	RFC 2865 - 5.41	Octets - 4 bytes	Start, Stop, Interim update
NAS-PORT	RFC 2865 - 5.5	Octets - 4 bytes	Start, Stop, Interim update
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String	Start, Stop, Interim update
3GPP-CHARGING-ID	3GPP 29.061 - 16.4.7.2-2	Octets - 4 bytes	Start, Stop, Interim update

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
3GPP-PDP-TYPE	3GPP 29.061 - 16.4.7.2-3	Octets - 4 bytes	Start, Stop, Interim update
3GPP-CHARGING-GATEWAY-ADDR	3GPP 29.061 - 16.4.7.2-4	IPV4 Address	Start, Stop, Interim update
3GPP-GPRS-NEG-QOS-PROFILE	3GPP 29.061 - 16.4.7.2-5 3GPP 29.274 - 8.7	Special Encoded Octets	Start, Stop, Interim update
3GPP-SGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-6	IPV4 Address	Start, Stop, Interim update This attribute is not included in the 5G accounting-start message.
3GPP-GGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-7	IPV4 Address	Start, Stop, Interim update
3GPP-IMSI-MCC-MNC	3GPP 29.061 - 16.4.7.2-8	String	Start, Stop, Interim update
3GPP-GGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-9	String	Start, Stop, Interim update
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10	String	Start, Stop, Interim update
3GPP-SELECTION-MODE	3GPP 29.061 - 16.4.7.2-12	String	Start, Stop, Interim update
3GPP-CHARGING-CHARACTERISTICS	3GPP 29.061 - 16.4.7.2-13	String	Start, Stop, Interim update
3GPP-SGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-18	String	Start, Stop, Interim update
3GPP-IMEISV	3GPP 29.061 - 16.4.7.2-20	String	Start, Stop, Interim update
3GPP-RAT-TYPE	3GPP 29.061 - 16.4.7.2-21	Octet - 1 byte	Start, Stop, Interim update

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
3GPP-USER -LOCATION	3GPP 29.061 - 16.4.7.2-22 3GPP 29.274 - 8.21-4 3GPP 29.274 - 8.21-5	Special Encoded Octets	Start, Stop, Interim update
3GPP-MS-TIMEZONE	3GPP 29.061 - 16.4.7.2-23 3GPP 29.274 - 8.44	Special Encoded Octets	Start, Stop, Interim update
3GPP-NEGOTIATED -DSCP	3GPP 29.061 – 16.4.7.2-26	Octet – 1 byte	Start, Stop, Interim update This attribute is sent only if the associated configuration is present.
Acct-Status-Type	RFC 2866	Start/Stop/Interim	Start, Stop, Interim update
Accounting-Session-Id	RFC 2866	String	Start, Stop, Interim update
Acct-Delay-time	RFC 2866	Octet	Start, Stop, Interim update
Acct-Input-Octets	RFC 2866	Integer	Stop, Interim update
Acct-Output-Octets	RFC 2866	Integer	Stop, Interim update
Acct-Input-Gigawords	RFC 2869	Integer	Stop, Interim update
Acct-Output-Gigawords	RFC 2869	Integer	Stop, Interim update
Acct-Input-packets	RFC 2866	Integer	Stop, Interim update
Acct-Output-Packets	RFC 2866	Integer	Stop, Interim update
Acct-Session-Time	RFC 2866	Integer	Stop, Interim update
Acct-Terminate-Cause	RFC 2866	String	Stop
Framed-MTU	RFC 2866	String	Start, Stop, Interim update
3GPP-Session -Stop-Indicator	3GPP 29.061	Bit String	Stop
Framed-Ip-Addr	RFC 2866	IPV4 Address	Start, Stop, Interim update
Acct-Authentic	RFC 2866	String	Start, Stop, Interim update

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
EventTimeStamp	RFC 2869	String	Start, Stop, Interim update

Note The WiFi call attributes are the same as the 4G call.

For complete description of the RADIUS accounting attributes, see the RADIUS Attribute Definition, on page 1129 section in this guide.

Call Flows

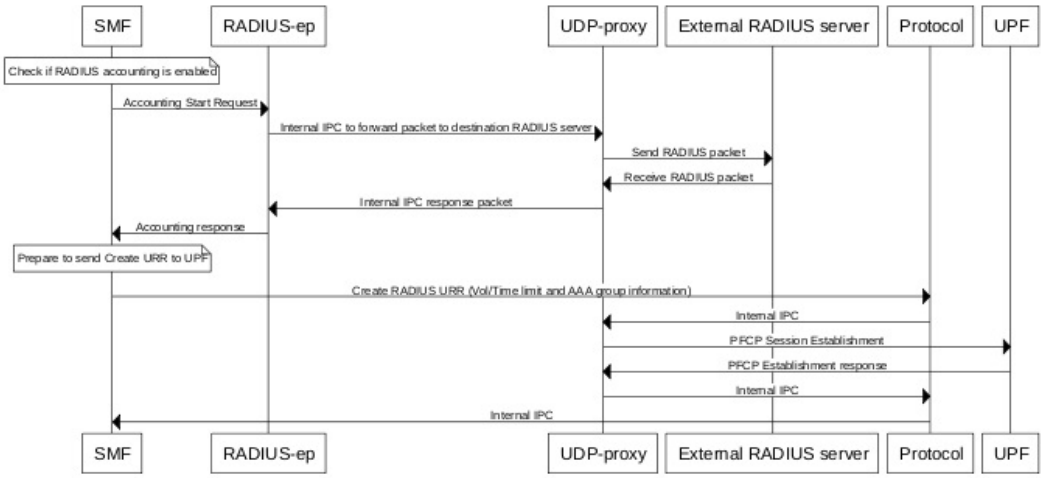
This section describes the following call flows:

- RADIUS Accounting Start Call Flow
- RADIUS Accounting Stop Call Flow
- Asynchronous Accounting Interim-Update Call Flow
- Synchronous Accounting Interim-Update Call Flow, on page 1127

RADIUS Accounting Start Call Flow

This section describes the call flow associated with the initiation of RADIUS accounting procedure.

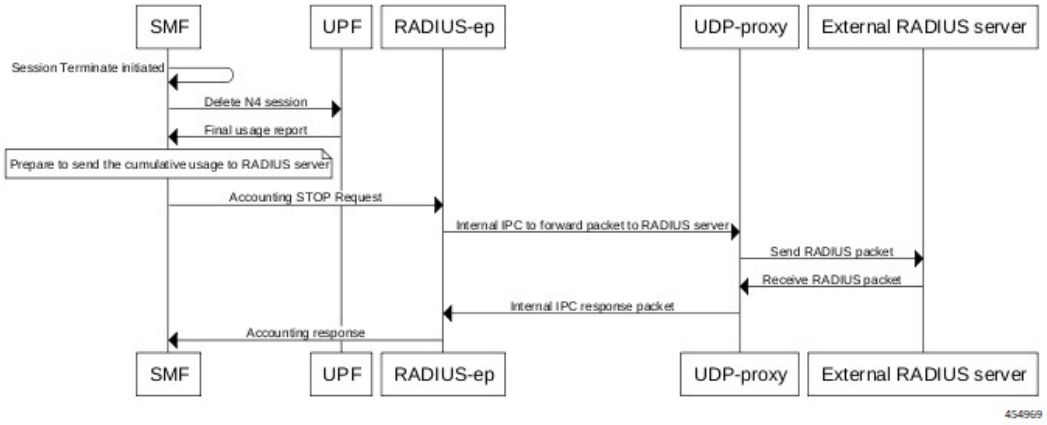
Figure 224: RADIUS Accounting Start Call Flow



RADIUS Accounting Stop Call Flow

This section describes the call flow associated with the termination of RADIUS accounting procedure.

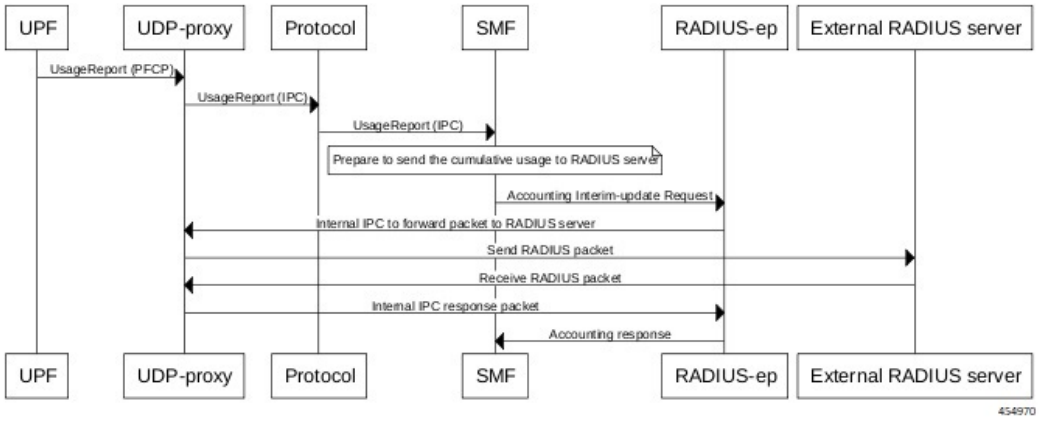
Figure 225: RADIUS Accounting Stop Call Flow



Asynchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the asynchronous interim-update request.

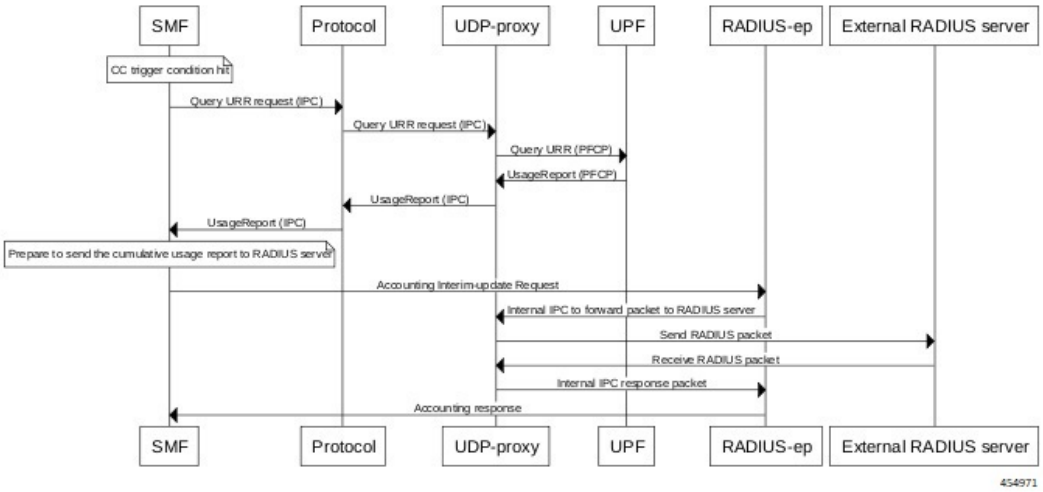
Figure 226: Asynchronous Accounting Interim-Update Call Flow



Synchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the synchronous interim-update request.

Figure 227: Synchronous Accounting Interim-Update Call Flow



Processing of Usage Reporting Rules

After enabling the RADIUS accounting, the SMF creates the Usage Reporting Rule (URR) and relays the rule to the UPF through the Create URR Information Element (IE). The Create URR IE is present in the N4 Session Establishment Request and it contains the volume and time limits as per the configuration.

The SMF associates the RADIUS URR only to the dynamic Packet Detection Rules (PDRs) and not for the static and predefined rules. With AAA group name in N4 session establishment request, the UPF associates the static and predefined PDRs with the RADIUS URR. The UPF sends the usage report for the RADIUS URR when the Volume limit or the Time limit is hit. Then, the SMF sends the usage in the Interim-Update Accounting-Request message to the RADIUS server.

The SMF receives the usage report for RADIUS URR in N4 Modification Response or N4 Deletion Response when any one of the following conditions are met:

- CC event condition is hit and the SMF performs Query URR
- Session Delete Response is sent

The SMF stores the values of Volume and Time thresholds reported for a previous session and reports the cumulative usage by adding the currently reported value to the stored value. The SMF sends the cumulative usage report in Accounting-Request Interim-Update and Accounting-Stop messages.

On receiving the usage report from UPF, the SMF identifies the URR IDs that are to be sent to the CHF server and to the RADIUS server. For example, if the URR ID is associated to “0x80 00 00 09”, then the SMF sends this URR ID to the RADIUS server, and the other URR IDs to the CHF server.

Dynamic Configuration Update

The SMF allows you to change the RADIUS accounting configuration dynamically without impacting the existing sessions.

The following table identifies the impact of dynamic update to the various RADIUS accounting configurations.

Table 385: Dynamic Update of RADIUS Accounting Configuration

Configuration	Dynamic Change	Impact on Existing Sessions
Enabling and disabling of RADIUS accounting configuration	Allowed at the system level	The existing sessions continue to use the old value.
CC trigger updates	Allowed as per current pod replica	The existing session uses the new value.
Volume and time limit changes	Allowed at the system level	The existing sessions continue to use the old value.
Global-level and group-level configurations **Note** If the group-level configuration is unavailable, then by default the system considers the global-level configurations.	Allowed at the system level	The existing request continue to use the old value. New request takes the newly configured values.

RADIUS Attribute Definition

The following section provides a full description of each attribute. The majority of the attribute values are common for the ISE and 3GPP dictionaries. The values are included especially in the attribute description section for the attributes with different attribute values for ISE and 3GPP dictionary:

- USER-NAME

  Description: String value encoded as per RFC 2865.

  - 5G call: GPSI value is used, with stripped-off "msisdn-"
  - 4G call: MSISDN value is used, with stripped-off "msisdn-"
  - The attribute value for 3GPP dictionary is imsi@apn.

Note PAP, CHAP, and MSCHAP authentication methods are not supported in releases prior to 2020.02.x.

In release 2020.02.x and beyond, the PAP, CHAP, and MSCHAP authentication methods are supported.

- PASSWORD

  Description: Encrypted string value encoded as per RFC 2865.

  For both 5G and 4G calls, selected RADIUS server's "secret" is set as user-password.

- CALLING-STATION-ID

Description: String value encoded as per RFC 2865.

5G call: GPSI value is used, with stripped of "msisdn-"

4G call: MSISDN value is used, with stripped of "msisdn-"

- CALLED-STATION-ID

  Description: String value encoded as per RFC 2865.

  For both 5G and 4G calls, DNN value is set as called-station-id.

- NAS-IP-ADDRESS

  Description: IPv4 address value encoded as per RFC 2865.

  For both 5G and 4G calls, user-configured RADIUS Client interface-type's VIP-IP is used.

- NAS-IDENTIFIER

  Description: String value encoded as per RFC 2865.

  For both 5G and 4G calls, user-configured nas-identifier attribute value is used.

- SERVICE-TYPE

  Description: 4-byte octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "FRAMED (2)" value is set.

- FRAMED-PROTOCOL

  Description: 4-byte octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "GPRS-PDP-CONTEXT (7)" value is set.

- NAS-PORT-TYPE

  Description: 4-byte octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, "WIRELESS-OTHER (18)" value is set.

- NAS-PORT

  Description: 4-byte octet (int) value encoded as per RFC 2865.

  For both 5G and 4G calls, the base value of respective instance is used. That is:

  0x4000... 0x407F is set for replica-0

  0x4080... 0x40FF is set for replica-1

- 3GPP-IMSI

  Description: String value encoded as per *3GPP TS 29.061*.

  5G call: SUPI value is used.

  4G call: IMSI value is used.

- 3GPP-CHARGING-ID

  Description: 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

  For both 5G and 4G calls, charging-ID is set.

- 3GPP-PDP-TYPE

Description: 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, pdp-type is set as follows:

- 0 = IPv4
- 2 = IPv6
- 3 = IPv4v6

- 3GPP-CHARGING-GATEWAY-ADDR

  Description: 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

  For both 5G and 4G calls, charging gateway address is set.

- 3GPP-GPRS-NEG-QOS-PROFILE

  Description: Octets (special encoding) value encoded as per *3GPP TS 29.061* and *29.274*.

  For 5G call, the values from default-qos profile of the system are used and the encoding is performed as follows:

Table 386: Non-GBR case

1-2	<Release indicator>- = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL Session-AMBR length (UTF-8 encoded)
10-m	UL Session-AMBR (UTF-8 encoded)
(m+1) - (m+2)	DL Session-AMBR length (UTF-8 encoded)
(m+3) – n	DL Session-AMBR (UTF-8 encoded)

Table 387: GBR case

1-2	<Release indicator> = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL MFBR length (UTF-8 encoded)
10-m	UL MFBR (UTF-8 encoded)
(m+1)-(m+2)	DL MFBR length (UTF-8 encoded)
(m+3)-n	DL MFBR (UTF-8 encoded)
(n+1)-(n+2)	UL GFBR length (UTF-8 encoded)
(n+3)-o	UL GFBR (UTF-8 encoded)

(o+1) – (o+2)	UL GFBR length (UTF-8 encoded)
(o+3) - p	DL GFBR (UTF-8 encoded)

For 4G call, the values from the default-qos profile of the system are used and the encoding is performed as follows:

Table 388: Non-GBR case

1-2	<Release indicator>- = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL Session-AMBR (UTF-8 encoded)
12-15	DL Session-AMBR (UTF-8 encoded)

Table 389: GBR case

1-2	<Release indicator> = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL MBR (UTF-8 encoded)
12-15	DL MBR (UTF-8 encoded)
16-19	UL GBR (UTF-8 encoded)
20-23	DL GBR (UTF-8 encoded)

- 3GPP-SGSN-ADDRESS

  Description: 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

  For 5G call, the AMF address is set.

  For 4G call, the S-GW address is set.

- 3GPP-GGSN-ADDRESS

  Description: 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

  For both 5G and 4G calls, the SMF-Service IP is set.

  For 3GPP dictionary, PGW control IP address as sent in CSRsp.

- 3GPP-IMSI-MCC-MNC

  Description: String value encoded as per *3GPP TS 29.061*.

  For 5G call, SUPIs MCC and MNC values are set.

  For 4G call, IMSIs MCC and MNC values are set.

MCC is first 3 bytes, MNC is next 2 or 3 bytes.

If MCC value is any of the following, then MNC will be of 3 bytes, else MNC will be of 2 bytes.

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

- 3GPP-GGSN-MCC-MNC

  Description: String value encoded as per *3GPP TS 29.061*.

  For both 5G and 4G calls, configured MCC and MNC value of SMF is used.

  MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-SGSN-MCC-MNC

  Description: String value encoded as per *3GPP TS 29.061*.

  For 5G call, AMFs MCC and MNC values are set.

  For 4G call, SGWs MCC and MNC values are set.

  MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-NSAPI

  Description: String value encoded as per *3GPP TS 29.061*.

  For 5G call, QFI value from the defaultQos profile is set.

  For 4G call, EPS bearer ID is set.

- 3GPP-SELECTION-MODE

  Description: String value encoded as per *3GPP TS 29.061*.

  For both 4G and 5G calls, the value is set to "0".

  For 3GPP dictionary, the selection mode value is received in CSReq.

- 3GPP-CHARGING-CHARACTERISTICS

  Description: String value encoded as per *3GPP TS 29.061*.

  For both 4G and 5G calls, generic charging character is set.

- 3GPP-IMEISV

  Description: String value encoded as per *3GPP TS 29.061*.

  For 5G call, PEI value is set.

  For 4G call, IMEI value is set.

- 3GPP-RAT-TYPE

  Description: 1-byte octet encoded as per *3GPP TS 29.061*.

  For 5G call, value "NR (51)" is set.

  For 4G call, value "EUTRAN (6)" is set.

  For WLAN call, value "WLAN (3)" is set.

- 3GPP-USER-LOCATION

  Description: Special octet value encoded as per *3GPP TS 29.061*.

For 5G call, the following encoding logic is used:

1	Location-Type Only TAI = 136 Only NCGI = 135 Both TAI + NCGI =137
2-7	TAI-Encoding (if present)
8-15	NCGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-6	TAC value	

NCGI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	SPARE	NCI
5-8	NR Cell Identifier (NCI)	

For 4G call, the following encoding logic is used:

1	Location-Type
	Only TAI = 128
	Only ECGI = 129
	Both TAI + ECGI =130
2-6	TAI-Encoding (if present)
7-13	ECGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-5	TAC value	

ECGI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	Spare	ECI
5-7	EUTRAN Cell Identifier (ECI)	

- 3GPP-MS-TIMEZONE

  Description: Special octet value encoded as per *3GPP TS 29.061*.

  Timezone string (for example: -07:00+1) is encoded as two-byte value as mentioned in the following table.

1	TIMEZONE The first byte timezone is encoded as per 3GPP 29.061, 3GPP 29.274, 3GPP 24.008, and 3GPP 23.040 (section 9.2.3.11).
2	DAYLIGHT SAVING 0, or +1 or +2 The second byte daylight consists of two bits used (00-0, 01-+1, 10-+2, 11 – Unused).

- 3GPP-NEGOTIATED-DSCP

  Description: 1-byte octet encoded as per *3GPP TS 29.061*

  For both 5G and 4G calls, DSCP configuration from DNN qos-profile configuration is used.

  Sub -> DNN profile -> QosProfile -> DSCPMap -> Qi5 value check -> ARP priority check

- Acct-Status-Type

  Description: Enum value encoded as per RFC 2866. The value of this attribute can be one of the following:

  - 1 - Start
  - 2 - Stop
  - 3 - Interim Update

- Acct-Delay-Time

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of time client is trying to send the accounting record.

- Acct-Input-Octets

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of bytes received. This attribute contains 4 bytes.

  The SMF wraps values when the number crosses the maximum value.

- Acct-Output-Octets

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of bytes transmitted. This attribute contains 4 bytes.

  The SMF wraps values when the number crosses the maximum value.

- Acct-Input-Packets

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of packets received. This attribute contains 4 bytes.

  The SMF wraps values when the number crosses the maximum value.

- Acct-Output-Packets

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of packets transmitted. This attribute contains 4 bytes.

  The SMF wraps values when the number crosses the maximum value.

- Acct-Input-Gigawords

  Description: Integer value encoded as per RFC 2869. This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided. This value is incremented whenever Acct-Input-Octets is wrapped.

- Acct-Output-Gigawords

  Description: Integer value encoded as per RFC 2869. This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 over the course of this service being provided. This value is incremented whenever Acct-Output-Octets is wrapped.

- Acct-Session-Id

  Description: String value encoded as per RFC 2866. This attribute represents the unique accounting ID of subscriber. The accounting ID is unique to make it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct-Session-Id. An Accounting-Request packet MUST have an Acct-Session-Id.

  An Access-Request packet MAY have an Acct-Session-Id; if it does, then the NAS MUST use the same Acct-Session-Id in the Accounting-Request packets for that session. The Acct-Session-Id contains UTF-8 encoded 10646 characters.

- Acct-Session-Time

  Description: Integer value encoded as per RFC 2866. This attribute represents the amount of time the subscriber is active.

- Framed-MTU

  Description: This attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). The default value is 1500.

  It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that value, but the server is not required to honour the hint.

- Acct-Terminate-cause

  Description: Enum value encoded as per RFC 2866. This attribute represents the reason for termination of subscriber.

- FRAMED-IP

  The IPv4 address value decoded as per RFC 2865.

  For both 4G and 5G calls, the received value is set as the IPv4 address for the subscriber.

- FRAMED-IPv6-PREFIX

The IPv6 Prefix + Length value decoded as per RFC 3162.

For both 4G and 5G calls, the received value is set as the IPv6 prefix for the subscriber.

Important If the received prefix-length is !=64, the SMF overrides to 64.

- IDLE-TIMEOUT

  The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

  For both 4G and 5G calls, the received value is used as the maximum number of consecutive seconds of idle time that the user is permitted before being disconnected by the NAS.

- SESSION-TIMEOUT

  The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

  For both 4G and 5G calls, the received value is used as the maximum number of seconds that the user is allowed to remain connected by the NAS.

- 3GPP-Negotiated-QoS-Profile
  - Access-request

    For ISE or default dictionary: ARP PCI and ARP PVI were sent out incorrectly and did not match value received in CSReq. Also APN AMBR was sent out in bps instead of Kbps.

    For 3GPP dictionary: ARP PCI and ARP PVI values are fixed and in sync with what is received in CSReq. Also APN AMBR is sent out in Kbps.

  - Accounting-request

    For ISE or default dictionary: ARP PCI and ARP PVI were sent out incorrectly and did not match value received in CSReq/Gx CCA-I. Also APN AMBR was sent out in bps instead of Kbps.

  - For 3GPP dictionary: ARP PCI and ARP PVI values are fixed and in sync with what is received in CSReq/Gx-CCA-I. Also APN AMBR is sent out in Kbps.

- 3GPP-IMEI-SV
  - Access-request

    For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit imei: 112233445566778.

    For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778.

  - Accounting-request

    For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit IMEI: 112233445566778.

  - For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778.

- 3GPP-UE-Location

- Access-request

  For ISE or default dictionary: ECI value is going as 0.

  For 3GPP dictionary: the value is received in CSReq.

- Accounting-request

  For ISE or default dictionary: For 16 bit IMEI: imeisv-1122334455667788 and for 15 bit IMEI: 112233445566778.

- For 3GPP dictionary: For 16 bit IMEI: 1122334455667788 and for 15 bit IMEI: 112233445566778
  .

Note The WiFi call attributes are the same as the 4G call.

Standards Compliance

The RADIUS Client feature complies with the following standards:

- RFC 2865: RADIUS
- RFC 2866: RADIUS Accounting
- RFC 3162: RADIUS and IPv6
- 3GPP TS 29.061
- 3GPP TS 29.274
- 3GPP TS 29.561, version 16.4.0

Limitations and Restrictions

The SMF has the following limitations:

- The SMF supports only single RADIUS attribute profile, and does not support dictionary selection.
- If RADIUS accounting is enabled and server-group is configured within DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment. The UPF displays an error if there is a server group mismatch between SMF and UPF.

  In this scenario, static and predefined usage are not accounted in the RADIUS URR. However, the dynamic rules traffic is accounted in the RADIUS URR.

Configuring the RADIUS Client

The RADIUS client provides both RADIUS authentication and accounting functionalities. For using these functionalities, it is important to enable the RADIUS authentication and accounting framework through the associated CLI configuration.

This section describes how to configure the RADIUS client.

Important Configuring the VIP-IP of the RADIUS client interface is mandatory for the RADIUS client to work. Also, the VIP-IP must be the same as the IP of the UDP proxy pod.

Configuring the RADIUS Client involves the following:

- Configuring RADIUS Server, on page 1139
- Configuring RADIUS Server Selection Logic, on page 1140
- Configuring RADIUS Attributes, on page 1141
- Configuring RADIUS Detect Dead Server, on page 1144
- Configuring RADIUS Dead Time, on page 1144
- Configuring RADIUS Retries, on page 1145
- Configuring RADIUS Timeout, on page 1147
- Configuring RADIUS Pod, on page 1147
- Configuring Secondary Authentication Method, on page 1150
- Configuring PAP, CHAP, or MSCHAP-based Authentication, on page 1151
- Enabling RADIUS Accounting, on page 1152
- Defining RADIUS Server Group in DNN Profile, on page 1153
- Configuring RADIUS Accounting Options, on page 1153
- Configuring RADIUS Accounting Server Group, on page 1154
- Configuring the Session Disconnect Feature, on page 1155
- Enabling RADIUS Authentication Allow Parameter, on page 1142
- Configuring Consecutive Failure, on page 1142
- Configuring Max Transmissions, on page 1146
- Configuring Internal Virtual IP for Protocol Endpoint, on page 1143

Configuring RADIUS Server

Use the following sample configuration to configure the RADIUS server.

```
config
  profile radius
    server ipv4_address port_num
      secret secret_key
      priority priority_value
      type { acct | auth }
      commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server** *ipv4_address port_num*: Specify the IPv4 address and port of the RADIUS server.
- **secret** *secret_key*: Specify the secret key.
- **priority** *priority_value*: Specify the server priority.
- **type { acct | auth }**: Specify the type of the RADIUS server. The server can be one of the following:
  - **acct**: RADIUS server used for the accounting requests
  - **auth**: RADIUS server used for the authentication requests
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS server configuration.

```
profile radius
 server 209.165.200.238 1812
  secret   $8$73a0i4G3ILj0Np+8tn2QOoWDj3QkB+oefPc2ZK6RE6A=
  priority 1
 exit
 server 209.165.200.240 1812
  secret   $8$VccEEUVou7m5ptA9WZRPR7KDmxQ/L3KlJ3QqgHjexkk=
  priority 2
 exit
exit
```

Verifying the RADIUS Configuration

Use the **show radius** command to display information about the RADIUS servers (both accounting and authentication) that are configured in the system.

The following configuration is a sample output of the **show radius** command:

```
bng# show radius
radius
-------------------------------------------------------
 Server: 209.165.200.231, port: 1812, status: up, port-type: Auth
 2 requests, 0 pending, 0 retransmits
 1 accepts, 1 rejects, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 4 ms latest rtt
-------------------------------------------------------
-------------------------------------------------------
 Server: 209.165.200.231, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 0 retransmits
 3 responses, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
-------------------------------------------------------
```

Configuring RADIUS Server Selection Logic

Use the following sample configuration to configure the RADIUS server selection logic.

```
config
  profile radius
     algorithm { first-server | round-robin }
     commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **algorithm { first-server | round-robin }**: Define the algorithm for selecting the RADIUS server.
  - **first-server**: Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin**: Set the selection logic as round-robin order of servers.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS server selection logic configuration.

```
config
   profile radius
      algorithm round-robin
      exit
```

Configuring RADIUS Attributes

To configure the RADIUS attributes for authentication and accounting, use the following sample configuration:

```
config
   profile radius
      attribute [ [ instance gr_instance_id ]  [ nas-identifier nas_id ] [
nas-ip ipv4_address ] ]
      end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **attribute [[instance** *gr_instance_id* **] [nas-identifier** *nas_id* **] [nas-ip** *ipv4_address* **]]**: Configure the RADIUS identification parameters.
  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-identifier** *nas_id*: Specify the attribute name by which the system will be identified in Accounting-Request messages. *nas_id* must be an alphanumeric string.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.
- The NAS-IP-Address and NAS-Identifier attributes can be configured per instance-id in RADIUS profile configuration. In this case, NAS-IP-Address and NAS-Identifier attributes under instance configuration are treated as high priority over the non-instance based attribute configuration.

Example

The following is an example of the RADIUS attributes configuration.

```
config
   profile radius
      attribute
         instance 1
            nas-identifier CiscoSmf
         exit
      exit
   exit
exit
```

Enabling RADIUS Authentication Allow Parameter

Use the following configuration to enable allow-auth in the RADIUS server.

```
config
   profile radius
      enable-allow-auth
      end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **enable-allow-auth** : If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

Use the following configuration to enable allow-auth in the RADIUS server group.

```
config
   profile radius
      server-group group_name
         enable-allow-auth
         end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server-group** *group_name*: Enter the server group on which you want to enable the allow-auth.
- **enable-allow-auth** : If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth..

Configuring Consecutive Failure

Use the following configuration to configure consecutive failure in the RADIUS server. Even if there is no option for dead-server-detection, consecutive-failure is enabled by default and its default value is 10. To turn it off, the user must set the value to 0.

```
config
   profile radius
```

```
detect-dead-server consecutive-failures value
end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **detect-dead-server consecutive-failures** *value*: When a server's failure count reaches the threshold for consecutive failures, the server is declared as dead server.

  value: must be an integer in the range of 1–1000. Default: 10.
- It is recommended to configure the consecutive failure value more than the request maxTransmissions value in the setup.

  Example: The consecutive failure count may be greater than 6 if maxRetry = 2 and maxTransmissions = 6, so as not to affect the server switch caused by maxtransmissions. Moreover, a server level value called consecutive-failure is increased when successive requests are made to the same server.

Configuring Internal Virtual IP for Protocol Endpoint

The protocol endpoint is the configuration for the UDP-Proxy pod. The UDP-Proxy pod receives the IPC request to send the UDP message from the RADIUS-EP pod. The UDP-Proxy pod then converts the message to a proper UDP packet and sends it to the radius server. When radius server is sending UDP packet to the SMF, the UDP-Proxy pod receives and forwards the packet on the TCP connection to the RADIUS-EP pod.

```
config
  instance instance-idgr_instance_id
    endpoint protocol
      replicasreplica_id
      nodesnode_id
      internal-vip{ SMF_UDP_PROXY_INTERNAL_VIP }
      vip-ip{ client_ipv4_address }
    exit
  exit
```

NOTES:

- **instance instance-id***gr_instance_id*: Specify GR Instance ID.
- **endpoint protocol**: Enter the endpoint configuration mode.
- **replicas***replica_id*: Specifies the replica server's ID.
- **nodes***node_id*: Specify the node ID for the SMF peer node. The value must be a string.
- **internal-VIP***{ SMF_UDP_PROXY_INTERNAL_VIP }*: Specify the IP address of the UDP-Proxy for internal SMF communication, Radius-ep uses this IP address to reach the UDP proxy for outgoing AAA messages.
- **VIP-ip***{ client_ipv4_address }*: Specify the IP address of the dynamic authorization client. *ipv4_address* must be in standard IPv4 dotted decimal notation.

Example

The following is an example configuration.

```
config
   instance instance-id 1
      endpoint protocol
         replicas 1
         nodes 2
         internal-vip {SMF_UDP_PROXY_INTERNAL_VIP}
         vip-ip { client_ipv4_address}
      exit
   exit
```

Configuring RADIUS Detect Dead Server

Use the following sample configuration to configure the RADIUS detect dead server.

```
config
   profile radius
      detect-dead-server response-timeout value
      commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **detect-dead-server response-timeout** *value*: Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.

  value must be an integer in the range of 1–65535. Default: 10 seconds.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS detect dead server configuration.

```
config
   profile radius
      detect-dead-server response-timeout 100
      exit
```

Configuring RADIUS Dead Time

Use the following sample configuration to configure the RADIUS dead time.

```
config
   profile radius
      deadtime value
      commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **deadtime** *value*: Set the time to elapse between RADIUS server marked unreachable and when we can reattempt to connect.

  value must be an integer in the range of 1–65535. Default: 10 minutes.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS dead time configuration.

```
config
   profile radius
     deadtime 15
     exit
```

Configuring RADIUS Dictionary

Use the following sample configuration to configure the RADIUS dictionary.

```
config
  profile radius
     dictionary { ISE dictionary | 3GPP dictionary }
     commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **dictionary { ISE dictionary | 3GPP dictionary }**: The SMF service renders the RADIUS configuration and populates the request messages with the ISE or 3GPP specific parameters as selected.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS dictionary configuration.

```
config
   profile radius
      dictionary { ISE dictionary | 3GPP dictionary }
      exit
```

Configuring RADIUS Retries

Use the following sample configuration to configure the maximum RADIUS retries.

```
config
  profile radius
     max-retry value
     commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **max-retry** *value*: Set the maximum number of times that the system will attempt retry with the RADIUS server.

  value must be an integer in the range of 0–65535. Default: 2
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS retries configuration.

```
config
   profile radius
      max-retry 2
      exit
```

Configuring Max Transmissions

Use the following configuration to configure max transmissions in the RADIUS server.

```
config
   profile radius
      max-transmissions value
      end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **max-transmissions** *value*: Max transmission allows you to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available or if maxtransimissions limit is reached, then the server database sends out the timeout response.

  value: must be an integer in the range of 0–65535. Default: 6.
- Max transmission value should always be higher value than the max retries +1. It is recommended to use maxTransmissions number as multiples of (maxRetries +1).
- Based on the maxTransmissions, time spent on a single request increases and remains in the system without providing a response by retrying on other servers. As a result, system resources are used up, which may lead to performance degradation.

Use the following configuration to configure max transmissions in the RADIUS server group.

```
config
   profile radius
      server-group group_name
        max-transmissions value
        end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server-group** *group_name*: Enter the server group on which you want to configure the max-transmissions.
- **max-transmissions** *value*: Max transmission allows you to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available or if maxtransimissions limit is reached, then the server database sends out the timeout response.

  value: must be an integer in the range of 0–65535. Default: 6.

- Max transmission value should always be higher value than the max retries +1. It is recommended to use maxTransmissions number as multiples of (maxRetries +1).
- Based on the maxTransmissions, time spent on a single request increases and remains in the system without providing a response by retrying on other servers. As a result, system resources are used up, which may lead to performance degradation.

Configuring RADIUS Timeout

Use the following sample configuration to configure the RADIUS timeout.

```
config
  profile radius
     timeout value_in_seconds
     commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **timeout** *value_in_seconds*: Set the time to wait for response from the RADIUS server before retransmitting.

  value_in_seconds must be an integer in the range of 1–65535. Default: 2 seconds.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS timeout configuration.

```
config
   profile radius
      timeout 4
      exit
```

Configuring RADIUS Pod

Use the following sample configuration to configure the RADIUS pod.

```
config
   instance instance-id gr_instance_id
      endpoint radius
         replicas number_of_replicas
         commit
```

NOTES:

- **endpoint radius**: Enter the RADIUS endpoint configuration mode.
- **replicas** *number_of_replicas*: Set the number of replicas required.
- **commit**: Commit the configuration.

Example

The following is an example of the RADIUS pod configuration.

```
config
   instance instance-id 1
      endpoint radius
         replicas 3
         exit
```

Configuring RADIUS NAS-IP

This section describes how to configure the RADIUS NAS-IP.

Multiple RADIUS NAS-IP Configuration

Note The NAS-Identifier attribute configuration can be defined per instance-id in RADIUS profile configuration. In this case, NAS-Identifier attribute under instance configuration is treated as high priority over the non-instance based NAS-Identifier attribute configuration.

To configure multiple RADIUS NAS-IP addresses at various levels, use the following sample configuration:

```
config
   profile radius
      attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address ] ]
      accounting attribute [[ instance gr_instance_id ] [ nas-ip ipv4_address ]
 ]
      server-group group_name attribute [[ instance gr_instance_id ] [ nas-ip
ipv4_address ] ]
      server-group group_name accounting attribute [[ instance gr_instance_id
] [ nas-ip ipv4_address ] ]
      end
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **attribute [[instance** *gr_instance_id* **] [nas-ip** *ipv4_address* **]]**: Set the global NAS-IP address value.
  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.
- **accounting attribute [[instance** *gr_instance_id* **] [nas-ip** *ipv4_address* **]]**: Set the global accounting NAS-IP address value.
  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.

- **server-group** *group_name* **attribute [[instance** *gr_instance_id* **] [nas-ip** *ipv4_address* **]]**: Set the per server-group common NAS-IP address value.
  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.
- **server-group** *group_name* **accounting attribute [[instance** *gr_instance_id* **] [nas-ip** *ipv4_address* **]]**: Set the per server-group accounting NAS-IP address value.
  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.

Example:

The following is an example of the multiple RADIUS NAS-IP configuration.

```
config
 profile radius
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
  exit
  accounting
   attribute
    instance 1
     nas-ip 209.165.200.225
     nas-identifier  smf1
    exit
    instance 2
     nas-ip 209.165.201.2

     nas-identifier  smf2
    exit
   exit
  exit
 exit
 server-group g1
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
```

```
  exit
 exit
 accounting
  attribute
   instance 1
    nas-ip 209.165.200.225
    nas-identifier  smf1
   exit
   instance 2
    nas-ip 209.165.201.2

    nas-identifier  smf2
   exit
  exit
 exit
exit
```

Configuring Secondary Authentication Method

Use the following sample configuration to configure the secondary authentication method.

```
config
   profile dnn dnn_name
      authentication secondary radius [ group group_name ]
      commit
```

NOTES:

- **profile dnn** *dnn_name*: Enter the DNN Profile configuration mode.
- **authentication secondary radius [group** *group_name* **]**: Enable secondary authentication under the DNN profile and sets method as RADIUS.

  group *group_name*: This keyword is optional. This keyword defines the RADIUS server group name.
- **commit**: Commit the configuration.

Example

The following is a configuration example of the secondary authentication method.

```
config
   profile dnn intershat
   ...
   authentication secondary radius
   exit
```

Verifying the RADIUS Authentication Configuration

Use the **show radius auth-server** command to display detailed statistics for RADIUS authentication server and port.

The following configuration is a sample output of the **show radius auth-server** command:

```
bng# show radius auth-server
-----------------------------------------------------
 Server: 209.165.200.232, port: 1812, status: up, port-type: Auth
 2 requests, 0 pending, 0 retransmits
 1 accepts, 1 rejects, 0 timeouts
 0 bad responses, 0 bad authenticators
```

```
 0 unknown types, 0 dropped, 4 ms latest rtt
----------------------------------------------------------
```

Configuring PAP, CHAP, or MSCHAP-based Authentication

This section provides the configuration to enable the PAP, CHAP, and MSCHAP-based RADIUS authentication. This configuration aids in converting the CHAP Challenge and Response received in PCO IE as MSCHAP Challenge and Response.

Defining Priority for Authentication Algorithm

Use the following sample configuration to define the priority for different authentication algorithms (PAP or CHAP or MSCHAP) for RADIUS-based authentication in SMF.

```
config
   profile dnn profile_name
     authentication { { secondary radius [ group group_name  ] | { algorithm
 { pap priority_value [ password-use-pco ] | chap priority_value [
convert-to-mschap ] | mschap priority_value } }
      end
```

NOTES:

- **password-use-pco**: This keyword overrides the DNN configured password with PCO password. The default setting is disabled.

  If the host level password is not configured at DNN, then the SMF uses the UE given password for PAP-based authentication even though this configuration is disabled.

- **convert-to-mschap**: This keyword converts the received CHAP Challenge and Response to MSCHAP if the CHAP Response length is 49 bytes. Otherwise, the SMF sends as CHAP only even though this configuration is explicitly enabled.

- The default priority for PAP, CHAP, and MSCHAP algorithms is 0 which means that the configuration is disabled. The valid values are 1, 2, and 3. Lower the value, higher is the priority. It is used to resolve conflicts if the UE sends multiple authentication parameters in the PCO, EPCO, or APCO IE.

Configuring Host Password

Use the following sample configuration to specify the host password at DNN level which is used as a password for PAP-based authentication.

```
config
   profile dnn profile_name
      outbound password password
      end
```

NOTES:

- **profile dnn** *profile_name*: Specify the DNN profile name as an alphanumeric string to enter the DNN configuration mode.

- **outbound password** *password*: Specify the DNN host password for authentication. By default, the SMF sends this password in PAP user-password if it is not explicitly overridden using the **password-use-pco** option.

By default, the SMF encrypts the given password using AES-128-CFB encryption algorithm.

Enabling RADIUS Accounting

Use the following sample configuration to enable RADIUS accounting on SMF and configure the RADIUS accounting specific parameters.

```
config
  profile charging charging_profile_name
    accounting limit { duration value | volume { downlink value | total
value | uplink value } }
    accounting triggers [ ambr-change | plmn-change | qos-change |
rat-change | serv-node-change | tft-change | ue-time-change |
user-loc-change ]
    commit
```

NOTES:

- **profile charging** *charging_profile_name*: Specify the charging profile name. *charging_profile_name* must be an alphanumeric string.
- **accounting**: Specify this option to enable RADIUS accounting on SMF for the subscribesrs.
- **limit { duration** *value* **| volume { downlink** *value* **| total** *value* **| uplink** *value* **} }**: Specify the volume and time limits for RADIUS accounting.

  duration *value*: Specify the time duration value as an integer in the range of 0–2147483647.

  downlink *value*: Specify the downlink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

  total *value*: Specify the total volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

  uplink *value*: Specify the uplink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

- **accounting triggers [ambr-change | plmn-change | qos-change | rat-change | serv-node-change | tft-change | ue-time-change | user-loc-change]**: Enable the appropriate RADIUS accounting triggers according to the following conditions:
  - AMBR change
  - PLMN change
  - Quality of Service change
  - Routing Area Information change
  - Serving node change
  - Traffic Flow Template (TFT) change
  - UE time change
  - User Location Information change - applicable only for PGW-C and GGSN.

Important Enabling any one of these triggers turns off the remaining triggers.

- **commit**: Commit the configuration.

Defining RADIUS Server Group in DNN Profile

Use the following sample configuration to set RADIUS server-group to use for accounting in DNN profile.

All subscribers under the specified DNN will have RADIUS accounting enabled.

```
config
  profile dnn dnn_profile_name
    accounting server-group group_name
    commit
```

NOTES:

- **profile dnn** *dnn_profile_name*: Specify the DNN profile name to enter the DNN configuration mode. *dnn_profile_name* must be an alphanumeric string.
- **accounting server-group** *group_name*: Specify the RADIUS server-group to use for accounting in the configured DNN profile. *group_name* must be an alphanumeric string.
- **commit**: Commit the configuration.

Configuring RADIUS Accounting Options

To configure the RADIUS accounting options, use the following sample configuration:

```
config
  profile radius accounting
    algorithm { first-server | round-robin }
    attribute [ [ instance gr_instance_id ]  [ nas-identifier nas_id ] [
nas-ip ipv4_address ] ]
    deadtime value
    detect-dead-server response-timeout value
    max-retry value
    timeout value
    end
```

NOTES:

- **profile radius accounting**: Enter the RADIUS accounting configuration mode.
- **algorithm { first-server | round-robin }**: Define the algorithm for selecting the RADIUS server.
  - **first-server**: Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin**: Set the selection logic as round-robin order of servers.
- **attribute [[instance** *gr_instance_id* **] [nas-identifier** *nas_id* **] [nas-ip** *ipv4_address* **]]**: Configure the RADIUS identification parameters.

  - **instance** *gr_instance_id*: Specify the Geographic Redundancy (GR) instance ID. *gr_instance_id* must be an integer.
  - **nas-identifier** *nas_id*: Specify the attribute name by which the system will be identified in Accounting-Request messages. *nas_id* must be an alphanumeric string.
  - **nas-ip** *ipv4_address*: Specify the NAS IPv4 address. *ipv4_address* must be an IPv4 address in dotted decimal notation.

- **deadtime** *value*: Set the time to elapse between RADIUS server marked unreachable and when we can re-attempt to connect.

  value must be an integer from 0 through 65535. Default: 10 minutes.

- **detect-dead-server response-timeout** *value*: Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.

  value must be an integer from 1 through 65535. Default: 10 seconds.

- **max-retry** *value*: Set the maximum number of times that the system will attempt retry with the RADIUS server.

  value must be an integer in the range of 0–65535. Default: 2

- **timeout** *value*: Set the time to wait for response from the RADIUS server before retransmitting.

  value must be an integer in the range of 1–65535. Default: 2 seconds.

- All the keyword options under the RADIUS accounting configuration mode are also available within the RADIUS configuration mode.

Configuring RADIUS Accounting Server Group

Use the following sample configuration to configure the RADIUS server group.

```
config
  profile radius
    server-group group_name
    commit
```

NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **server group** *group_name*: Specify the name of server group for use in RADIUS accounting. *group_name* must be an alphanumeric string.
- **commit**: Commit the configuration.

Verifying the RADIUS Accounting Configuration

Use the **show radius acct-server** command to display statistics for RADIUS accounting server and port.

The following configuration is a sample output of the **show radius acct-server** command:

```
bng# show radius acct-server
-------------------------------------------------------
 Server: 209.165.200.228, port: 1813, status: up, port-type: Acct
```

```
 3 requests, 0 pending, 0 retransmits
 3 responses, 0 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
-------------------------------------------------------
```

Configuring the Session Disconnect Feature

This section describes how to configure the Session Disconnect feature.

Configuring the Session Disconnect feature in SMF involves the following steps:

- Configuring the Dynamic Authorization Service, on page 1155
- Configuring the CoA-NAS Interface, on page 1156

Configuring the Dynamic Authorization Service

Use the following sample configuration to enable the NAS as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the RADIUS Disconnect and Change of Authorization (CoA) functionality.

```
config
   profile radius-dynamic-author
      client ipv4_address [ secret shared_secret ]
      nas-identifier value
      secret shared_secret
      end
```

NOTES:

- **profile radius-dynamic-author**: Enter the dynamic authorization configuration mode.
- **client** *ipv4_address* **[secret** *shared_secret* **]**: Specify the IP address of the Dynamic Authorization Client. *ipv4_address* must be in standard IPv4 dotted decimal notation.

  You can add a list of client IPs from which the Disconnect message is accepted.

  secret *shared_secret*: This is an optional keyword. Specify the secret key at the client level.

Important Configuring the server key at the client level overrides the server key configured at the global level.

- **nas-identifier** *value*: Specify the dynamic authorization specific NAS-Identifier value. *value* must be an alphanumeric string of 1 to 64 characters.

  If this keyword is configured, it is validated against the value received in DM request. If this keyword is not configured, the input value is silently ignored. That is, the DM requests from unlisted or unauthenticated clients are silently discarded.

- **secret** *shared_secret*: Specify the global shared secret key of the server.

Verifying the Session Disconnect Feature Configuration

This section describes how to verify the configuration associated with the Session Disconnect feature.

To view the information about the RADIUS Dynamic Authorization Clients that are configured in the system, use the **show radius-dyn-auth** command.

The following is a sample output of the **show radius-dyn-auth** command.

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
-------------------------------------------------------
 IP: 209.165.200.227
 ------------------
 COA:
 0 total-requests     0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
 DISCONNECT:
 0 total-requests     0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
 UnknownTypesRcvd: 0
-------------------------------------------------------
```

Configuring the CoA-NAS Interface

Use the following sample configuration to define Change of Authorization (CoA) NAS interface in the RADIUS endpoint.

```
config
   instance instance-id gr_instance_id
      endpoint radius
         interface coa-nas
            vip-ip ipv4_address vip-port port_number
            end
```

NOTES:

- **endpoint radius**: Enter the RADIUS endpoint configuration mode.
- **interface coa-nas**: Enter the CoA NAS interface configuration mode. This keyword defines a new interface "coa-nas".
- **vip-ip** *ipv4_address* **vip-port** *port_number*: Specify the IP address of the host. *ipv4_address* must be in standard IPv4 dotted decimal notation.

  You can configure a list of VIP-IPs to listen to the inbound CoA or DM requests.

  vip-port *port_number*: Specify the port number of the UDP proxy. By default, the port number is 3799. This default value is used only when the VIP-IP is specified.

Important This configuration allows only port to be specified per IP.

The SMF (udp-pxy) listens to the inbound CoA or DM request messages on these ports, and ACK or NAK messages sent with the respective source IP and port.

RADIUS Client OA&M Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

RADIUS Authentication Statistics

This feature supports the following statistics related to RADIUS Authentication:

- SMF-Service:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
- RADIUS-EP:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
  - Number of RADIUS packets sent
  - Number of RADIUS packets received

RADIUS Accounting Statistics

The SMF maintains the following statistics to track the total number of attempted, successful, and failed RADIUS Accounting Start, Accounting Update Interim and Accounting Terminate requests and responses.

- SMF_SERVICE_STATS for the following procedure types:
  - radius_initial: This counter gets incremented for Accounting Start request and response.
  - radius_update: This counter gets incremented for Accounting Interim Update request and response.
  - radius_terminate: This counter gets incremented for Accounting Terminate request and response.

RADIUS Access Management Statistics

The following statistics track the number of times the AVP is received in the RADIUS Access-Accept messages at SMF.

- SmfRadiusMessageStats

  INBOUND:
  - radius_access_accept
    - radius_avp_session_timeout
    - radius_avp_idle_timeout

PAP, CHAP, or MSCHAP-based Authentication Statistics

The SMF supports the following statistics to track the number of times the AVP sent in Access-Request messages.

Group: smf_radius_message_stats

Format: {app_name, cluster, data_center, direction, instance_id, message_type, radius_avp_type, rat_type, service_name}

message_type: radius_access_request

radius_avp_type:

- radius_avp_pap_user_password
- radius_avp_pap_username
- radius_avp_chap_challenge
- radius_avp_chap_response
- radius_avp_mschap_challenge
- radius_avp_mschap_response

Example:

```
smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",direction="outbound",
instance_id="0",message_type="radius_access_request",radius_avp_type="radius_avp_pap_user_password",
rat_type="NR",service_name="smf-service"} 1

smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",
direction="outbound",instance_id="0",message_type="radius_access_request",
radius_avp_type="radius_avp_pap_username",rat_type="NR",service_name="smf-service"} 1
```

The SMF supports these additional statistics to track the number of attempted, successful and failed responses received due to PAP, CHAP, and MSCHAP authentication.

Group: radius_authentication_message_stats

Format: {app_name, cluster, data_center, dnn, instance_id, radius_auth_algorithm, rat_type, reason, service_name, status}

radius_auth_algorithm:

- radius_auth_algorithm_default
- radius_auth_algorithm_pap
- radius_auth_algorithm_chap
- radius_auth_algorithm_mschap

rat_type:

- NR
- EUTRA
- WLAN

status:

- decode_failed
- encode_failed
- attempted
- success
- failed
- timeout

reason:

- parse_error
- invalid_code
- invalid_option
- invalid_pco
- invalid_epco
- invalid_apco
- write_error

Example:

```
radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",
radius_auth_algorithm="radius_auth_algorithm_default",rat_type="NR",reason="",
service_name="smf-service",status="attempted"} 2

 radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_default",
rat_type="NR",reason="",service_name="smf-service",status="success"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",data_center="DC",
dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",
rat_type="EUTRA",reason="",service_name="smf-service",status="attempted"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",

rat_type="EUTRA",reason="",service_name="smf-service",status="failed"} 2
```

RADIUS Disconnect and CoA Request Related Statistics

The RADIUS endpoint (radius-ep) pod supports the following statistics.

Radius_Server_Status

Description: Display the active or inactive status of RADIUS server.

Metrics-Type: Gauge

Metrics-Value: 1 – ActiveServer, 0 – Inactive Server

Labels:

- Label: radSvrIP

- Description: Server IP Address
- Value: <any-ip-address>

- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>

- Label: radSvrPortType
  - Description: Authentication or Accounting type
  - Value: Auth, Acct

Radius_Requests_Current

Description: Displays the outstanding authentication and accounting requests

Metrics-Type: Gauge

Labels:

- Label: radMsgCode
  - Description: RADIUS Message Type
  - Values: SecondaryAuthenReq, RadiusAcctReq, TestAuth, TestAcct

- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>

- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>

- Label: radSvrPortType
  - Description: Authentication or Accounting type
  - Value: Auth, Acct

- Label: dnn
  - Description: DNN of subscriber
  - Value: <string>

- Label: procType
  - Description: Procedure-type
  - Value: <string>

- Label: ratType
  - Description: RAT type of subscriber
  - Value: <string>
- Label: sessType
  - Description: Session-type of subscriber
  - Value: <string>
- Label: grInstId
  - Description: Geographic redundancy (GR) instance ID
  - Value: <string>

Radius_Requests_Statistics

Description: Displays the total authentication and accounting requests transmitted, retransmitted, and responses received

Metrics-Type: Counter

Labels:

- Label: radMsgCode
  - Description: Radius Message Type
  - Values: SecondaryAuthenReq, RadiusAcctReq, TestAuth, TestAcct
- Label: radPacketType
  - Description: Direction of packet
  - Value: Tx, Rx, Retry_Tx
- Label: radResult
  - Description: Result of operation
  - Value: Success, Failed, Timeout, Failure_Reject, ...
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>
- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>
- Label: radSvrPortType

- Description: Authentication or Accounting type
- Value: Auth, Acct

- Label: dnn
  - Description: DNN of subscriber
  - Value: <string>

- Label: procType
  - Description: Procedure-type
  - Value: <string>

- Label: ratType
  - Description: RAT type of subscriber
  - Value: <string>

- Label: sessType
  - Description: Session-type of subscriber
  - Value: <string>

- Label: grInstId
  - Description: Geographic redundancy (GR) instance ID
  - Value: <string>

Radius_CoaDM_Requests_Current

Description: Displays the outstanding CoA and DM requests being processed.

Metrics-Type: Gauge

Labels:

- Label: radMsgCode
  - Description: RADIUS Message Type
  - Values: DisconnectRequest, CoARequest

- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>

- Label: grInstId
  - Description: Geographic redundancy (GR) instance ID
  - Value: <string>

Radius_CoaDM_Requests_Statistics

Description: Displays the total CoA and DM requests received and processed.

Metrics-Type: Counter

Labels:

- Label: radMsgCode
  - Description: Radius Message Type
  - Values: DisconnectRequest, DisconnectACK, DisconnectNAK, CoARequest, CoaDMReq, CoAACK
- Label: radPacketType
  - Description: Direction of packet
  - Value: Tx, Rx
- Label: radResult
  - Description: Result of operation
  - Value: Success, Failure_Invalid_Request, Failure_Drop_Retry_Coa, Failure_Unknown_Error...
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>
- Label: nakErrorCause
  - Description: Error-cause set during COA-NAK / DM-NAK (not applicable for other cases)
  - Value: Missing-Attribute, NAS-Identification-Mismatch, Unsupported-Service, Invalid-Attribute-Value, Session-Context-Not-Found, Internal-Error
- Label: grInstId
  - Description: Geographic redundancy (GR) instance ID
  - Value: <string>

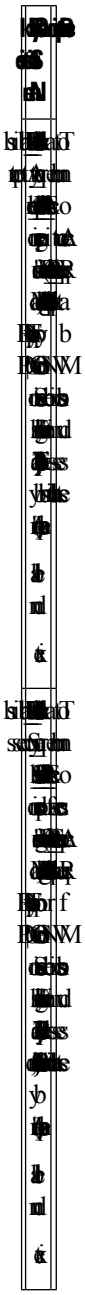
Troubleshooting Information

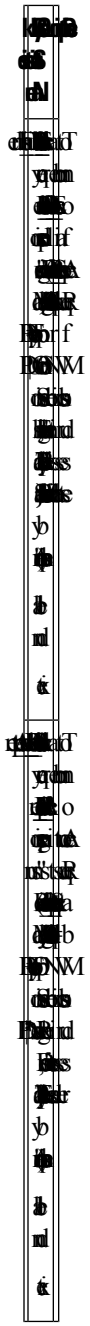
This section provides information on using the command line interface (CLI) commands, alerts, logs, and metrics for troubleshooting any RADIUS related issues that may arise during system operation.

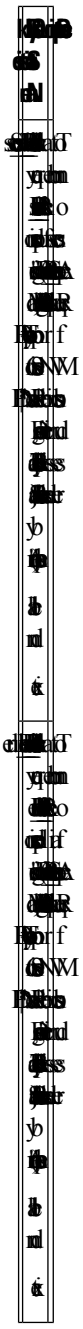
RADIUS Bulk Statistics

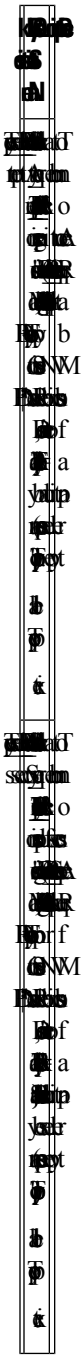
Use the following bulk statistics to monitor the failures or issues associated with RADIUS authentication, RADIUS accounting, and Disconnect Message requests.

Table 390: RADIUS Accounting Message (Per endpoint)









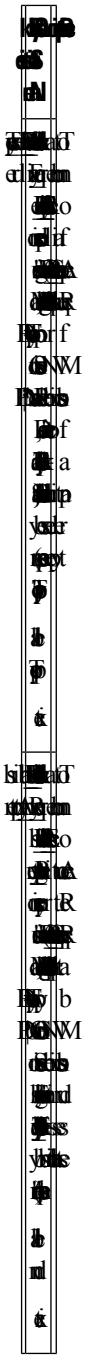


Table 391: RADIUS Accounting Message (Per SMF service)

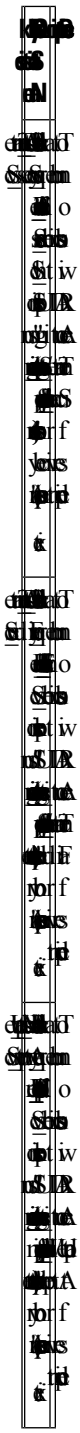


Table 392: Disconnect Message

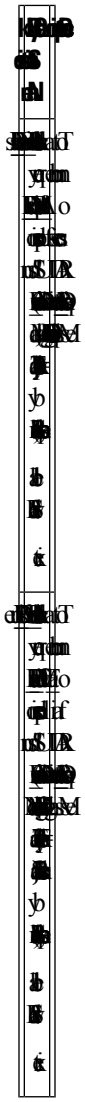
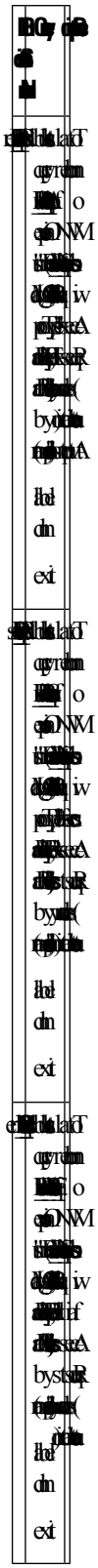


Table 393: RADIUS Access Request (Secondary Authentication)



Subscriber Details for RADIUS-specific Information

The **show subscriber supi** *supi_id* **nf-service smf full** CLI command displays the subscriber details for RADIUS-specific use cases.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
full
subscriber-details
{
…
"alwaysOn": "None",
        "dcnr": "None",
        "wps": "Wps Session",
        "ratType": "NR",
        "idleTimeout": 600,     << can be overwritten from Radius in Auth Resp

        "sessTimeout": 1200,    << can be overwritten from Radius in Auth Resp

        "radiusEpInfo": "209.165.200.228:1812",
        "authAlg": "pap-default",
        "authStatus": "Authenticated"
…
…
        "accountingEnabled": "true",
        "n40ChargingEnabled": "true",
        "acctSessId": "198.15.1.40016777221"
…
…
"upfServData": {
        "numberOfTunnels": 2,
        "smfSeid": 72057615828912656,
        "UPState": "Activated",
        "urrInfo": [
          {
            "id": 2147483657,
            "chgName": "radiusurr",
            "method": {
              "duration": "false",
              "volume": "true",
              "event": "false"
            },
```

RADIUS Endpoint Authentication and Accounting Statistics

The **show radius** CLI command displays statistics for RADIUS Authentication and Accounting from RADIUS endpoint.

```
[unknown] smf# show radius
radius
-----------------------------------------------------------
 Server: 209.165.200.240, port: 1812, status: up, port-type: Auth
 3 requests, 0 pending, 0 retransmits
 2 accepts, 0 rejects, 1 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
-----------------------------------------------------------
-----------------------------------------------------------
 Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 6 retransmits
```

```
 0 responses, 3 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 0 ms latest rtt
----------------------------------------------------------
 Server: 209.165.200.245, port: 1813, status: up, port-type: Acct
 5 requests, 0 pending, 3 retransmits
 3 responses, 2 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 6 ms latest rtt
----------------------------------------------------------
[unknown] smf#
```

```
[unknown] smf# show radius acct-server
----------------------------------------------------------
 Server: 209.165.200.234, port: 1813, status: up, port-type: Acct
 3 requests, 0 pending, 6 retransmits
 0 responses, 3 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 0 ms latest rtt
----------------------------------------------------------
 Server: 209.165.200.240, port: 1813, status: up, port-type: Acct
 5 requests, 0 pending, 3 retransmits
 3 responses, 2 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 6 ms latest rtt
----------------------------------------------------------
[unknown] smf#
```

```
[unknown] smf# show radius auth-server
----------------------------------------------------------
 Server: 209.165.200.243, port: 1812, status: up, port-type: Auth
 3 requests, 0 pending, 0 retransmits
 2 accepts, 0 rejects, 1 timeouts
 0 bad responses, 0 bad authenticators
 0 unknown types, 0 dropped, 1 ms latest rtt
----------------------------------------------------------
[unknown] smf#
```

RADIUS Endpoint Disconnect Message and CoA Statistics

The **show radius-dyn-auth** CLI command displays statistics for RADIUS Disconnect Message and CoA from RADIUS endpoint.

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
----------------------------------------------------------
 IP: 209.165.201.20
 ------------------
 COA:
 0 total-requests       0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 0 ack-sent             0 nak-sent
 ------------------
 DISCONNECT:
 2 total-requests       0 inprocess-requests
     0 retry-request-drops  0 invalid-requests
     0 bad-authenticators   0 internal-errors
 1 ack-sent             1 nak-sent
 ------------------
 UnknownTypesRcvd: 0
----------------------------------------------------------
[unknown] smf#
```

External Inbound and Outbound Connections

The **show peers all** CLI command fetches the list of external inbound and outbound connections established by the SMF.

```
[unknown] smf# show peers all | include radius
RadiusServer  -     209.165.202.145:1813   Outbound   radius-ep-0    Udp   18 hours   Radius
  Status: Active,Type: Acct  1
RadiusServer  -     209.165.201.20:1812    Outbound   radius-ep-0    Udp   17 hours   Radius
  Status: Active,Type: Auth  1
RadiusServer  -     209.165.201.20:1813    Outbound   radius-ep-0    Udp   17 hours   Radius
  Status: Active,Type: Acct  1
[unknown] smf#
```

Important During application startup or configuration updates, RADIUS endpoint sends test authentication and accounting requests to check the status of RADIUS server peer. The output of the **show peers** command displays the peer status result.

The results of these dummy requests will be overwritten by the outcomes of actual authentication and accounting requests.

Internal and External Connections

The **show endpoint info** CLI command fetches the list of internal and external connections established by the SMF.

```
[unknown] smf# show endpoint all | include radius
Radius:209.165.201.4:     209.165.201.1:3799     Udp   Started  RADIUS     false     18
hours  <none>   1
[unknown] smf#
```

Status of Pods

The **show running-status** CLI command fetches the current status of pods. This function is analogous to the K8 **kubectl get pods –n** <> CLI command.

```
[unknown] smf# show running-status | include radius
radius-ep-0      Started      19 hours
[unknown] smf#
```

Configuration Errors

The **show config-error** CLI command displays the validation criteria — Pass or Failed. The Pass criteria appears when no entries exist.

```
[unknown] smf# show config-error | include radius
[unknown] smf#
```

show alerts

This section provides the sample output for different variants of the **show alerts** CLI command.

show alerts | include radius

```
alerts history radius_test cfb253587397
alerts history radius_test 911f84aff47c
alerts history radius_test 3ed7a5112905
alerts history radius_test 292af807b299
 source      radius-ep-n0-0
 labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
 source      radius-ep-n0-0
 labels     [ "name: k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
 "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
 in namespace: smf has been restarted." ]
 source      radius-ep-n0-0
 labels      [ "name: k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
alerts history radius_test 1c17e31c13f9
alerts history radius_test ffaabfce0929
 source      radius-ep-n0-0
 labels      [ "name: k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
 source      radius-ep-n0-0
 labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
 source      radius-ep-n0-0
 labels     [ "name: k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
 "namespace: smf" "pod: radius-ep-n0-0" ]
 annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
 in namespace: smf has been restarted." ]
[unknown] cee#
```

show alerts active detail | include radius

```
alerts active detail Radius_Server_Down 0fe030aba3ce
 summary  "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
than 15min."
alerts active detail Radius_Server_Down 6f41c340311c
 summary  "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
than 15min."
alerts active detail Radius_Server_Down 8a290c5ed1de
 summary  "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
than 15min."
[unknown] cee#
[unknown] cee#
alerts active detail Radius_Server_Down 0fe030aba3ce
 severity major
 type     "Processing Error Alarm"
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more
than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 6f41c340311c
```

```
 severity major
 type     "Processing Error Alarm"
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more
than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.202.145" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 8a290c5ed1de
 severity major
 type     "Processing Error Alarm"
 startsAt 2020-12-11T13:30:16.874Z
 source   System
 summary  "Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more
than 15min."
 labels   [ "namespace: smf" "radSvrIP: 209.165.201.20" "radSvrPort: 1812" ]

[unknown] cee# show alerts active summary | include RTT
Radius_Server_RTT      1d0353b3db82  major     12-11T15:10:16  System   RTT for Radius
Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#
```

show alerts active summary | include RTT

```
Radius_Server_RTT     1d0353b3db82  major    12-11T15:10:16  System RTT for Radius Server:
 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
[unknown] cee#
```

show alerts active summary | include radius

```
Radius_Server_RTT      1d0353b3db82  major     12-11T15:10:16  System                 RTT
for Radius Server: 209.165.201.20, Port: 1812 in namespace: smf is more than 5 ms.
Radius_Acct_Establish  520d9943d53f  major     12-11T15:05:16  System                 This
 alert is fired when the percentage of successful Radius Accounting Establish responses
received is lesser than threshold
Radius_Server_Down     0fe030aba3ce  major     12-11T13:30:16  System               Radius
 Server: 209.165.201.20, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     6f41c340311c  major     12-11T13:30:16  System               Radius
 Server: 209.165.202.145, Port: 1813 in namespace: smf is DOWN for more than 15min.
Radius_Server_Down     8a290c5ed1de  major     12-11T13:30:16  System               Radius
 Server: 209.165.201.20, Port: 1812 in namespace: smf is DOWN for more than 15min.
```

RADIUS Alerts

The RADIUS endpoint for MVNO or PAPN flow supports new alerts. Following sections describe some basic alerts. These alerts can be enhanced based on RAT or as required by the users.

Important These alerts are configurable only through the CEE Ops-center CLI.

RADIUS EP Down Alert

Use the following example to configure alerts related to RADIUS EP Down.

```
alerts rules group RadiusEP
 rule Radius_Server_Down
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Status{radSvrPortType=~\"Auth|Acct\"} < 1)"
  duration   15m
```

```
  severity   major
  type       "Processing Error Alarm"
  annotation summary
  value "\"Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }} in namespace:
 {{ $labels.namespace }} is DOWN for more than 15min.\""
  exit
 exit
```

RADIUS Accounting Establishment Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Establishment Failure threshold.

```
alerts rules group RadiusEP
 rule Radius_Acct_Establish_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
    value "This alert is fired when the percentage of successful Radius Accounting Establish
 responses received is lesser than threshold"
   exit
  exit
```

RADIUS Accounting Release Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Release Failure threshold.

```
rule Radius_Acct_Release_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
    value "This alert is fired when the percentage of successful Radius Accounting Release
 responses received is lesser than threshold"
   exit
  exit
```

RADIUS Authentication Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Authentication Failure threshold.

```
rule Radius_Auth_SR
   expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\", procType=\"PDU
Session Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by
(namespace) (increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\",
procType=\"PDU Session Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
    value "This alert is fired when the percentage of successful Radius Authentication
Request responses received is lesser than threshold"
```

```
   exit
  exit
```

RADIUS Disconnect Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Disconnect Message Failure threshold.

```
rule Radius_Disconnect_Message_SR
   expression "sum by (namespace)
(increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectACK\", radPacketType=\"Tx\",
 radResult=\"Success\"}[5m])) / sum by
(namespace)(increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectRequest\",
radPacketType=\"Rx\"}[5m])) < 0.80"
   severity   major
   type       "Communications Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Disconnect Message (DM)
responses sent is lesser than threshold"
   exit
  exit
exit
```

RADIUS Server RTT Alert

Use the following example to configure alerts related to RADIUS server RTT.

```
rule Radius_Server_RTT
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Rtt_ms{radSvrPortType=~\"Auth|Acct\"} > 5)"
duration   15m
  severity   warning
  type       "Communications Alarm"
  annotation summary
   value "\"RTT for Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }}
in namespace: {{ $labels.namespace }} is more than 5 ms.\""
  exit
 exit
```

RADIUS Accounting Start Initial Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Start Initial Message Failure threshold.

```
rule Radius_Acct_Start_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Start successful response received is lesser than threshold"
   exit
  exit
```

RADIUS Accounting Interim/Update Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Interim/Update Message Failure threshold.

```
rule Radius_Acct_Interim_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Interim Update successful response received is lesser than threshold"
   exit
  exit
```

RADIUS Accounting Stop/Terminate Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Accounting Stop/Terminate Message Failure threshold.

```
rule Radius_Acct_Stop_SR
   expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"attempted\"}[5m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This service based alert is fired when the percentage of successful Radius
Accounting Stop successful response received is lesser than threshold"
   exit
  exit
```

RADIUS Authentication Type Message Failure Threshold Alert

Use the following example to configure alerts related to RADIUS Authentication Type Message Failure threshold.

```
rule Radius_Auth_Type_SR
   expression "sum by (namespace, radius_auth_algorithm)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm_.*\",
 status=\"success\"}[1m])) / sum by (namespace)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm_.*\",
 status=\"attempted\"}[1m])) < 0.80"
   severity   major
   type       "Processing Error Alarm"
   annotation summary
     value "This alert is fired when the percentage of successful Radius Auth Type response
 received is lesser than threshold"
   exit
  exit
```

Grafana Charts

The Grafana charts are used for monitoring based on the RADIUS endpoint or Service endpoint.

- RADIUS endpoint for call flows involving RADIUS Authentication, Accounting, and Disconnect Message.
- Service endpoint for accounting flows specific to Accounting Initial, Interim, or Terminate packets.

Error Logs

This section explains the basic error conditions and the related logs to debug the failures.

RADIUS Authentication

Authentication Request Not Responded by Server

The following is an error log for RADIUS Authentication Request not responded by the RADIUS server.

```
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [GenericAAA.go:786]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Secondary
 Authentication Failed: TIMEOUT
[smf-service-n0-0] *errors.errorString Secondary Authentication Failed: TIMEOUT
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/GenericAAA.go:786 (0x144fa52)
```

Call Failure at Authentication Stage

The following is a sample error log for call failure at the RADIUS authentication stage.

```
[smf-service-n0-0]
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [idlestate.go:504]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] *errors.errorString USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:580 (0x15d7ddc)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/4g/pdnsetup/idlestate.go:537 (0x15bc4f5)
```

Authentication Request Rejected by RADIUS Server

The following is an error log for RADIUS Authentication Request rejected by RADIUS server.

```
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [INFO] [idlestate.go:649]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Processing
 Secondary Authentication Response
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [ERROR] [GenericAAA.go:1173]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Secondary
Authentication Failed: REJECT
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [Genericutil.go:681]
[smf-service.smf-app.gen] Internal Transaction Submit with BP for MessageType: 118, SLA: 0

[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [idlestate.go:169]
[smf-service.smf-app.gen] inCallStatus:9

*********************************************
Transaction Log received from Instance: smf.radius-ep.ajay-smf1.smf.0
************* TRANSACTION: 00004 *************
TRANSACTION SUCCESS:
    Txn Type             : SecondaryAuthenReq(2004)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/12/09 09:20:13.756 [TRACE] [infra.message_log.core] >>>>>>>>
```

```
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest for User
[msisdn-9884886688]
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Created new Radius Message for smf
AccessRequest
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Selected server: 209.165.200.229:1812
 , nasIP: 209.165.200.237 PID: 4194304
    2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Sending an IPC Message to UDP proxy
[198.18.1.4]
    2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response received on
channel
    2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] Authentication Result for user
[8899776655] = [REJECT]
    2020/12/09 09:20:13.764 [TRACE] [infra.message_log.core] <<<<<<<<

**********************************************
```

Authentication Response with Incorrect Authenticator

The following is an error log for RADIUS Authentication Response with incorrect authenticator.

```
[radius-ep-n0-0] ************* TRANSACTION: 00044 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : RadiusUdpProxyMsg(2002)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] Response received
from udp proxy
[radius-ep-n0-0]    2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
 SrcPort: 1812 DestIp: 209.165.201.4 DestPort: 16384
[radius-ep-n0-0]    2020/12/09 13:20:38.874 [ERROR] [Radius.smf.AAA] PID: 4194310 - Packet
 dropped due to invalid authenticator
[radius-ep-n0-0]     2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] **********************************************
```

RADIUS Accounting

Accounting Request Timeout

The following is an error log for RADIUS Accounting Request timeout.

```
[radius-ep-n0-0] ************* TRANSACTION: 00027 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : IntSmfAcctReqMsg(3)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest for User [msisdn-9884886688]
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Created new Radius
Message for smf AccountingRequest
[radius-ep-n0-0]     2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Selected server:
209.165.201.20:1813 , nasIP: 209.165.201.4 PID: 4194304
[radius-ep-n0-0]    2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Sending an IPC Message
```

```
 to UDP proxy [209.165.201.4]
[radius-ep-n0-0]    2020/12/09 13:09:15.091 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response
 received on channel
[radius-ep-n0-0]     2020/12/09 13:09:15.091 [ERROR] [Radius.smf.AAA] Retried MaxNumber of
 times without success
[radius-ep-n0-0]     2020/12/09 13:09:15.092 [DEBUG] [Radius.smf.AAA] Int-txn Accounting
Result for user [9884886688] = [TIMEOUT]
[radius-ep-n0-0]     2020/12/09 13:09:15.092 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] ******************************************
```

Idle Timeout-based Release

Idle Timeout Received from RADIUS

The following is a sample error log for idle timeout received from RADIUS.

```
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7158] [smf-service.smf-app.gen] Idle timeout value received from Radius:
10
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7168] [smf-service.smf-app.gen] Starting cp idle timer with timeout value:
 10
```

Absolute Session Timeout Received from RADIUS

The following is a sample error log for absolute session timeout received from RADIUS.

```
[smf-service-n0-0] 2020/09/23 16:10:11.964 smf-service [DEBUG]
[Genericutil.go:7200] [smf-service.smf-app.gen] Session absolute timeout value
received from Radius: 200
```

Session Cleanup

The following is a sample error log for session cleanup.

```
[smf-service-n0-0] 2020/09/23 16:10:21.966 smf-service [WARN] [stateHandler.go:187]
[smf-service.smf-app.gen] [imsi-123456789012345:5] [imsi-123456789012345:5] [21]
TIMEOUT -- Cp Idle Session Timer Expired, Triggering release
```

Disconnect Message

Disconnect Message Received from Unknown Client

The following is a sample error log when disconnect message is received from an unknown client.

```
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [INFO] [processor.go:157] [Radius.smf.Ipc]
 Process continue - 2003
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:23] [Radius.smf.AAA] []
 [] [11] Coa/Disconnect Req received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:43] [Radius.smf.AAA] []
 [] [11] SrcIp: 209.165.201.20 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [ERROR] [coa.go:253] [Radius.smf.Ipc]
Bng Coa/Disconnect req failed - Invalid Coa Client 209.165.201.20
.
.
.
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req received
 from udp proxy
```

```
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [ERROR] [Radius.smf.AAA] Unable to process
Coa/Disconnect request - Error during init of Radius Message Invalid Coa Client 209.165.201.20
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] ********************************************
```

Disconnect Message Received with Invalid Session ID Key

The following is a sample error log when disconnect message is received with invalid session ID key.

```
[radius-ep-n0-0] ************* TRANSACTION: 00009 *************
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0]     Txn Type             : RadiusUdpProxyCoaMsg(2003)
[radius-ep-n0-0]     Priority             : 1
[radius-ep-n0-0]     Session State        : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] >>>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
received from udp proxy
[radius-ep-n0-0]    2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] SrcIp: 209.165.201.20
 SrcPort: 3799 DestIp: 209.165.201.4 DestPort: 3799
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Decoded coa message
type is DisconnectRequest
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [ERROR] [Radius.smf.AAA] Unable to process
DisconnectRequest - Error during construct Invalid DNN/IPv4Addr/IPv6Pfx value
[radius-ep-n0-0]     2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] ********************************************
```

RADIUS Test CLI support

The **RADIUS test** CLI provides a mechanism for testing network connectivity with and configuration of RADIUS authentication and accounting servers.

This functionality is useful in determining the accuracy of the system RADIUS configuration, the configuration of the subscriber profile on the RADIUS server and troubleshooting the server response time.

Testing a RADIUS Accounting Server

When used to test a RADIUS accounting server, the tool generates an accounting request message for a specific username.

Note The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, enter the following command:

test-radius accounting { all | server-group *group_name* **| server** *server_ip_address* **port** *server_port* **} { client-nas** *client_nas_ip_address* **| grinstanceid** *gr_instanceID* **| username** *user_name* **}**

NOTES:

- **all**: Specify that all configured RADIUS accounting servers be tested.

- **server-group** *group_name*: Specify the configured RADIUS authentication servers in a RADIUS server group named *group_name* for server group functionality.
- **server** *server_ip_address*: Specify the IP address of a specific RADIUS accounting server to test.
- *server_port*: Specify the TCP port over that the system must use when communicating with the RADIUS accounting server to test.
- **username** *user_name*: Specify a username that is supplied to the RADIUS server for accounting.
- **client-nas** *client_nas_ip_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.
- **grinstanceid** *gr_instanceID*: Specify the GR instance ID. The default value is local instance ID.

Important **grinstanceid** is mandatory for non-native instances.

Example

The following command verifies all the RADIUS servers.

```
test-radius accounting all
```

The following command verifies the RADIUS accounting for user *user1* for the RADIUS server with the IP address *192.0.2.0*.

```
test-radius accounting server 192.0.2.0 port 5000 username user1
```

The following command verifies the RADIUS accounting server group *star1* for user *user1*.

```
test-radius accounting server-group star1 username user1
```

Testing a RADIUS Authentication Server

When used to test a RADIUS authentication server, the tool generates an authentication request message for a specific user name.

Note The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, in the Exec mode, use the following command:

```
test-radius authentication { all | server-group group_name | server
server_ip_address port server_port } { client-nas client_nas_ip_address | grinstanceid
 gr_instanceID | username user_name | password password }
```

NOTES:

- **all**: Specify that all configured RADIUS authentication servers be tested.
- **server-group** *group_name*: Specify the configured RADIUS authentication servers in a RADIUS server group named *group_name* for server group functionality.
- **server** *server_ip_address*: Specify the IP address of a specific RADIUS authentication server to test.

- *server_port*: Specify the TCP port over that the system must use when communicating with the RADIUS authentication server to test.
- **username** *user_name*: Specify a username that is supplied to the RADIUS server for authentication. The default user name is *test*.
- **password** *password*: Specify the password associated with the username that is supplied to the RADIUS server for authentication. The default password is *test*.
- **client-nas** *client_nas_ip_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.
- **grinstanceid** *gr_instanceID*: Specify the GR instance ID. The default value is local instance ID.

Important **grinstanceid** is mandatory for non-native instances.

Example

The following command verifies all the RADIUS servers.

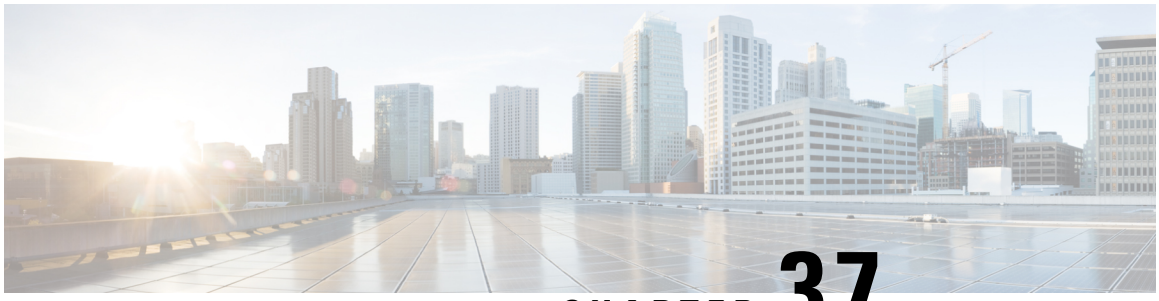
```
test-radius authentication all
```

The following command verifies the RADIUS authentication for user *user1* for the RADIUS server with the IP address *192.0.2.0*.

```
test-radius authentication server 192.0.2.0 port 5000 username user1
password dummyPwd
```

The following command verifies the RADIUS authentication server group *star1* for user *user1*.

```
test-radius authentication server-group star1 username user1
```



CHAPTER 37

Redundancy Support

- Feature Summary and Revision History, on page 1189
- Feature Description, on page 1190
- Types of Redundancies Supported, on page 1190
- High Availability Support, on page 1191
- Inter-Rack Redundancy Support, on page 1198
- Inter-site Geographic Redundancy, on page 1265

Feature Summary and Revision History

Summary Data

Table 394: Summary Data

Applicable Product or Functional Area	SMF
Applicable Platform	SMI
Feature Default Setting	• Redundancy Support: Enabled - Configuration required to disable. • Traffic Monitoring on L2 VIP for Active Instance: Disabled - Configuration required to enable. • Geo Strengthening: Enabled - Configuration required to disable. • Minimize Session Loss During Application VIP switchover: Not Applicable.
Related Documentation	Not Applicable

Revision History

Table 395: Revision History

Revision Details	Release
Enhanced the High Availability Redundancy support to minimize the session loss during application VIP switchover between master nodes.	2023.04.0
Support added for the following sub-features: • Traffic Monitoring on L2 VIP for Active Instance. • Inter-site Redundancy. • GR Strengthening.	2023.03.0
Support added for Maintenance Mode.	2021.04.0
Geographic Redundancy (GR) support introduced.	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description

This chapter provides an overview of the redundancy features, the architecture, and the configurations required to achieve the functionality in the failover scenario.

Types of Redundancies Supported

SMF supports following types of redundancies:

Redundancy Type	Description
Server	The solution is designed to sustain server failures and distribute the workload to another server in the cluster. In this scenario, most of the essential and service critical pods are running in Active and Standby modes, and they reside on a different server to cause minimum impact in the event of a hardware failure.
Rack	In this scenario, the Kubernetes cluster is mirrored in the same Data Center, but on different racks. In case of multiple server failures, software failures, or an adjacent routing layer issue, the sessions are switched to other racks. This way, it is assured to achieve the same level of service from the new rack.

Redundancy Type	Description
Site	In this scenario, the Kubernetes cluster is mirrored in different geographical data centers. In case of a whole data center is downtime, the sessions are switched to the other rack in a different data center. Through this, it is assured to achieve the same level of service from the new rack.

High Availability Support

Table 396: Feature History

Feature Name	Release Information	Description
Minimizing Session Loss During Application VIP switchover	2023.04	The High Availability redundancy support is enhanced in SMF in a way that when the gRPC IPC stream breaks, the App-Infra library re-tries immediately and the IPC connection is re-established between gRPC endpoints within milliseconds.

Feature Description

The SMF is built on the Kubernetes cluster strategy so that it inherits the high availability aspects of K8 cluster deployments. The SMF uses the construct that includes the components such as pods and services.

Each pod has at least 2 instances to ensure high availability against

- Pod instance restart or failure
- Pod lost due to node restart or failure

For details on the pods and services, see the Pods and Services Reference, on page 973 chapter in this guide.

High Availability of UDP Proxy

The SMF supports High Availability (HA) of UDP proxy. The HA model of UDP proxy is based on the keepalived virtual IP concepts.

For more information on UDP proxy redundancy, see the High Availability for the UDP Proxy, on page 978 section in the Pods and Services Reference, on page 973 chapter.

High Availability of Node Manager

The SMF supports IPAM redundancy and load balancing for each UPF. The IPAM running in the Node Manager microservice has two IPAM instances that are associated to each UPF. When one IPAM instance is inactive, the other IPAM instance manages the address allocation requests for the UPF.

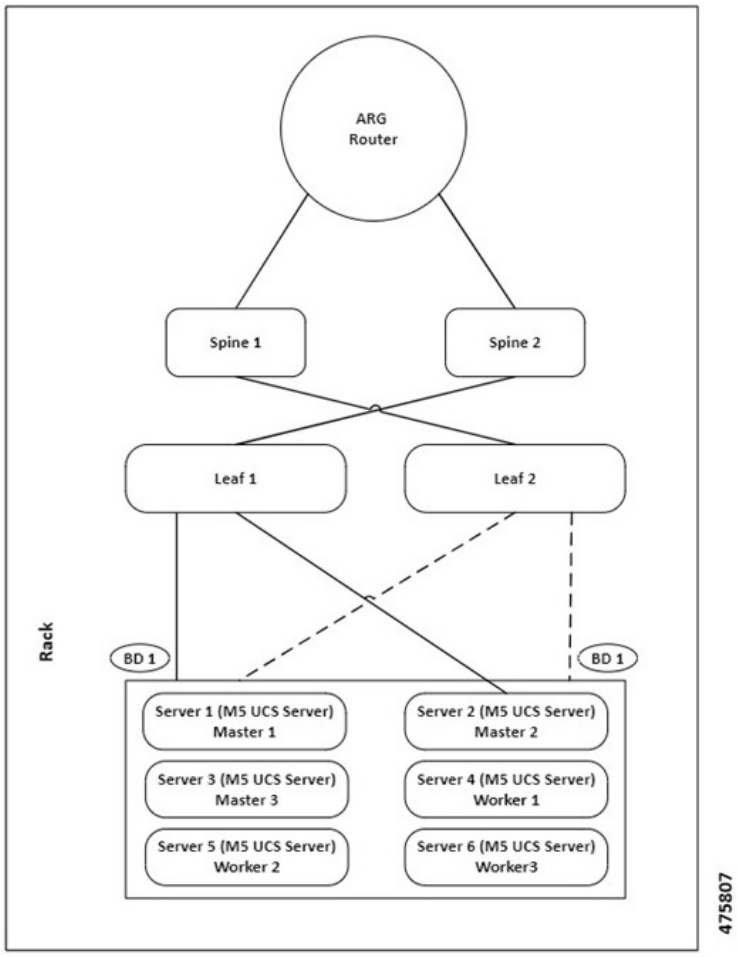
For more information on node manager redundancy, see the IPAM Redundancy Support Per UPF, on page 771 section in the IP Address Management, on page 737 chapter.

High Availability Inside Rack

High availability inside rack is an arrangement that handles server level redundancies. In this solution, in case of a single server failure, a few pods according to the design might get distributed in another available server. Meanwhile, other pods remain in pending state until the server comes back.

In this scenario, the critical pods that handle the external traffic run on Active-Stand-by pair on a different server. The redundancy support in the routing layer is provided by leaf and spine layers.

Figure 228: High Availability Layout



Architecture

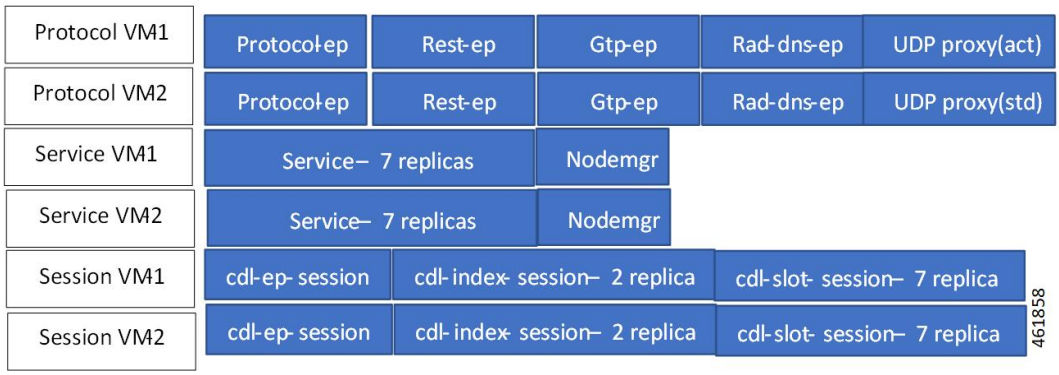
This section describes the recommended layout of SMF pods and VMs.

SMF Pod and VM Deployment Layout

This section describes the deployment of SMF pods and its microservices.

The following figure shows the deployment model of six VMs in SMF.

Figure 229: VM Deployment Model



In this model, the pods are deployed on VM pairs. Two replicas are available for each protocol pod (for example, rest-ep, protocol-ep, and gtp-ep). One instance is deployed on each protocol VM.

Similarly, service pods and session pods are distributed on both the service and session VMs equally. Such a distribution is controlled by labelling the VMs as well as implementing the K8 affinity and anti-affinity rules during pod scheduling.

This model ensures that, during VM reboot scenarios, at least 50% of the replicas of each pod type are available to handle user signaling.

Graceful pod restart allows pod to complete ongoing processing within 30 seconds. Abrupt pod restart will affect ongoing transactions without impact to PDU sessions.

How It Works

This section provides information on how the resiliency and HA can be achieved.

The SMF enables inter-pod communication during the pod failure or restart.

During a graceful pod restart:

- Ongoing processing is not impacted.
- New messages are not sent to this pod through the Kubernetes service.
- Messages with session affinity continue to be received by this pod.
- Existing call flow expected to complete within 30 seconds.

After the pod restarts:

- All Prometheus metrics of the pod are reset.
- Internal pod diagnostics once passed, the pod's status is changed to ready.
- The pod is ready to process the new messages.

When the SMF VM reboots or the VM is unavailable,

- All pods on the VM are lost.
- Pods on other available VM continue processing, thus providing high availability.

- VIP if present is switched to the other available node.
- It takes about 5 minutes of node unreachability for Kubernetes to detect the node as down.
- Pods on the node are thereafter not discoverable through the Kubernetes service.

After the pod restarts, pods on the VM are scheduled one after another. This operation is similar to the pod restart.

During the VIP and VM reboot, virtual IP is associated with a single VM. UDP proxy binds to N4 VIP address for communication with UPF. UDP proxy binds to S5 VIP address for communication with cnSGW.

Reboot of VM with active VIP causes VIP to switch to other protocol VM. The active UDP proxy failure causes VIP to switch to the other protocol VM.

Before the Subscriber Microservices Infrastructure (SMI) handles the VIP monitoring and switchover, make sure that the appropriate VIP configuration is available in the SMI deployer. Also, check if the port is set to 28000 and the host priority is equal.

The BGP-speaker monitors the IP address changes on its node. In case of addition or deletion of service IP addresses, it immediately advertises them with the proper Med value using "IP monitor" support by netlink.

During the VIP switchover, when the gRPC IPC stream breaks, the App-Infra library re-tries immediately and IPC connection is reestablished between gRPC endpoints within milliseconds.

During BGP POD graceful shutdown, all VIPs failover to other master and the traffic should be served by the other node immediately. To take immediate traffic of the peer pod/node, the shutting pod reduces Med preference, i.e., 1217/1218.

BGP speaker needs to move the VIP immediately to other master, when the BFD links are detected as down from both the leafs. This is achieved by restarting the monitoring of Keepalived interfaces from the BGP speaker and identify when the BFD links are down.

Configuring Pod-level Labelling and Replicas

The node label is configured on the SMI cluster deployer. For information on the configuration commandsin the chapter.

Configuration Example

The following is an example of VM labelling and replica configuration.

```
k8 label protocol-layer key smi.cisco.com/node-type value smf-proto
exit
k8 label service-layer key vm-type value smf-svc
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit

endpoint pfcp
 replicas 1
 nodes    2
exit
endpoint service
 replicas 1
 nodes    2
exit
```

```
endpoint protocol
 replicas 1
 nodes    2
 vip-ip 209.165.201.28
exit
endpoint sbi
 replicas 1
 nodes    2
```

Configuration Verification

To verify the configuration, use the following show command:

show running-config instance instance-id *instance_id* **endpoint**

The following is an example output of this show command.

```
[unknown] smf# show running-config instance instance-id 1 endpoint
instance instance-id 1
 endpoint nodemgr
  replicas 1
  nodes    2
 exit
 endpoint gtp
  replicas 1
  vip-ip 209.165.202.149
 exit
 endpoint pfcp
  replicas                2
  enable-cpu-optimization true
  interface n4
   heartbeat
    interval               0
    retransmission-timeout 3
    max-retransmissions    5
   exit
  exit
 exit
 endpoint service
  replicas 2
 exit
 endpoint protocol
  replicas 1
  vip-ip 209.165.202.149
 exit
exit
```

This command output displays the configurations related to multiple endpoints, such as endpoint names, pod replicas, nodes, and so on.

Traffic Monitoring on L2 VIP for Active Instance

Feature Description

SMF identifies active L2 VIPs on the protocol node that do not have any traffic. If case of an active L2 VIPs, there may not be any traffic due to various reasons, including network connectivity issues.

Upon detecting the no traffic scenario on active L2 VIPs, the SMF attempts to restart the pod or triggers the GR based on the CLI configuration action. It facilitates the restoration of traffic resulting in minimal loss of sessions.

This feature can be enabled or disabled using a CLI.

How It Works

- The traffic monitoring on IPC L2 VIP happens periodically and is matched with configurable **no-traffic-duration** time.
- If there is no traffic on the active IPC L2 VIP for the configured time duration, depending on the action configured either the GR trigger happens, so that other rack can handle the traffic, or the pod restarts, so that VIP switches to the other pod restoring traffic.
- If a pod restart action is configured and even after the VIP switchover if traffic is not restored, the IPC connection monitoring feature will trigger the GR scenario if configured to minimize the impact.
- Following checks are monitored periodically. If the checks fulfill the condition, the traffic is monitored:
  - CLI config **no-traffic-duration** should be greater than 10 seconds.
  - CLI config **session-threshold** should be greater than or equal to 1000. The default value is 1000.
  - Whether any of the GR Instance ID roles is PRIMARY.
  - Whether internal VIP is present on the protocol node.
  - If the session count is greater than or equal to the session threshold configured using the CLI, traffic monitoring is triggered. However, if the session count is less than 1000, traffic monitoring is stopped.
- Single IPC endpoint handles traffic for both the GR Instance IDs in GR mode. Traffic monitoring on IPC endpoint will not be GR Instance ID specific. However, checks are done for both the GR Instance IDs.

Configuring HA and GR Scenarios

Use the following configuration to trigger HA (pod-restart) scenario or GR (trigger-switch-over) scenario:

```
config
   monitor
      active-instance-traffic {  no-traffic-duration no_traffic_duration
session-threshold session_threshold action { pod-restart | trigger-switch-over  } }
```

NOTES:

- **active-instance-traffic**—Specify this keyword to enable or disable active traffic monitoring.
- **no-traffic-duration** *no_traffic_duration*—Maximum allowed time in seconds of no traffic on active instance. The value range is 10-300. There is no default value set for this CLI. The value of **no-traffic-duration** should be less than the value of **max-conn-downtime** if set.
- **session-threshold** *session_threshold*—Minimum session count required to start the active instance traffic monitoring. The value range is 10-10000000. The default value is 1000.
- **action {** *pod-restart* | *trigger-switch-over* **}**—Action to take on condition fulfillment. The possible values for this command are *pod-restart* and *trigger-switch-over*. The default value is *pod-restart*.

Configuration Example

Following example shows the configuration of this feature:

```
smf(config)# monitor active-instance-traffic no-traffic-duration 15 session-threshold 1000
 action pod-restart
```

Configuration Verification

Following show command displays the output for this feature:

```
smf# show running-config monitor active-instance-traffic
monitor active-instance-traffic no-traffic-duration 15 session-threshold 1000 action
pod-restart
```

OAM Support

This section defines various statistics supported in this feature.

KPI

Following KPIs are supported as part of this feature:

Active Instance Traffic Monitor Services KPI

KPI Name	Description	Labels
active_instance_traffic_monitor_services	This statistic displays services which have registered for traffic monitoring.	interface_name internal_vip_ip

Active Instance Traffic Monitor Status KPI

KPI Name	Description	Labels	Possible Values
active_instance_traffic_monitor_status	This statistic displays the status of active instance traffic monitoring.	interface_name internal_vip_ip	0 – Not Monitoring 1 – Monitoring

Active Instance Traffic Monitor Reason KPI

KPI Name	Description	Labels	Possible Values
active_instance_traffic_monitor_reason	This statistic displays the reason if conditions do not meet for active instance traffic monitoring in the monitoring or not-monitoring state.	interface_name internal_vip_ip	1 - GR Instance ID is not Primary 2 - Current session count is less than session threshold count 3 - Internal VIP not active 4 - Active Instance Traffic Monitor not configured

Active Instance Traffic Monitor Session Count KPI

KPI Name	Description	Labels
active_instance_traffic_monitor_session_count	This statistic displays the current session count.	interface_name internal_vip_ip

Note The count displayed will be from the affinity cache.

Active Instance Traffic Monitor Last Received Traffic KPI

KPI Name	Description	Labels
active_instance_traffic_monitor_last_recv_traffic	This statistic displays the last received traffic time in seconds.	interface_name internal_vip_ip

Note This statistic will be calculated only when all the conditions of the **active instance traffic monitor** are met.

Inter-Rack Redundancy Support

Inter-Rack redundancy support refers to the ability of a system or service to maintain its functionality and availability in the event of a failure or outage in one rack can be mitigated by moving the operations to another rack in the same geo location.

Feature Description

The SMF supports Inter-Rack redundancy in the active-active mode. The Inter-Rack redundancy is achieved through replication of sessions, configuration, and any other data required for seamless failover and failback of services to the remote rack.

How It Works

SMF (CNF) can be deployed in the same data center to provide service for a catastrophic failure localized to a rack hosting an SMF SMF cluster.

Each CNF instance service registers with NRF and S11/S5 for DNS entry for MME/SGW. Local HA redundancy allows instance to achieve rack level redundancy in addition to K8 cluster level failures within same data center or handle locally within same K8 cluster if failed containers are per Type-2 < *n*.

where, *n* is a value. For less than 50% of container failures, HA should handle the failures. For more than 50% of container failures, Inter-rack switchover is triggered.

Overview

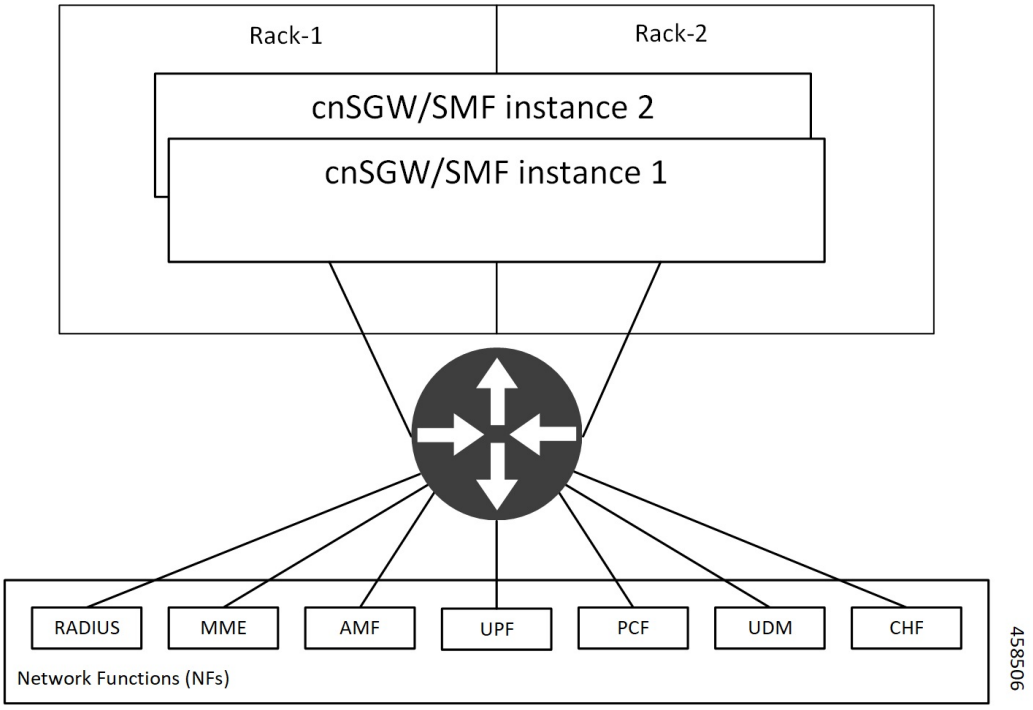
In active-active mode,

- The inter-rack deployment is transparent to the adjacent NFs.
- The inter-rack deployment contains two instances of the CCG function, each instance manifest itself with a set of interface IPs.
- Each instance support sets of sessions and continue to use the same IP for session consistency.
- At a specific time period, one CCG instance can be primary only on one rack and standby on the other rack.
- The set of interface IPs that are associated with the CCG instance, dynamically route to the primary rack of the instance.

SMF supports primary/standby redundancy in which data is replicated from the primary to standby instance. The primary instance provides services in normal operation. If the primary instance fails, the standby instance becomes the primary and takes over the operation. To achieve inter-rack redundancy, two primary/standby pairs can be set up where each rack is actively processing traffic and standby is acting as backup for the remote rack.

In an Active-Active inter-rack redundancy deployment, consider there are two racks: Rack-1 and Rack-2 located in the same data center. All the NFs are trying to reach instance-1 and instance-2.

Figure 230: Active-Active Inter-Rack Redundancy Deployment



For NFs, both the instances are active. But in real, instance-1 and instance-2 are divided across racks.

Rack-1 has instance-1 and instance-2. In a pre-trigger scenario, instance-1 is local and acts as Primary and instance-2 is in Standby mode.

Rack-2 also has instance-1 and instance-2. In a pre-trigger scenario, instance-2 is local and acts as Primary and instance-1 is in Standby mode.

In case, if Rack-1 goes down, the traffic moves to Rack-2. On Rack-2 both the instances, instance-1 and instance-2 acts as Primary.

Inter-Rack Redundancy Triggers

Inter-rack redundancy supports the following triggers:

- **CLI-based Switchover:** Manual CLI commands are used to switch the roles and trigger inter-rack redundancy failover.
- **BFD Link Failover Detection:** When both the BFD links between the connected rack and the leafs are down, inter-rack redundancy failover is triggered.
- **Local Rack POD Failure Detection:** When threshold percentage of POD replica-sets failing is greater than the configured threshold value, the inter-rack redundancy failover is triggered.
- **Remote Rack POD Failure Detection:** When the remote POD monitoring detects failure breaching threshold percentage, the POD becomes self-primary for that instance.
- **Remote Rack Role Monitoring:** When the remote role monitoring detects that the rack is in Standy_error state, it becomes self-primary.
- **Multi-Compute Failure:** When two or more servers are powered down, it triggers inter-rack redundancy failover.

Rack NF Roles

The following is a list of applicable rack NF roles:

Note

- The **Cachepod**/**ETCD** and the **CDL Replication** happen during all the roles mentioned in the following section.
- If the inter-rack links are down or under periodic heartbeat fails, then these inter-rack redundancy triggers get suspended.

- **PRIMARY**: In this role, the rack is in ready state and actively taking traffic for the given instance.
- **STANDBY**: In this role, the rack is in standby mode, ready to take traffic, but not taking traffic for the given instance.
- **STANDBY_ERROR**: In this role, the rack is in problem state, not active, and not ready to take traffic for the given instance.

Note When the instance role is in **STANDBY_ERROR**, data replication gets halted. The command **show georeplication-status** consistently fails under this condition. However, once the instance role gets transitioned to **STANDBY**, data replication resumes automatically, and the command displays the result as **pass**.

- **FAILOVER_INIT**: In this role, the rack has started to fail over and not in condition to take traffic. The buffer time is two seconds for the application to complete their activity.

For fresh installation, the rack boots-up with the following roles:

- **PRIMARY**: In this role, the rack is in for the local instance (each rack has local **instance-id** configured to identify the local instance). It is recommended not to configure the pods for monitoring during fresh installation. Once the setup is ready, you can configure the pods for monitoring.
- **STANDBY**: In this role, the rack is in for other instances.

For upgrades, the rack boots-up with the following roles:

- **STANDBY_ERROR**: In this role, the rack is for all the instances as moving the traffic post upgrade needs manual intervention.

General Guidelines

Before configuring the inter-rack redundancy deployment, here are some general guidelines:

- Both racks should be on the same software version.
- Both racks should be configured with same configuration.
- Loopback port of Instance 1 and Instance 2 should be different. Else, REST-EP POD would not come up due to K8 IP/Port conflict.
- Respective interface on both the racks should be on the same VLAN. For example, N4 VLAN of Instance1 and Instance2 should be on the same VLAN. Else, there is a route conflict on Kernel while enforcing BGP policies.
- Consult your Cisco Technical Representative to perform the following procedures to make sure proper roles are assigned.

  For more information, see Software Upgrade on GR Pairs, on page 1227.
- Post failover, perform the failback manually after ensuring the rack is healthy. Autonomous failback is not supported.

  For more information, see Recovery Procedure, on page 1249.
- Use non-bonded interface in BGP speaker PODs for BGP peering.
- BGP peering per Proto node is supported with only two BGP routers/leafs. Considering two Proto nodes, there can be maximum of four BGP neighborships.
- Use bonded interfaces for Service traffic.
- Geo pod uses two VIPs:
  - Internal-VIP for Inter-POD communication (within the rack)
  - External-VIP for Inter-rack Geo pod communication. Configure only on Proto Nodes on L2 Subnet. This is used to communicate across the racks. This node has external connectivity to other rack.
- Geo Internal IP to be reachable to all nodes within the rack.
- Geo External IP:

- CDL/Kafka VIPs: Configure on CDL Labeled Nodes on L2 Subnet.
- Enable LI tapping on both the racks.
- MDF server should be reachable from both the racks.

Instance Awareness

Instance awareness configuration in SMF helps to distinguish local rack instance and remote rack instance.

Configuring Inter-Rack Redundancy Instance

This configuration is needed to provide a inter-rack redundancy configuration for multiple rack. With instance ID, endpoint configurations should be configured for each rack.

Sample Configuration 1

The following is a sample configuration for endpoint VIP configuration under one instance:

```
config
  instance instance-id gr_instanceId
    endpoint endpoint_name
        vip-ip vip_ip_address
  exit
exit
```

Example:

```
config
instance instance-id 1
 endpoint sbi
  vip-ip 209.165.201.21
 exit
exit
```

Sample Configuration 2

The following is a sample configuration to provide information on system-id, cluster-id and slice-name under an instance:

```
config
  instances instance instance_id
   system-id system_id
   cluster-id cluster_id
   slice-name cdl_slice_name
  exit
exit
```

Example:

```
config
 instances instance 1
  system-id smf
  cluster-id smf
  slice-name 1
 exit
exit
```

Note It is recommended to have the same values for *system-id*, *cluster-id* in the instance, and *app-name*, *cluster-name* in deployment.

Configuring Endpoint Instance Awareness

Only two instances can be configured on each local and remote rack, and corresponding endpoints can be instantiated.

A local instance-id is the identity of the local rack irrespective of if the rack is redundant or not.

Local Instance ID Configuration

The local instance is configured using the local-instance command.

```
local-instance instance 1
```

Endpoint configuration must be under instance specified by each unique instance ID.

Endpoint Configuration Example

Following are a few configuration examples.

Note In the following example, *instance-id* "**1**" is a local instance-id, and endpoints configured under it belong to the local rack.

Optionally, remote rack *instance-id* "**2**" can be configured for endpoints belonging to the inter-rack.

```
instance instance-id 1
 endpoint li
  replicas 1
  nodes    2
  vip-ip 209.165.201.6
  vip-ip 209.165.201.13
 exit
 endpoint gtp
  replicas 1
  nodes    2
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.201.6
  vip-ip 209.165.201.4
  interface s5
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface s2b
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
 exit
exit
instance instance-id 2
 endpoint li
  replicas 1
```

```
  nodes    2
  vip-ip 209.165.201.6
  vip-ip 209.165.201.13
 exit
exit
endpoint gtp
  replicas 1
  nodes    2
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.201.6
  vip-ip 209.165.201.5
  interface s5
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface s2b
   echo interval 60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
 exit
exit
```

Configuring Profile SMF Instance Awareness

Add instance for PGW FQDN corresponding to local and remote instances.

Example

Following is a configuration example.

Note In the following example, *instance-id* "**1**" is a local instance-id, and the SMF profile configured under it belongs to the local rack.

Optionally, remote rack *instance-id* "**2**" can be configured for FQDN belonging to the inter-rack.

```
profile smf smf1
locality LOC1
allowed-nssai [ slice1 ]
instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123
instances 2 fqdn cisco.com.apn.epc.mnc567.mcc123
```

Dynamic Routing

Border Gateway Protocol (BGP) allows you to create loop-free inter-domain routing between autonomous systems (AS). An AS is a set of routers under a single technical administration. The routers can use an Exterior Gateway Protocol to route packets outside the AS. The Dynamic Routing by Using BGP feature enables you to configure the next-hop attribute of a BGP router with alternate local addresses to service IP addresses with priority and routes. The App-Infra BGP speaker pods enable dynamic routing of traffic by using BGP to advertise pod routes to the service VIP.

This feature supports the following functionality:

- Dynamic routing by using BGP to advertise service IP addresses for the incoming traffic.
- Learn route for outgoing traffic.

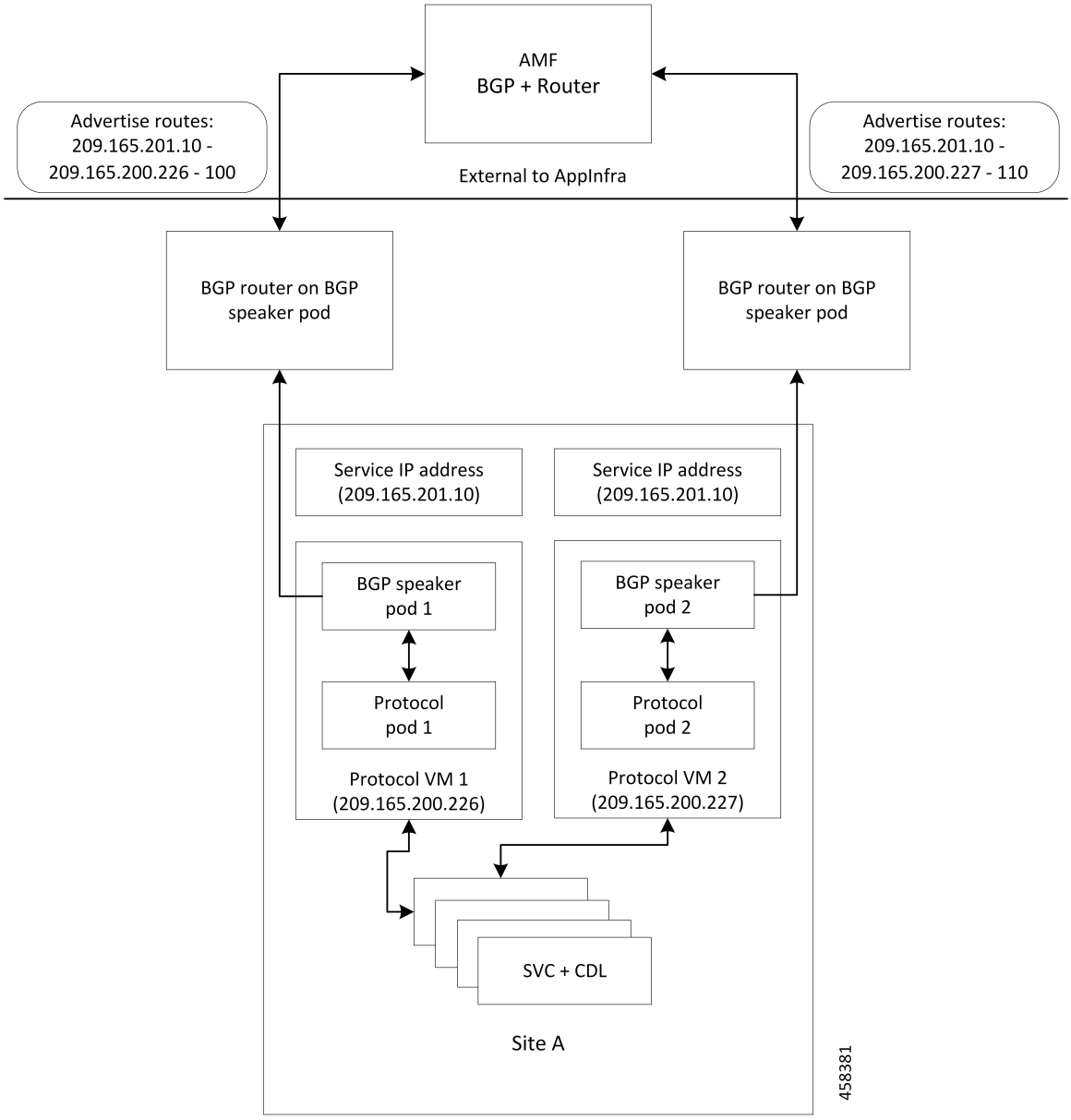
- Handling a BGP pod failover.
- Handling a protocol pod failover.
- Statistics and KPIs for the BGP speakers.
- Log messages for debugging the BGP speakers.
- Enable or disable the BGP speaker pods.
- New CLI commands to configure BGP.

Incoming Traffic

BGP uses TCP as the transport protocol, on port 179. Two BGP routers form a TCP connection between one another. These routers are peer routers. The peer routers exchange messages to open and confirm the connection parameters.

The BGP speaker publishes routing information of the protocol pod for incoming traffic in the active standby mode. Use the following image as an example to understand the dynamic routing functionality. There are two protocol pods, pod1 and pod2. Pod1 is active and pod2 is in the standby mode. The service IP address, 209.165.200.225 is configured on both the nodes, 209.165.200.226 and 209.165.200.227. pod1 is running on host 209.165.200.226 and pod2 on host 209.165.200.227. The host IP address exposes the pod services. BGP speaker publishes the route 209.165.200.225 through 209.165.200.226 and 209.165.200.227. It also publishes the preference values, 110 and 100 to determine the priority of pods.

Figure 231: Dynamic Routing for Incoming Traffic in the Active-standby Topology



For high availability, each cluster has two BGP speaker pods with Active-standby topology. Kernel route modification is done at host network level where the protocol pod runs.

MED Value

The Local Preference is used only for IGP neighbours, whereas the MED Attribute is used only for EGP neighbours. A lower MED value is the preferred choice for BGP.

Table 397: MED Value

Bonding Interface Active	VIP Present	MED Value	Local Preference
Yes	Yes	1210	2220
Yes	No	1220	2210
No	Yes	1215	2215
No	No	1225	2205

Bootstrap of BGP Speaker Pods

The following sequence of steps set up the BGP speaker pods:

1. The BGP speaker pods use TCP as the transport protocol, on port 179. These pods use the AS number configured in the Ops Center CLI.
2. Register the Topology manager.
3. Select the Leader pod. The Active speaker pod is the default choice.
4. Establish connection to all the BGP peers provided by the Ops Center CLI.
5. Publish all existing routes from ETCD.
6. Configure import policies for routing by using CLI configuration.
7. Start gRPC stream server on both the speaker pods.
8. Similar to the cache pod, two BGP speaker pods must run on each Namespace.

For more information on Dynamic Routing, see the *Dynamic Routing by Using BGP* chapter in the *UCC 5G Session Management Function - Configuration and Administration Guide*.

Configuring Dynamic Routing Using BGP

This section describes how to configure the dynamic routing using BGP.

Configuring AS and BGP Router IP Address

To configure the AS and IP address for the BGP router, use the following commands:

```
config
  router bgp local_as_number
  exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.

Configuring BGP Service Listening IP Address

To configure the BGP service listening IP address, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.

Configuring BGP Neighbors

To configure the BGP neighbors, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
      neighbor neighbor_ip_address remote-as as_number
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.
- **neighbor** *neighbor_ip_address*—Specify the IP address of the neighbor BGP router.
- **remote-as** *as_number*—Specify the identification number for the AS.

Configuring Bonding Interface

To configure the bonding interface related to the interfaces, use the following commands:

```
config
   router bgp local_as_number
      interface interface_name
      bondingInterface interface_name
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **interface** *interface_name*—Specify the name of the interface.
- **bondingInterface** *interface_name*—Specify the related bonding interface for an interface. If the bonding interface is active, then the BGP gives a higher preference to the interface-service by providing a lower MED value.

Configuring Learn Default Route

If the user configures specific routes on their system and they need to support all routes, then they must set the **learnDefaultRoute** as **true**.

Note This configuration is optional.

To configure the Learn Default Route, use the following commands:

```
config
   router bgp local_as_number
      learnDefaultRoute true/false
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **learnDefaultRoute** *true/false*—Specify the option to enable or disable the **learnDefaultRoute** parameter. When set to true, BGP learns default route and adds it in the kernel space. By default, it is false.

Configuring BGP Port

To configure the Port number for a BGP service, use the following commands:

```
config
   router bgp local_as_number
      loopbackPort port_number
   exit
exit
```

NOTES:

- **router bgp** *local_as_number*—Specify the identification number for the AS for the BGP router.
- **loopbackPort** *port_number*—Specify the port number for the BGP service. The default value is 179.

Policy Addition

The BGP speaker pods learns many route information from its neighbors. However, only a few of them are used for supporting the outgoing traffic. This is required for egress traffic handling only, when SMF is sending information outside to AMF/PCF. Routes are filtered by configuring import policies on the BGP speakers and is used to send learned routes to the protocol pods.

A sample CLI code for policy addition and the corresponding descriptions for the parameters are shown below.

```
$bgp policy <policy_Name> ip-prefix 209.165.200.225 subnet 16 masklength-range 21..24
as-path-set "^65100"
```

Table 398: Import Policies Parameters

Element	Description	Example	Optional
as-path-set	AS path value	"^65100"	Yes

Element	Description	Example	Optional
ip-prefix	Prefix value	“209.165.200.225/16”	Yes
masklength-range	Range of length	“21..24”	Yes
interface	Interface to set as source IP (default is VM IP)	eth0	Yes
gateWay	Change gateway of incoming route	209.165.201.30	Yes
modifySourceIp	Modify source ip of incoming route Default value is False.	true	Yes
isStaticRoute	Flag to add static IP address into kernel route Default value is False.	true	Yes

Configuring BGP Speaker

This configuration controls the number of BGP speaker pods in deployment. BGP speaker advertises service IP information for incoming traffic from both the racks.

Note

- Use non-bonded interface in BGP speaker pods for BGP peering.
- BGP peering per Proto node is supported with only two BGP routers/leafs. Considering two Proto nodes, there can be maximum of four BGP neighborships.

```
instance instance-id  instance_id endpoint bgpspeaker interface { bgp | bfd
 } internal base-port start base_port_number
```

```
config
instance instance-id instance_id
 endpoint bgpspeaker
   replicas replica_id
   nodes node_id
   interface bgp
     internal base-port start base_port_number
   exit
   interface bfd
     internal base-port start base_port_number
  exit
exit
```

NOTES:

- **instance instance-id** *instance_id*—Specify the GR instance ID.
- *base_port_number*—Specify the port range only if logical NF is configured. This range depends on your deployment.

Example

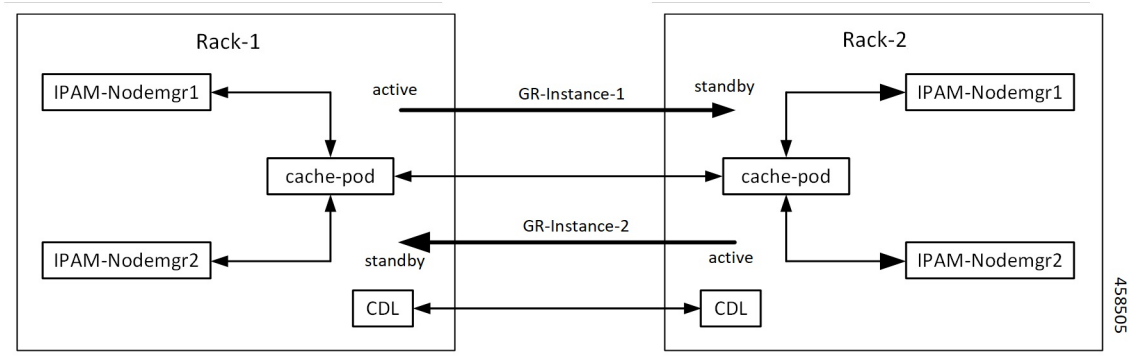
The following is a configuration example:

```
instance instance-id 1
endpoint bgpspeaker
   replicas 1
   nodes    2
   interface bgp
     internal base-port start {24000}
   exit
   interface bfd
     internal base-port start {25000}
 exit
```

IPAM

This section describes IP Address Management (IPAM) at the rack level.

Figure 232: IPAM



During UPF registration, active IPAM instance reserves four address-ranges per UPF per DNN.

- Range-1: Active cluster, nodemgr-1
- Range-2: Active cluster, nodemgr-2
- Range-3: Standby cluster, nodemgr-1
- Range-4: Standby cluster, nodemgr-2

During normal operation, Rack-1 handles UPF-register/release, address-allocate/release for subscribers coming up in GR-instance-1.

If Rack-2 goes down, Rack-1 gets role-change trigger for GR-Instance-2.

- IPAM in Rack-1, restores the content of GR-Instance-2 from local-cache-pod (which was already synced)
- IPAM in Rack-1 handles UPF-Register/Release and address-allocate/release for subscribers coming up with GR-Instance-2 using the restored content in addition to handling GR-Instance-1.

Each IPAM pool is associated to a GR-Instance, with the following:

- Pool name is unique across all the instances.
- Address-ranges are unique within VRF and across all the instances.

The same pool configuration must be configured in both the active and standby SMF clusters of a particular instance.

During address-allocation, active instance assign free-IP from reserved address-range for the UPF.

Incase new address-ranges is not available, change ownership of standby's address-range to current active instance and continue assigning address-ranges from it.

Configuring IPAM

The following section provides IPAM configuraton examples.

SMF-1 Example

The following is a configuration example for SMF-1:

```
ipam
 instance 1
  address-pool pool-1
  vrf-name ISP
   tags
   dnn dnn-1
  exit
  ipv4
    address-range 209.165.201.1 209.165.201.31
 exit
instance 2
 address-pool pool-2
  vrf-name ISP
  tags
   dnn dnn-2
  exit
  ipv4
    address-range 209.165.202.129 209.165.202.159
 exit
exit
```

SMF-2 Example

The following is a configuration example for SMF-2:

```
ipam
 instance 1
 address-pool pool-1
  vrf-name ISP
  tags
   dnn dnn-1
  exit
  ipv4
    address-range 209.165.201.1 209.165.201.31
 exit
 instance 2
 address-pool pool-2
  vrf-name ISP
   tags
   dnn dnn-2
  exit
  ipv4
    address-range 209.165.202.129 209.165.202.159
 exit
exit
```

Geo Replication

The Geo-replication is used in inter-rack communication and for POD or VIP or BFD monitoring within the rack. The Geographic Redundancy comprises with the following:

- Two instances of Geo pods are running for each rack.
- Two Geo pods functions in Active-Standby mode.
- Each Geo pod instance is spawned on a different Proto node or VM.
- Geo pod running on the Proto node or VM having VIP is Active Geo pod.
- In the event of Active Geo pod restart, VIPs get switched to other Proto node or VM and Standby Geo pod running on the other Proto node/VM becomes active.
- Geo pod uses host networking mode (similar to UDP-Proxy).
- Geo pod uses two VIPs:
  - **Internal**: VIP for Inter-POD communication (within the rack)
  - **External**: VIP for Inter-rack Geo pod communication

    It configures only on Proto Nodes on the L2 Subnet. It's used to communicate across the racks. This node has external connectivity to other Rack.
- Logical-NF-InstanceID must be configured same for both SMFs in GR-Pair.
- For KeepAliveD monitoring:
  - Geo pod uses base port as: 15000+(Logical-NF-InstanceID * 32) + 4

    Geo pod base port must be different than BGP speaker pod port.
    - The default port (without logical SMF) as: 15004
    - For Logical SMF configured with logical-nf-instance-id as 1, and then the port as: 15036
  - UDP-Proxy pod uses base port as: 28000+Logical-NF-InstanceID.
    - The default port (without logical SMF) as: 28000
    - For Logical SMF configured with logical-nf-instance-id as 1, and then the port as: 28001
  - BGPSpeaker-pod uses default base port as: 20000+(Logical-NF-InstanceID * 32)+4.
    - The default port (without logical SMF) as: 20004
    - For logically SMF configured with logical-nf-instance-id as 1, and then the port as: 20036

Note Only ETCD and cache pod data gets replicated to the standby rack.

Configuring ETCD/Cachepod Replication

Endpoints must be configured under an instance. Two Geo-Redundancy pods are needed on each rack. You should also configure VIP for internal and external Geo interface for ETCD/CachePod replication.

instance instance-id *instance_id* **endpoint geo interface { geo-internal | geo-external } vip-ip {** *vip_ip_address* **} vip-port {** *vip_port_number* **}**

```
config
instance instance-id instance_id
 endpoint geo
  replicas replica_id
  nodes node_id
  internal base-port start base_port_number
  interface geo-internal
   vip-ip vip_ip_address vip-port vip_port_number
  exit
  interface geo-external
   vip-ip vip_ip_address vip-port vip_port_number
  exit
exit
exit
```

NOTES:

- **instance instance-id** *instance_id*—Specify GR instance ID. One instance ID for local rack and other for another rack.
- **vip-ip** *vip_ip_address*—Specify VIP IP address for Internal/External Geo interface.
- **vip-port** *vip_port_number*—Specify VIP port number.
- **internal base-port start** *base_port_number*—Specify port range only if logical NF is configured.

Example

The following is a configuration example:

```
instance instance-id 1
endpoint geo
  replicas 1
  nodes 2
  internal base-port start 25000
  interface geo-internal
   vip-ip 209.165.201.8 vip-port 7001
  exit
  interface geo-external
   vip-ip 209.165.201.8 vip-port 7002
  exit
exit
```

Geo Monitoring

This section describes Geo monitoring.

Pod Monitoring

To configure pod monitoring and failover thresholds in the inter-rack setup, use the following sample configuration. The geo pod monitors the configured pod name.

```
config
 geomonitor
  podmonitor pods pod_name
   retryCount value
   retryInterval interval_value
   retryFailOverInterval failover_interval
   failedReplicaPercent percent_value
  exit
 exit
```

NOTES:

- **pods** *pod_name*—Specify the name of the pod to be monitored. For example, Cache-pod, rest-ep, and so on.
- **retryCount** *value*—Specify the retry counter value to retry if pod fails to ping after which pod is marked as down. It should be an integer in the range of 1-10.
- **retryInterval** *interval_value*—Specify the retry interval in milliseconds if the pod successfully pings. It should be an integer in the range of 200-10000.
- **retryFailOverInterval** *failover_interval*—Specify the retry interval in milliseconds if the pod fails to ping. It should be an integer in the range of 200-10000.
- **failedReplicaPercent** *percent_value*—Specify the percent value of failed replica after which the inter-rack redundancy failover is triggered. It should be an integer in the range of 10-100.

Configuration Example

The following is an example configuration.

```
geomonitor podmonitor pods cache-pod
 retryCount 3
 retryInterval 5
 retryFailOverInterval 1
 failedReplicaPercent 40
exit
```

Remote Cluster Monitoring

Remote cluster monitoring auto corrects roles (it becomes self-primary, when the remote rack is in **STANDBY_ERROR** state) for uninterrupted traffic flow of traffic. However, this auto role correction gets done only for specific roles.

To configure this feature, use the following sample configuration:

```
config
   geomonitor
      remoteclustermonitor
         retryCount value
         retryInterval interval_value
         end
```

NOTES:

- **retryCount** *value*—Specify the retry count before making the current rack **PRIMARY**. It should be an integer in the range of 1-10. The default value is 3.
- **retryInterval** *interval_value*—Specify the retry interval in the count of milliseconds, after which the remote rack status gets fetched. It should be an integer in the range of 200-50000. The default value is 3000.

Configuration Example

The following is an example configuration

```
geomonitor remoteclustermonitor
retryCount 3
retryInterval 3000
```

Traffic Monitoring

The following command is used to monitor the traffic.

```
config
 geomonitor
  trafficMonitor
   thresholdCount value
   thresholdInterval interval_value
  exit
 exit
```

NOTES:

- **thresholdCount** *value*—It specifies the number of calls received for standby instance. It should be an integer in the range of 0-10000. Default value is 0. Both UDP-proxy and REST-EP must be considered for the counter value.
- **thresholdInterval** *interval_value*—It specifies the maximum duration to hit the threshold count value in ms. It should be an integer in the range of 100-10000. Default value is 3000.

Configuration Example

The following is an example configuration

```
geomonitor trafficmonitor
thresholdCount 3
thresholdInterval 3000
```

Geo Redundancy Strengthening

The geo redundancy strengthening activity addresses multiple issues stemming from different scenarios such as the following:

- Hardware failure
- Network failure
- Process failure

- Abnormal conditions
- Code walkthroughs

These failed scenarios impact the functionality of the geo-replication pod, causing the system malfunction. To address these issues, it is necessary to strengthen various areas of the geo-replication pod.

How It Works

The following areas of the enhanced geo replication pod are part of the geo redundancy strengthening feature:

- The system makes GRPC replication and admin stream available when it becomes healthy.
- The system ensures that both instances have the correct role in all scenarios.
- The system maintains data replication between the geo replication pod of rack-1 and rack-2 in sync.
- The system verifies that checksum and checkpoint data is always correct on both racks to ensure data integrity.
- The system provides a mechanism for users to sync replication data, when it becomes out of sync, and requires manual intervention.

  To know more about the command, see the Geo Replication Pull Data section.
- The system ensures that Geo VIP movement between geo replication pods does not impact functionality.
- The system takes measures to prevent failures of dependent processes from affecting its functionality for users.

Limitations

Some of the known limitations of this feature are as follows:

- **Replication Data Loss**: It can occur when a switchover occurs because both cache pods are down on the partner rack.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

KPI Support

The following set of statistics supports the geo redundancy strengthening and securing feature:

1. KPI Name: **geo_replication_finalpull_total**

   The following table lists **geo_replication_finalpull_total** KPI details.

Description	Functionality	Label Names	Possible Values
This KPI displays the total number of geo replications present in the final pull of the feature messages.	**geo_replication_finalpull_total**, it is the functionality output.	**MessageType**	It is a request or a response message type.
		TotalTimeTaken	It is the total time taken to process the request.
		GRInstanceNumber	It is the GR Instance ID in number from the list of the following: • 1 • 2 • Instance.1 • Instance.2

BFD Monitoring

Bidirectional Forwarding Detection (BFD) protocol is used for Faster Network Failure Detection along with BGP. Whenever connectivity between BGP peering fails with cluster (NF), failover is triggered to minimize traffic failure impact.

```
config
  router bgp as
    bfd interval interval min_rx min_rx multiplier multiplier
    loopbackPort loopbackPort loopbackBFDPort loopbackBFDPort
  interface interface_id (BGP on non-bonded interface <-- loopbackEth)
    bondingInterface bondingInterface (leaf6-nic)
    bondingInterface bondingInterface (leaf6-nic)
    neighbor neighbor_ip_address remote-as remote_as fail-over fail_over_type
  exit
  interface interface_id (BGP on non-bonded interface <-- loopbackEth)
    bondingInterface bondingInterface (leaf7-nic)
    bondingInterface bondingInterface (leaf7-nic)
    neighbor bondingInterface remote-as remote_as fail-over fail_over_type
  exit
  policy-name policy_name
   as-path-set as_path_set
   gateWay gateWay_address
   interface interface_id_source
   ip-prefix ip_prefix_value
   isStaticRoute false | true
   mask-range mask_range
   modifySourceIp false | true
  exit
exit
```

NOTES:

- **bgp** *as*—Specify the Autonomous System (AS) path set.
- **bfd**—Specify BFD configuration.
  - **interval** *interval* —Specify BFD interval in milliseconds.
  - **min_rx** *min_rx*—Specify BFD minimum RX in milliseconds.
  - **multiplier** *multiplier*—Specify BFD interval multiplier.
- **interface** *interface_id*—Specify BGP local interface.
  - **bondingInterface** *bondingInterface*—Specify linked bonding interface.
  - **neighbor** *neighbor_ip_address*—Specify IP address of neighbor.
    - **fail-over** *fail_over_type*—Specify failover type.
    - **remote-as** *remote_as*—Specify Autonomous System (AS) number of BGP neighbor.
- **learnDefaultRoute**—Learn default route and add it in kernel space
- **loopbackBFDPort** *loopbackBFDPort*—Specify BFD local port.
- **loopbackPort** *loopbackPort*—Specify BGP local port.
- **policy-name** *policy_name*—Specify policy name.
  - **as-path-set** *as_path_set*—Specify Autonomous System (AS) path set.
  - **gateWay** *gateWay_address*—Specify gateway address.
  - **interface** *interface_id_source*—Specify interface to set as source IP.
  - **ip-prefix** *ip_prefix_value*—Specify IP prefix value.
  - **isStaticRoute** *false | true*—Specify whether to add static route in kernel space. Default value is false.
  - **mask-range** *mask_range*—Specify mask range.
  - **modifySourceIp** *false | true*—Modify source IP of the incoming route. Default value is false.

    true: This option is used for non-UDP related VIPs. Source IP of the given interface is used as Source IP while sending out packets from SMF.

    false: This option is used for all UDP related VIPs. VIP is used as Source IP while sending out packets from SMF.

Example

Following are configuration examples:

```
router bgp 65000
  bfd interval 250000 min_rx 250000 multiplier 3
  loopbackPort 179 loopbackBFDPort 3784
interface ens160 (BGP on non-bonded interface <-- loopbackEth)
  bondingInterface enp216s0f0 (leaf6-nic)
  bondingInterface enp216s0f1 (leaf6-nic)
  neighbor leaf6-ip remote-as 60000 fail-over bfd
```

```
exit
interface ens192 (BGP on non-bonded interface <-- loopbackEth)
  bondingInterface enp94s0f1 (leaf7-nic)
  bondingInterface enp94s0f0 (leaf7-nic)
  neighbor leaf7-ip remote-as 60000 fail-over bfd
exit
policy-name allow-all ip-prefix 209.165.201.30/0 mask-range 0...32
exit
```

BGP router configuration with BFD

```
show running-config router
router bgp 65142
 learnDefaultRoute false
 bfd interval 250000 min_rx 250000 multiplier 3
 interface enp94s0f0.3921
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.201.24 remote-as 65141 fail-over bfd
 exit
 interface enp94s0f1.3922
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.24 remote-as 65141 fail-over bfd
```

Show BFD status of neighbor

```
show bfd-neigbor
status-details

----- bgpspeaker-pod-1----

Peer             Status

209.165.202.142  STATE_DOWN
----- bgpspeaker-pod-2----

Peer             Status

209.165.202.142  STATE_UP
```

```
policy-name allow-n11 ip-prefix 209.165.200.225/54 mask-range 25..32 interface bd1.n11.2271
 modifySourceIp true isStaticRoute true gateWay 209.165.201.14
```

In the above example, *modifySourceIp* is set to true.

- AMF subnet: 209.165.200.225/54

  N11 Svc Bonded Physical Interface: bd1.n11.2271 (IP address - 209.165.201.23)

  N11 Svc Bonded VxLAN Anycast GW: 209.165.201.14

  N11 VIP Address: 209.165.201.7

- SMF Outbound Packet (will have source IP as 209.165.201.23)

  Inbound Packet to SMF (will have destination IP as 209.165.201.7)

```
policy-name allow-n4-1 ip-prefix 209.165.201.17/41 mask-range 24..32 interface bd2.n4.2274
 gateWay 209.165.201.17
```

In the above example, *modifySourceIp* is set to false (default).

- UPF N4 Interface IP: 209.165.201.17/41

  N4 Svc Bonded Physical Interface: bd2.n4.2274 (IP address - 209.165.201.23)

N4 Svc Bonded VxLAN Anycast GW: 209.165.201.17

N4 VIP Address: 209.165.201.14

- SMF Outbound Packet (will have source IP as 209.165.201.14)

  Inbound Packet to SMF (will have destination IP as 209.165.201.14)

CDL GR Deployment

By default, CDL is deployed with two replicas for db-ep, 1 slot map (2 replicas per map), and 1 index map (2 replicas per map).

Note It is recommended to configure the CDL container in YANG.

Prerequisites for CDL GR

Before deploying the CDL GR, user must configure the following:

- CDL Session Database and define the base configuration.
- Kafka for CDL.
- Zookeeper for CDL.

CDL Instance Awareness and Replication

In CDL, along with existing GR related parameters, GR instance awareness must be enabled using a feature flag on all the racks. Also, the mapping of system-id to slice names should also be provided for this feature to work on all the racks.

The CDL is also equipped with Geo Replication (GR) failover notifications, which can notify the timer expiry of session data and bulk notifications to the currently active rack. The CDL uses Border Gateway Protocol (BGP) through App-Infra for the GR failover notifications.

The CDL subscribes to the key value on both the GR racks. The App-Infra sends notifications to the CDL when there is any change in these key values. A key value indicates the state of the CDL System ID or the GR instance. The GR instance is mapped to the CDL slices using the CDL system ID or the GR instance ID in the key.

The system ID is mandatory on both the racks. The GR instance ID in the NF configuration must match the CDL system ID.

CDL has instance-specific data slices. It also allows users to configure instance-specific slice information at the time of bringing up.

- CDL notifies the data on expiry or upon bulk notification request from the active slices.
- CDL determines the active instance based on the notification from app-infra memory-cache.
- CDL slice is a partition within a CDL instance to store a different kind of data. In this case, NF stores a different instance of data.

Note CDL slice name should match with the slice-name configured in GR.

Configuring CDL Instance Awareness

The following command is used to configure CDL instance awareness.

```
config
cdl
 datastore datastore_session_name
   features
    instance-aware-notification
      enable [ true | false ]
      system-id system_id
       slice-names slice_names
  end
```

NOTES:

- **datastore** *datastore_session_name*—Specify the datastore name.
- **enable [true | false]**—Enables the GR instance state check for slices.
- **system-id** *system_id*—Mapping of system ID to slice name.
- **slice-names** *slice_names*—Specify the list of slice names associated with the system ID. CDL slice name should match with the slice-name configured in GR.

Example

The following is a configuration example:

```
cdl datastore session
 features instance-aware-notification enable true
 features instance-aware-notification system-id 1
  slice-names [ sgw1 smf1 ]
 exit
 features instance-aware-notification system-id 2
  slice-names [ sgw2 smf2 ]
 end
```

Configuring CDL Replication

This section describes CDL replication configuration.

1. Configure Rack-1 CDL HA system without any Geo-HA-related configuration parameters.
   a. Set the System ID as 1 in the configuration.
   b. Set the slot map/replica and index map/replica and Kafka replica as per requirements.

   The following is a sample configuration:

   ```
   cdl system-id 1
   cdl node-type session
   cdl datastore session
   endpoint replica replica_id
   ```

```
  slot map 4
  slot replica 2
  index map 1
  index replica 2
cdl kafka replica 2
```

1. Configure external IPs on Rack-1 for Rack-2 to Rack-1 communication.
   a. Enable geo-replication on Rack-1 and configure the remote Rack as 2 for Rack-1.

      cdl enable-geo-replication *true*
   b. Configure the external IP for CDL endpoint to be accessed by Rack-2.

      cdl datastore session endpoint external-ip *site-1_external_ip*
   c. Configure the external IP and port for all Kafka replicas.

      So, if two replicas (default) are configured for Kafka, user need to provide two different <*ip*>+<*port*> pairs.

      cdl kafka external-ip *site-1_external_ip port1* **cdl kafka external-ip** *site-1_external_ip port2*

2. Add remote rack information on Rack-2.
   - Remote rack cdl-ep configuration on Rack-2:

     cdl remote-site 1 db-endpoint host *site-1_cdl_ep_ip*

     cdl remote-site 1 db-endpoint port *site-1_cdl_ep_port*

     (Port Example: 8882)
   - Remote rack Kafka configuration on Rack-2:

     cdl remote-site *1* kafka-server *site-1_kafka1_ip site-1_kafka1_port*

     cdl remote-site *1* kafka-server *site-1_kafka2_ip site-1_kafka2_port*
   - Direct the session datastore configuration to remote Rack-2 configuration:

     cdl datastore session geo-remote-site *1*
   - (Optional) Configure the SSL certificates to establish a secure connection with remote rack on Rack-1. All the certificates are in multi-line raw text format. If the certificates are not valid, the server continues with non-secure connection.

     cdl ssl-config certs *site-2_external_ip* **ssl-key** *<ssl_key>*

     cdl ssl-config certs *site-2_external_ip* **ssl-crt** *<ssl_crt>*

3. Commit GR configuration on Rack-2:
   - Commit the configuration and let the pods be deployed on Rack-2.
   - Verify all pods are in running state.
   - Once both the racks are deployed, verify that the mirror maker pods on both racks are running and in ready state.

Examples

HA:

```
cdl node-type db-ims

cdl datastore session
 endpoint replica 2
 index map    1
 index write-factor 1
 slot replica 2
 slot map     4
 slot write-factor 1
exit

k8 label cdl-layer key smi.cisco.com/node-type value smf-ims-session
```

Rack-1:

```
cdl system-id          1
cdl node-type          session
cdl enable-geo-replication true
cdl zookeeper replica 1

cdl remote-site 2
 db-endpoint host 209.165.201.21 >> Rack-2 external CDL IP
 db-endpoint port 8882
 kafka-server 209.165.201.21 10092 >> Rack-2 external CDL IP
 exit
exit

cdl label-config session
 endpoint key smi.cisco.com/node-type1
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type1
  value smf-cdl
 exit
 index map 1
  key   smi.cisco.com/node-type1
  value smf-cdl
 exit
exit
cdl logging default-log-level debug

cdl datastore session
 label-config    session
 geo-remote-site [ 2 ]
 slice-names     [ 1 2 ]
 endpoint cpu-request 100
 endpoint replica 2
 endpoint external-ip 209.165.201.25 >> Rack-1 external CDL IP
 endpoint external-port 8882
 index cpu-request 100
 index replica 2
 index map   1
 slot cpu-request 100
 slot replica 2
 slot map    1
exit

cdl kafka replica 1
cdl kafka label-config key smi.cisco.com/node-type1
cdl kafka label-config value smf-cdl
cdl kafka external-ip 209.165.201.25 10092 >> Rack-1 external CDL IP
```

Rack-2:

```
cdl system-id          2
cdl node-type          session
cdl enable-geo-replication true
cdl zookeeper replica 1

cdl remote-site 1
 db-endpoint host 209.165.201.25 >> Rack-1 external CDL IP
 db-endpoint port 8882
 kafka-server 209.165.201.25 10092 >> Rack-1 external CDL IP
 exit
exit

cdl label-config session
 endpoint key smi.cisco.com/node-type12
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type12
  value smf-cdl
 exit
 index map 1
  key   smi.cisco.com/node-type12
  value smf-cdl
 exit
exit

cdl datastore session
 label-config    session
 geo-remote-site [ 1 ]
 slice-names     [ 1 2 ]
 endpoint cpu-request 100
 endpoint replica 2
 endpoint external-ip 209.165.201.21 >> Rack-2 external CDL IP
 endpoint external-port 8882
 index cpu-request 100
 index replica 2
 index map   1
 slot cpu-request 100
 slot replica 2
 slot map    1
exit

cdl kafka replica 1
cdl kafka label-config key smi.cisco.com/node-type12
cdl kafka label-config value smf-cdl
cdl kafka external-ip 209.165.201.21 10092 >> Rack-2 external CDL IP
```

Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept control and data messages of the targeted mobile users. To invoke this support, the LEA requests the network operator to start the interception of a particular mobile user. Legal approvals support this request.

1. Lawful Intercept (LI) tap should be configured/enabled on all the racks. If LI configuration fails on one rack, LEA should re-configure it so that for a given subscriber tap is enabled on all the racks.

Note LI tap configuration is not synchronized across racks.

Hence, LI tap configuration is mandatory on all the racks.

For more information on LI tap configuration, contact your Cisco Technical Representative.

2. GR instance awareness is applicable for lawful-intercept src-address only.

   Example:

   ```
   lawful-intercept instance 1 src-addr 209.165.200.225
   ```

   OR

   ```
   lawful-intercept
     instance 1
       src-addr 209.165.200.225
   ```

3. `show` commands are not instance-aware. It shows all the taps configured in a given cluster.

   For more information on LI `show` commands, contact your Cisco Technical Representative.

4. In case all GR instances are in Standby state in a cluster and active LI tap fails with CLI message `Rack is in standby mode, Active Tap is not allowed. Try camp on`, configure camp-on tap for the same subscriber.

RADIUS Configuration

NAS-IP and NAS-Identifier is instance-aware. You can configure different NAS-IP and NAS-Identifier per instance-id in profile-radius configuration. Existing non-instance based NAS-IP and NAS-Identifier configuration is used as default nas-ip and default nas-id for local instance of the rack.

Example

Following are a few configuration examples.

```
profile radius
 attribute
  instance 1
   nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for common AUTH & ACCT
   nas-identifier  smf1    --> Instance-1 specific NAS-Identifier, used for common AUTH &
ACCT
  exit
  instance 2
   nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for common AUTH & ACCT
   nas-identifier  smf2    --> Instance-2 specific NAS-Identifier, used for common AUTH &
ACCT
  exit
 exit
 accounting
  attribute
   instance 1
    nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for common ACCT
    nas-identifier  smf1    --> Instance-1 specific NAS-Identifier , used for common ACCT
   exit
   instance 2
    nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for common ACCT
    nas-identifier  smf2    --> Instance-2 specific NAS-Identifier , used for common ACCT
```

```
  exit
 exit
exit
server-group g1
 attribute
  instance 1
   nas-ip 209.165.200.225  --> Instance-1 specific NAS-IP, used for server-group <g1> AUTH
& ACCT
   nas-identifier  smf1    --> Instance-1 specific NAS-ID, used for server-group <g1> Auth
&Acct
  exit
  instance 2
   nas-ip 209.165.200.230  --> Instance-2 specific NAS-IP, used for server-group <g1> AUTH
& ACCT
   nas-identifier  smf2    --> Instance-2 specific NAS-ID,used for server-group <g1>AUTH&ACCT

  exit
 exit
 accounting
  attribute
   instance 1
    nas-ip 209.165.200.225 --> Instance-1 specific NAS-IP, used for server-group <g1> ACCT

    nas-identifier  smf1   --> Instance-1 specific NAS-ID, used for server-group <g1> ACCT

   exit
   instance 2
    nas-ip 209.165.200.230 --> Instance-2 specific NAS-IP, used for server-group <g1> ACCT

    nas-identifier  smf2   --> Instance-2 specific NAS-ID, used for server-group <g1> ACCT

   exit
  exit
 exit
exit
```

Since **endpoint** *pod* configuration is moved under specific instance, Radius Disconnect-Request VIP is also instance-aware.

```
instance instance-id 1
 endpoint radius
  replicas 1
  interface coa-nas
   vip-ip 209.165.202.130 vip-port 3799  --> Instance-1 specific Radius-Disconnect-Msg-VIP
 & PORT
  exit
 exit
exit
instance instance-id 2
 endpoint radius
  replicas 1
  interface coa-nas
   vip-ip 209.165.202.129 vip-port 3799  --> Instance-2 specific Radius-Disconnect-Msg-VIP
 & PORT
  exit
 exit
exit
```

Software Upgrade on GR Pairs

Considering `config commit` as reference. The same checklist is also applicable for other upgrade scenarios.

Checklist

Note Do not perform `cluster sync` on both racks (Rack-1 and Rack-2) at the same time. Trigger manual switchover on Rack-1 before proceeding with Rack-1 upgrade.

- Do not perform `config commits` on both racks at the same time. Perform `config commit` on each rack separately.
- Before to the `config commit` procedure on Rack-1, initiate the CLI-based switchover on Rack-1 and make sure that Rack-2 is having Primary ownership for both the instances (instance-id 1 and instance-id 2).
- Perform `config commit` on Rack-1. Wait for the successful `config commit`, PODs restart, and are back in running state to fetch the latest helm charts (if applicable).
- Revert the role of Rack-1 to be Primary (Switch/Reset roles on both racks).
- Verify that the available roles of Rack-1 (Primary) and Rack-2 (Standby) are on the expected status.
- Repeat the preceding checklist for Rack-2.

Software Upgrade

Upgrading the Rack-1, when the GR is Enabled:

1. Verify that the available roles of both instances on Rack-1 are in PRIMARY/STANDBY.

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

2. Initiate switch role for both instances on Rack-1 to STANDBY with failback-interval of 0 seconds. This step transitions the roles from PRIMARY/STANDBY to STANDBY_ERROR/STANDBY_ERROR.

```
geo switch-role instance-id 1 role standby [failback-interval 0]
geo switch-role instance-id 2 role standby [failback-interval 0]
```

Note
- Heartbeat between both the racks must be successful.
- The CLI **failback-interval** is an optional command to provide backward compatibility of upgrades between releases. The value of **failback-interval** is 0. It is deprecated from current release and will be discontinued from the subsequent releases.

3. Verify that the available roles of both instances have moved to STANDBY_ERROR on Rack-1.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

4. Verify that the available roles of both instances have moved to PRIMARY on Rack-2.

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "PRIMARY"
```

5. Perform rolling upgrade (or) non-graceful upgrade using system mode shutdown/running as per the requirement on Rack-1. To allow replication to finish, give a 5-minute gap between the GR switchover and SMF shutdown.
6. Perform the following steps post completion of the upgrade procedure. Perform health check on Rack-1 and ensure the PODs have come up and Rack-1 is healthy.
7. Verify that the available roles of both instances remain in STANDBY_ERROR mode on Rack-1.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

8. Initiate reset role for both instances on Rack-1 to STANDBY. This step transitions the roles from STANDBY_ERROR/STANDBY_ERROR to STANDBY/STANDBY.

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

9. Verify that the roles of both instances have moved to STANDBY on Rack-1.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

10. Initiate switch role for instance-id 1 on Rack-2 to STANDBY. This step transitions the available roles of Rack-2 from PRIMARY/PRIMARY to STANDBY_ERROR/PRIMARY and Rack-1 from STANDBY/STANDBY to PRIMARY/STANDBY.

```
geo switch-role instance-id 1 role standby [failback-interval 0]
```

11. Verify that the available roles of the instances on Rack-2 are in STANDBY_ERROR/PRIMARY.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "PRIMARY"
```

12. Verify that the available roles of both instances on Rack-1 are in PRIMARY/STANDBY.

```
show role instance-id 1
 result "PRIMARY"

show role instance-id 2
 result "STANDBY"
```

13. Initiate reset role for instance-id 1 on Rack-2 to STANDBY. This step transitions the roles of Rack-2 from STANDBY_ERROR/PRIMARY to STANDBY/PRIMARY.

```
geo reset-role instance-id 1 role standby
```

14. Verify that the available roles of both instances on Rack-2 are in STANDBY/PRIMARY.

```
show role instance-id 1
result "STANDBY"
```

```
show role instance-id 2
 result "PRIMARY"
```

Upgrading the Rack-2, when the GR is Enabled:

1. Verify that the available roles of both instances on Rack-2 are in STANDBY/PRIMARY.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

2. Initiate switch role for both instances on Rack-2 to STANDBY with failback-interval of 0 seconds. This step transitions the roles from STANDBY/PRIMARY to STANDBY_ERROR/STANDBY_ERROR.

```
geo switch-role instance-id 1 role standby [failback-interval 0]
geo switch-role instance-id 2 role standby [failback-interval 0]
```

3. Verify that the available roles of both instances move to STANDBY_ERROR on Rack-2.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

4. Verify that the available roles of both instances move to PRIMARY on Rack-1.

```
show role instance-id 1
 result "PRIMARY"

show role instance-id 2
 result "PRIMARY"
```

5. Perform rolling upgrade (or) non-graceful upgrade via system mode shutdown/running as per the requirement on Rack-2.

6. Perform the subsequent steps post completion of the upgrade procedure. Perform the health check on Rack-2 and ensure the PODs have come up and Rack-2 is healthy.

7. Verify that the available roles of both the instances remain in STANDBY_ERROR on Rack-2.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

8. Initiate reset role for both instances on Rack-2 to STANDBY. This step transitions the roles from STANDBY_ERROR/STANDBY_ERROR to STANDBY/STANDBY.

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

9. Verify that the available roles of both instances move to STANDBY on Rack-2.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

10. Initiate switch role for instance-id 2 on Rack-1 to STANDBY. This step transitions the available roles of Rack-1 from PRIMARY/PRIMARY to PRIMARY/STANDBY_ERROR and Rack-2 from STANDBY/STANDBY to STANDBY/PRIMARY.

```
geo switch-role instance-id 2 role standby [failback-interval 0]
```

11. Verify that the available roles of both instances on Rack-1 are in PRIMARY/STANDBY_ERROR.

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY_ERROR"
```

12. Verify that the available roles of both instances on Rack-2 are in STANDBY/PRIMARY.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

13. Initiate reset role for instance-id 2 on Rack-1 to STANDBY. This step transitions the roles of Rack-1 from PRIMARY/STANDBY_ERROR to PRIMARY/STANDBY.

```
geo reset-role instance-id 2 role standby
```

14. Verify that the available roles of both the instances on Rack-1 are in PRIMARY/STANDBY.

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

GR CLI

The following section provides information on GR CLI based commands.

Geo Replication Pull Data

The following sample setup configures the Geo Replication Pull Data. These commands help and perform the replication data sync activities, during the event of any malfunction scenario. To transition to the GR role and minimize any replication data mismatch on the system, you can initiate the following commands to synchronize the data across all accessible racks:

geo replication-pull instance-id *gr_instanceId*

NOTES:

- **geo replication-pull**—It pulls the replication data from the peer rack and syncs it with the local rack.
- **instance-id** *gr_instanceId*—Specify the GR Instance ID.

Geo Reset Role

To reset the GR instance role (for example, roles from **STANDBY_ERROR** to **STANDBY** to **PRIMARY**), use the following sample commands:

geo reset-role role *role* **instance-id** *gr_instanceId*

NOTES:

- **role** *role*—Specify the new role for the given rack.

  The role can be **PRIMARY** or **STANDBY**.

- **instance-id** *gr_instanceId*—Specify the GR Instance ID.

Important `The command` **`geo reset-role`** triggers change in the role for the given instance on the local rack. The remote rack does not receive any message for the same command. It is only possible to change the role for the given instance ID from **`STANDBY_ERROR`** to **`STANDBY`** and **`STANDBY`** to **`PRIMARY`**. Another role change is not possible.

Geo Switch Role

To switch the GR role, initiate the command on the primary rack (for example, role **`PRIMARY`** to **`STANDBY`** only), and use the following command.

`geo switch-role { role` *`primary | standby`* **`instance-id`** *`gr_instanceId`* **`[ failback-interval`** *`failback_interval`* **`] }`**

NOTES:

- **role** *role*—Specify the new role for the given rack.

  The roles can be *primary* or *standby*. It's mandatory to trigger manual switchover from primary role for a specific GR instance ID.

- **instance-id** *gr_instanceId*—Specify the GR Instance ID
- **failback-interval** is an optional command to provide backward compatibility of upgrades between releases. The recommended value of **failback-interval** is 0.

Important **`geo switch-role`** command triggers manual failover from one rack to another rack for specific instance ID. The rack which triggers the failover changes from the **`PRIMARY`** role to the **`STANDBY_ERROR`** role. In between, the rack which triggers the failover, sends a failover (Trigger GR) message to another rack. The other rack which receives the failover message changes from the **`STANDBY`** role to the **`PRIMARY`** role.

Note **failback-interval** is deprecated from current release and will be discontinued from the subsequent releases.

Troubleshooting

This section describes about various applicable troubleshooting scenarios.

show/clear Commands

This section describes show/clear commands that help in debugging issues.

clear subscriber

To clear gr-instance aware subscriber, use the following command:

`clear subscriber all gr-instance` *`gr_instanceId`*

Note **gr-instance** is optional parameter. If **gr-instance** is not specified, `show subscriber all` considers the local instance-id of that rack.

Example

The following is a configuration example.

```
clear subscriber all gr-instance 1
result
ClearSubscriber Request submitted
```

show BFD Status

To view the BFD status of neighbors, use the following command:

show bfd-neighbor

Example

The following is a list of few configuration examples:

```
show bfd-neighbor
status-details

-----example-bgp-ep-1 ----

Peer             Status

 209.165.202.142  STATE_DOWN
-----example-bgp-ep-2 ----

Peer             Status

 209.165.202.142  STATE_DOWN

show bfd-neigbor
status-details

-----bgpspeaker-pod-1 ----

Peer             Status

 209.165.202.131
-----bgpspeaker-pod-2 ----

Peer             Status

 209.165.202.131   STATE_UP
```

show BGP Global

To view BGP global configuration, use the following command:

show bgp-global

Example

The following is a list of few configuration examples:

```
show bgp-global
global-details
-----example-bgp-ep-2 ----
AS:        65000
Router-ID: 209.165.202.149
Listening Port: 179, Addresses: 209.165.202.149
-----example-bgp-ep-1 ----
AS:        65000
Router-ID: 209.165.202.148
Listening Port: 179, Addresses: 209.165.202.148
```

```
show bgp-global
global-details

-----bgpspeaker-pod-2 ----
AS:        65061
Router-ID: 209.165.202.132
Listening Port: 179, Addresses: 209.165.202.132
```

show bgp kernel route

To view BGP kernel configured routes, use the following command:

show bgp-kernel-route kernel-route

Example

The following is a list of few configuration examples:

```
show bgp-kernel-route
kernel-route

-----example-bgp-ep-2 ----

 DestinationIP  SourceIP        Gateway

-----example-bgp-ep-1 ----

 DestinationIP      SourceIP          Gateway
 209.165.202.133    209.165.202.148   209.165.202.142
 209.165.202.134    209.165.202.148   209.165.202.142
```

```
show bgp-kernel-route
kernel-route

-----bgpspeaker-pod-2 ----

 DestinationIP        SourceIP            Gateway

 209.165.202.135    209.165.202.132    209.165.202.131

-----bgpspeaker-pod-1 ----

 DestinationIP  SourceIP        Gateway
```

show bgp neighbors

To view BGP neighbors status, use the following command

show bgp-neighbors neighbor-details
show bgp-neighbors ip *ip_address* **neighbor-details**

Example

The following is a list of few configuration examples:

```
show bgp-neighbors neighbor-details
-----example-bgp-ep-1 ----
Peer             AS  Up/Down State       |#Received  Accepted
209.165.202.142 60000 00:25:06 Establ      |        3         3
-----example-bgp-ep-2 ----
Peer             AS Up/Down State       |#Received  Accepted
209.165.202.142 60000   never Idle        |        0         0

show bgp-neighbors ip 209.165.202.142 neighbor-details
-----example-bgp-ep-2 ----
BGP neighbor is 209.165.202.142, remote AS 60000
  BGP version 4, remote router ID unknown
  BGP state = ACTIVE
  BGP OutQ = 0, Flops = 0
  Hold time is 0, keepalive interval is 0 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised
    route-refresh:      advertised
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised
  Message statistics:
                        Sent       Rcvd
    Opens:               130          0
    Notifications:         0          0
    Updates:               0          0
    Keepalives:            0          0
    Route Refresh:         0          0
    Discarded:             0          0
    Total:               130          0
  Route statistics:
    Advertised:            0
    Received:              0
    Accepted:              0

-----example-bgp-ep-1 ----
BGP neighbor is 209.165.202.142, remote AS 60000
  BGP version 4, remote router ID 209.165.202.136
  BGP state = ESTABLISHED, up for 00:25:20
  BGP OutQ = 0, Flops = 0
  Hold time is 90, keepalive interval is 30 seconds
  Configured hold time is 90, keepalive interval is 30 seconds

  Neighbor capabilities:
    multiprotocol:
        ipv4-unicast:   advertised and received
    route-refresh:      advertised and received
    extended-nexthop:   advertised
        Local:  nlri: ipv4-unicast, nexthop: ipv6
    4-octet-as: advertised and received
  Message statistics:
                        Sent       Rcvd
    Opens:                 1          1
    Notifications:         0          0
    Updates:               1          1
    Keepalives:           51         51
    Route Refresh:         0          0
    Discarded:             0          0
```

```
    Total:                 53         53
  Route statistics:
    Advertised:             0
    Received:               3
    Accepted:               3
```

show bgp route summary

To view BGP route summary, use the following command:

show bgp-route-summary

Example

The following is a configuration example.

```
show bgp-route-summary
route-details
-----example-bgp-ep-1 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 5, Path: 5
-----example-bgp-ep-2 ----
Table afi:AFI_IP safi:SAFI_UNICAST
Destination: 2, Path: 2
```

show BGP Routes

To view BGP routes information, use the following command:

show bgp-routes

Example

The following is a configuration example:

```
show bgp-routes
bgp-route

-----example-bgp-ep-1 ----
   Network              Next Hop             AS_PATH      Age        Attrs
*> 209.165.202.133/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med: 0}]
*> 209.165.200.225/32   209.165.202.148                   00:26:00   [{Origin: e} {LocalPref:
 100} {Med: 600}]
*> 209.165.202.134/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med: 0}]
*> 209.165.202.140/24   209.165.202.142        60000      00:25:55   [{Origin: i} {Med: 0}]
*> 209.165.202.146/32   209.165.202.148                   00:26:00   [{Origin: e} {LocalPref:
 100} {Med: 600}]

-----example-bgp-ep-2 ----
   Network              Next Hop             AS_PATH      Age        Attrs
*> 209.165.200.225/32   209.165.202.149                   00:26:24   [{Origin: e} {LocalPref:
 100} {Med: 600}]
*> 209.165.202.146/32   209.165.202.149                   00:26:24   [{Origin: e} {LocalPref:
 100} {Med: 600}]
```

show endpoint

To view endpoints that are now gr-instance aware, use the following command:

show endpoint all grInstance *gr_instanceId*

Note **grInstance** is optional parameter. If **grInstance** is not specified, `show subscriber all` considers the local instance-id of that rack.

Example

The following is a configuration example:

```
show endpoint all grInstance 1
                                                                                                START
STOPPED  GR
ENDPOINT                          ADDRESS        TYPE  STATUS   INTERFACE  INTERNAL  TIME
     TIME     INSTANCE
-------------------------------------------------------------------------------------------------------
209.165.202.137:2123       209.165.202.137:2123  Udp   Started             false     10
hours  <none>   1
Gtpu:209.165.202.137:2152  209.165.202.137:2152  Udp   Started  GTPU       false     10
hours  <none>   1
N4:209.165.202.137:8806    209.165.202.137:8806  Udp   Started  N4         false     10
hours  <none>   1
S2B-GTP                    209.165.202.138:2124  Udp   Started  s2b        false     10
hours  <none>   1
S5-GTP                     209.165.202.138:2125  Udp   Started  s5         false     10
hours  <none>   1
S5S8S2B-GTP                209.165.202.138:2123  Udp   Started  s5s8s2b    false     10
hours  <none>   1
Sxa:209.165.202.137:8805   209.165.202.137:8805  Udp   Started  SXA        false     10
hours  <none>   1
n10-1                      209.165.202.139:9010  Rest  Started  N10-1      false     10
hours  <none>   1
n11-1                      209.165.202.139:9011  Rest  Started  N11-1      false     10
hours  <none>   1
n40-1                      209.165.202.139:9040  Rest  Started  N40-1      false     10
hours  <none>   1
n7-1                       209.165.202.139:9007  Rest  Started  N7-1       false     10
hours  <none>   1
sbi-1                      209.165.202.139:8090  Rest  Started  SBI-1      false     10
hours  <none>   1
```

show ETCD/Cache Pod Replication

To view replication details for etcd and cache-pod data, use the following command:

show georeplication checksum instance-id *gr_instanceId*

Example

The following is a configuration example:

```
show georeplication checksum instance-id
Value for 'instance-id' (<string>): 1
checksum-details
--              ----    --------
 ID             Type    Checksum
 --             ----    --------
 1              ETCD    1617984439
 IPAM           CACHE   1617984439
 NRFCache       CACHE   1617984439
 NRFSubs        CACHE   1617984439
```

```
IDMGR           CACHE   1617984439
NRFMgmt         CACHE   1617984439
```

show role

To view the current role of the GR instance, use the following command:

show role instance-id *gr_instanceId*

Note The following is a list of possible values for the role:

- **PRIMARY**
- **STANDBY**
- **INIT**
- **FAILOVER_INIT**
- **STANDBY_ERROR**

Example

The following is a list of few configuration examples:

```
show role instance-id 1
result
"PRIMARY"
```

```
show role instance-id 2
result
"STANDBY"
```

show ipam dp with type and address

To view the instance ID and flag to indicate chunk for remote instance, use the following command:

show ipam dp { ***dp_type* **} { ***addr_type* **}

NOTES:

- **dp** *dp_type*—Specify DP type.
- *addr_type*—Specify IPv4/IPv6 address type.

Example

The following is a configuration example.

```
show ipam dp 209.165.202.145:209.165.202.144  ipv4-addr
================================================================
Flag Indication: S(Static) O(Offline) R(For Remote Instance)
G:N/P Indication: G(GR InstId) N(Native NM InstId) P(Peer NM InstId)
================================================================
StartAddress    EndAddress      AllocContext                    Route              G:N/P
Utilization Flag
================================================================
209.165.200.240 209.165.200.243 209.165.202.145:209.165.202.144 209.165.200.240/24 1:0/1
```

```
0.00%        R
=====================================================================
```

show ipam dp

To view all the instances this DP has chunks from, use the following command:

show ipam dp *dp_name*

NOTES:

- **dp** *dp_name*—Specify data plane allocation name.

Example

The following is a configuration example.

```
show ipam dp 209.165.202.145:209.165.202.144
-------------------------------------------------------
Ipv4Addr [Total/Used/Utilization] = 257 / 1 / 0.39%
Ipv6Addr [Total/Used/Utilization] = 0 / 0 / 0.00%
Ipv6Prefix [Total/Used/Utilization] = 2048 / 0 / 0.00%
Instance ID = 1
-------------------------------------------------------
```

show ipam pool

To view instance ID information under which pool is configured, use the following command:

show ipam pool *pool_name*

NOTES:

- **pool** *pool_name*—Specify pool name.

Example

The following is a list of few configuration examples.

```
show ipam pool

=============================================================================================
PoolName                      Ipv4Utilization  Ipv6AddrUtilization  Ipv6PrefixUtilization
=============================================================================================
poolv6DNN2                    0.00%            0.00%                0.00%
poolv6                        0.00%            0.00%                0.00%
poolv4vDNN                    0.00%            0.00%                0.00%
poolv4DNN2                    0.00%            0.00%                0.00%
poolv4                        0.00%            0.00%                0.00%
poolv6vDNN                    0.00%            0.00%                0.00%
poolv4DNN3                    -                -                    -
=============================================================================================

show ipam pool poolv4DNN3
-------------------------------------------------------
Ipv4Addr [Total/Used/Utilization] = 2814 / 0 / -
Ipv6Addr [Total/Used/Utilization] = 0 / 0 / -
Ipv6Prefix [Total/Used/Utilization] = 65536 / 0 / -
Instance ID = 1
isStatic = true
-------------------------------------------------------
```

```
show ipam pool poolv4
-------------------------------------------------------
 Ipv4Addr   [Total/Used/Utilization] = 2814 / 0 / 0.00%
 Ipv6Addr   [Total/Used/Utilization] = 0 / 0 / 0.00%
 Ipv6Prefix [Total/Used/Utilization] = 0 / 0 / 0.00%
 Instance ID                         = 1
-------------------------------------------------------
```

show nrf discovery-info discovery-filter

To view GR Instance ID information to determine for which GR instance the discovery filter information belongs, use the following command:

show nrf discovery-info *nf_type* **discovery-filter**

Example

The following is a configuration example.

```
=====================================================
-----------------------------------------------------
Discovery Filter: dnn=intershat;
Expiry Time: 1580146356
GR Instance ID: 1
-----------------------------------------------------
=====================================================================
```

show nrf discovery-info

To view GR Instance ID information to determine for which GR instance the discovery information belongs, use the following command:

show nrf discovery-info

Example

The following is a configuration example.

```
show nrf discovery-info
=====================================================
------Discovered NFs:-------
    NF Type: AMF
    Number of Discovery Filters: 15
    Number of NF Profiles: 15
    GR Instance ID: 1
------Discovered NFs:-------
    NF Type: UDM
    Number of Discovery Filters: 1
    Number of NF Profiles: 3
    GR Instance ID: 2
=====================================================
```

show nrf registration-info

To view GR Instance ID information to determine which GR instance the registration information belongs to, use the following command:

show nrf registration-info

Example

The following is a configuration example.

```
show nrf registration-info
=============================================================================
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 GR Instance ID: 1
========

show nrf registration-info

=============================================================================
 Gr-instance:
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 Uri:
 Host Type:

=============================================================================
 Gr-instance:
 NF Status: Not Registered
 Registration Time:
 Active MgmtEP Name:
 Heartbeat Duration: 0
 Uri:
 Host Type:

=============================================================================
```

show nrf subscription-info

To view GR Instance ID information to determine for which GR instance the subscription information belongs, use the following command:

show nrf subscription-info

Example

The following is a configuration example.

```
show nrf subscription-info
=====================================================================
NF Instance Id: f9882966-a253-32d1-8b82-c785b34a7cc9
SubscriptionID : subs123459
Actual Validity Time : 2020-01-21 12:39:45 +0000 UTC
Requested Validity Time : 2020-01-21 12:39:45 +0000 UTC
GR Instance ID: 1
=====================================================================
```

show peers

To view peers that are now gr-instance aware, use the following command:

show peers all grInstance *gr_instanceId*

Note **grInstance** is optional parameter. If **grInstance** is not specified, `show subscriber all` considers the local instance-id of that rack.

Example

The following is a configuration example.

```
show peers all grInstance 1
                                                                    POD              CONNECTED
ADDITIONAL  INTERFACE  GR
ENDPOINT  LOCAL ADDRESS   PEER ADDRESS     DIRECTION  INSTANCE TYPE TIME     RPC DETAILS
NAME       INSTANCE
-------------------------------------------------------------------------------------------------------
<none>  209.165.202.139 209.165.201.22:8001 Outbound rest-ep-0 Rest 10 hours UDM <none>
n10        1
<none>  209.165.202.139 209.165.201.22:8002 Outbound rest-ep-0 Rest 10 hours AMF <none>
n11        1
<none>  209.165.202.139 209.165.201.22:8003 Outbound rest-ep-0 Rest 10 hours PCF <none>
n7         1
<none>  209.165.202.139 209.165.201.22:8004 Outbound rest-ep-0 Rest 10 hours CHF <none>
n40        1
<none>  209.165.202.139 209.165.201.22:9040 Outbound rest-ep-0 Rest 10 hours CHF <none>
n40
```

show subscriber

To view subscriber details that are made gr-instance aware, use the following command:

show subscriber { all | gr-instance *gr_instanceId* **}**

Note `show subscriber all` displays only the local instance subscriber details.

gr-instance is optional parameter. If **gr-instance** is not specified, `show subscriber all` considers the local instance-id of that rack.

Example

The following is a configuration example.

```
show subscriber gr-instance 1 all
subscriber-details
{
"subResponses": [
[
""
],
[
""
],
[
"roaming-status:homer",
"supi:imsi-123456789300001",
"gpsi:msisdn-22331010301010",
"psid:1",
"dnn:intershat",
"emergency:false",
```

```
"rat:nr",
"access:3gpp access",
"connectivity:5g",
"udm-uecm:209.165.202.150",
"udm-sdm:209.165.202.150",
"auth-status:unauthenticated",
"pcfGroupId:PCF-*",
"policy:2",
"pcf:209.165.202.152",
"upf:209.165.202.154",
"upfEpKey:209.165.202.154:209.165.202.158",
"ipv4-addr:v4pool1/209.165.200.250",
"ipv4-pool:v4pool1",
"ipv4-range:v4pool1/209.165.200.249",
"ipv4-startrange:v4pool1/209.165.200.250",
"id-index:1:0:0:32768",
"id-value:8",
"chfGroupId:CHF-*",
"chf:209.165.202.151",
"amf:209.165.202.153",
"peerGtpuEpKey:209.165.202.154:209.165.202.155",
"namespace:smf",
"nf-service:smf"
]
]
}
```

Monitor Subscriber

To capture messages for subscriber (gr-instance aware), use the following command:

monitor subscriber [capture-duration *duration* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [yes] | namespace [sgw | smf] | nf-service [sgw | smf] | supi** *supi_id* **| transaction-logs [yes]]**

Note In 2021.02 and later releases, the **namespace** keyword is deprecated and replaced with the **nf-service** keyword.

NOTES:

- **capture-duration** *duration*: Specify the duration in seconds during which monitor subscriber is enabled. The default value is 300 seconds (5 minutes). This is an optional parameter.
- **gr-instance** *gr_instance_id*: Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **imei** *imei_id*: Specify the subscriber IMEI. For example: 123456789012345, *
- **imsi** *imsi_value*: Specify the subscriber IMSI. For example: 123456789, *
- **internal-messages [yes]**: Enable internal messages when set to **yes**. By default, it is disabled. This is an optional parameter.
- **namespace [sgw | smf]**: Enable the specified namespace. By default, namespace is set to none. This is an optional parameter.

Important This keyword is deprecated in release 2021.02.0 and replaced with **nf-service** keyword.

- **nf-service [sgw | smf]** : Enable the specified NF service. By default, nf-service is set to none. This is a mandatory parameter.

Important The **nf-service** keyword replaces the **namespace** keyword in release 2021.02 and beyond.

- **supi** *supi_id*: Specify the subscriber identifier. For example: imsi-123456789, imsi-123*
- **transaction-logs [yes]**: Enable transaction logs when set to **yes**. By default, it is disabled. This is an optional parameter.

  To view the transaction history logs, use the **dump transactionhistory** command.

Note The most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

Example

The following is a configuration example.

```
monitor subscriber imsi 123456789 gr-instance 1
supi: imsi-123456789
captureDuration: 300
enableInternalMsg: false
enableTxnLog: false
namespace(deprecated. Use nf-service instead.): none
nf-service: none
gr-instance: 1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   295  100    98  100   197  10888  21888 --:--:-- --:--:-- --:--:-- 29500
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_sub","parameters":{"supi":"imsi-123456789","duration":300,
"enableTxnLog":false,"enableInternalMsg":false,"action":"start","namespace":"none",
"nf-service":"none","grInstance":1}} http://oam-pod:8879/commands
Result start mon_sub, fileName
->logs/monsublogs/none.imsi-123456789_TS_2021-04-09T09:59:59.964148895.txt
Starting to tail the monsub messages from file:
logs/monsublogs/none.imsi-123456789_TS_2021-04-09T09:59:59.964148895.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n smf' to see all the containers in this pod.
```

Monitor Protocol

To capture packets on different interfaces (gr-instance aware), use the following command:

monitor protocol { interface *interface_name* **[capture-duration** *duration* **| gr-instance***gr_instance* **| pcacp yes | |] | list [|] }**

NOTES:

- **interface** *interface_name*—Specify the interface name on which PCAP is captured. This CLI allows the configuration of multiple interface names in a single CLI command.
- **capture-duration** *duration*—Specify the duration in seconds during which pcap is captured. The default is 300 seconds (5 minutes).
- The configured interface names can be retrieved using the **show endpoint** CLI command.
- **gr-instance** *gr_instance_id*—Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **pcap yes**—Configure this option to enable PCAP file generation. By default, this option is disabled.
- **list**—Monitor protocol list files.

Example

The following is a configuration example.

```
monitor protocol interface sbi gr-instance 1
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   220  100    95  100   125   8636  11363 --:--:-- --:--:-- --:--:-- 20000
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_pro","parameters":{"interface":"sbi","duration":300,"action":
"start","enable_pcap":false,"grInstance":1}} http://oam-pod:8879/commands
Result start mon_pro, fileName
->logs/monprologs/sessintfname_sbi_at_2021-04-30T05:26:22.712229347.txt
Starting to tail the monpro messages from file:
logs/monprologs/sessintfname_sbi_at_2021-04-30T05:26:22.712229347.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n cn' to see all of the containers in this pod.
```

Geographic Redundancy OAM Support

This section describes operations, administration, and maintenance information for this feature.

Health Check

The following section provides information on GR setup health check.

- All critical pods are in good condition to serve user traffic.

  Use the following command to check whether GR and CDL related pods are in Running state.

  ```
  kubectl get pods -n cn-cn1 -o wide | grep georeplication-pod
  kubectl get pods -n cn-cn1 -o wide | grep cdl
  kubectl get pods -n cn-cn1 -o wide | grep mirror-maker
  ```

- Keepalived pods are in healthy state to monitor all VIPs which are configured for check-interface/check-port.

  Use the following command to check whether keepalived pods in “smi-vips” namespace are in “Running” state.

  ```
  kubectl get pods -n smi-vips
  ```

- Health-check of pods related to CDL: Check the status of CDL db-endpoint, slot and indexes. All should be in STARTED or ONLINE state for both System IDs 1 and 2.

```
cdl show status
message params: {cmd:status mode:cli dbName:session sessionIn:{mapId:0 limit:500 key:
purgeOnEval:0 filters:[] nextEvalTsStart:0 nextEvalTsEnd:0 allReplicas:false
maxDataSize:4096} sliceName:}
db-endpoint {
    endpoint-site {
        system-id 1
        state STARTED
        total-sessions 4
        site-session-count 2
        total-reconciliation 0
        remote-connection-time 66h37m31.36054781s
        remote-connection-last-failure-time 2021-07-13 11:24:10.233825924 +0000 UTC
        slot-geo-replication-delay 2.025396ms
    }
    endpoint-site {
        system-id 2
        state STARTED
        total-sessions 4
        site-session-count 2
        total-reconciliation 0
        remote-connection-time 66h58m49.83449066s
        remote-connection-last-failure-time 2021-07-13 11:02:51.759971655 +0000 UTC
        slot-geo-replication-delay 1.561816ms
    }
}
slot {
    map {
        map-id 1
        instance {
            system-id 1
            instance-id 1
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h38m37.335813523s
            sync-duration 9.298061ms
        }
        instance {
            system-id 1
            instance-id 2
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h39m11.1268024s
            sync-duration 8.852556ms
        }
        instance {
            system-id 2
            instance-id 1
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h28m38.274713022s
            sync-duration 8.37766ms
        }
        instance {
            system-id 2
```

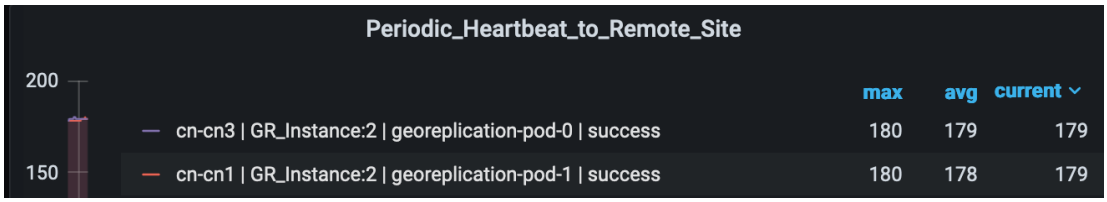
```
            instance-id 2
            records 4
            capacity 2500000
            state ONLINE
            avg-record-size-bytes 1
            up-time 89h29m37.934345015s
            sync-duration 8.877442ms
        }
    }
}
index {
    map {
        map-id 1
        instance {
            system-id 1
            instance-id 1
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h38m16.119032086s
            sync-duration 2.012281769s
            leader false
            geo-replication-delay 10.529821ms
        }
        instance {
            system-id 1
            instance-id 2
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h39m8.47664588s
            sync-duration 2.011171261s
            leader true
            leader-time 89h38m53.761213379s
            geo-replication-delay 10.252683ms
        }
        instance {
            system-id 2
            instance-id 1
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h28m29.5479133s
            sync-duration 2.012101957s
            leader false
            geo-replication-delay 15.974538ms
        }
        instance {
            system-id 2
            instance-id 2
            records 4
            capacity 60000000
            state ONLINE
            up-time 89h29m11.633496562s
            sync-duration 2.011566639s
            leader true
            leader-time 89h28m51.29928233s
            geo-replication-delay 16.213323ms
        }
    }
}
```

- CDL replication status

Check whether four gRPC connections are established between the CDL EP session pods (of each namespace) across the racks in **GRPC_Connections_to_RemoteSite** panel of **CDL Replication Stats** Grafana dashboard. Check Grafana on both racks.

- Admin port status between the racks for geo-replication.

  Check heartbeat messages between geo-replication pods across the racks in **Periodic_Heartbeat_to_Remote_Site** panel of **GR Statistics** Grafana dashboard.



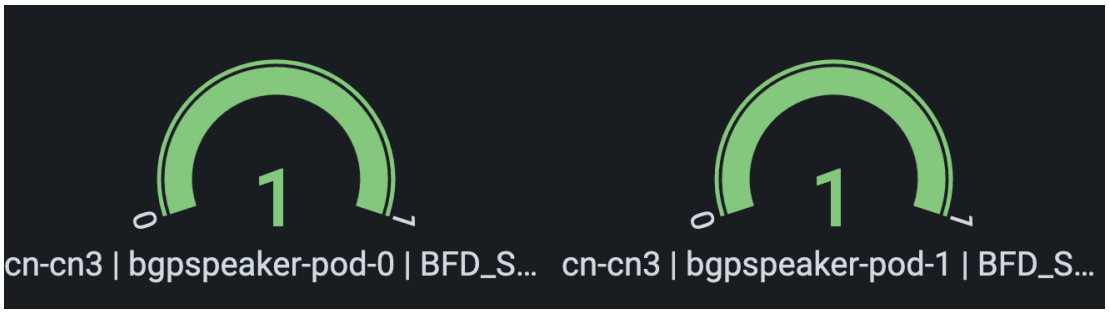
- BGP/BFD link status on rack

  Check whether neighborship with BGP peers is established in **BGP Peers** panel of **BGP, BFD Statistics** Grafan dashboard.

BGP Peers

Time	as_path	namespace	peer_ip	pod	Value
2021-07-16 06:29:18	3333	cn-cn1	192.204.10.6	bgpspeaker-pod-0	1
2021-07-16 06:29:18	3333	cn-cn1	192.204.10.6	bgpspeaker-pod-1	1
2021-07-16 06:29:18	3333	cn-cn3	192.204.18.6	bgpspeaker-pod-0	1
2021-07-16 06:29:18	3333	cn-cn3	192.204.18.6	bgpspeaker-pod-1	1

Check whether BFD link is in connected state in **BFD Link Status** panel of **BGP, BFD Statistics** Grafana dashboard.



- Roles of each instances are in healthy state

  Check that in each rack the roles are not in STANDBY_ERROR state at any point of time.

  - **Active/Standby Model**: Roles should be in the following states on each rack

    Rack-1:

    ```
    show role instance-id 1
    result "PRIMARY"
    show role instance-id 2
    result "PRIMARY"
    ```

    Rack-2:

    ```
    show role instance-id 1
    result "STANDBY"
    show role instance-id 2
    result "STANDBY"
    ```

  - **Active/Active Model**: Roles should be in the following states on each rack.

    Rack-1:

    ```
    show role instance-id 1
    result "PRIMARY"
    show role instance-id 2
    result "STANDBY"
    ```

    Rack-2:

    ```
    show role instance-id 1
    result "STANDBY"
    show role instance-id 2
    result "PRIMARY"
    ```

Recovery Procedure

On Rack-1

1. Verify that roles of both instances on Rack-1 are in STANDBY_ERROR.

   ```
   show role instance-id 1
   result "STANDBY_ERROR"

   show role instance-id 2
   result "STANDBY_ERROR"
   ```

2. Initiate reset role for both instances on Rack-1 to STANDBY. This step transitions the roles from STANDBY_ERROR/STANDBY_ERROR to STANDBY/STANDBY.

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

3. Verify that roles of both instances have moved to STANDBY on Rack-1.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "STANDBY"
```

4. Initiate switch role for instance-id 1 on Rack-2 to STANDBY with failback-interval of 30 seconds. This step transitions the roles of Rack-2 from PRIMARY/PRIMARY to STANDBY_ERROR/PRIMARY and Rack-1 from STANDBY/STANDBY to PRIMARY/STANDBY.

```
geo switch-role instance-id 1 role standby [failback-interval 0]
```

5. Verify that roles of both instances on Rack-2 are in STANDBY_ERROR/PRIMARY.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "PRIMARY"
```

6. Verify that roles of both instances on Rack-1 are in PRIMARY/STANDBY.

```
show role instance-id 1
result "PRIMARY"

show role instance-id 2
result "STANDBY"
```

7. Initiate reset role for instance-id 1 on Rack-2 to STANDBY. This step transitions the roles of Rack-2 from STANDBY_ERROR/PRIMARY to STANDBY/PRIMARY.

```
geo reset-role instance-id 1 role standby
```

8. Verify that the roles of Rack-2 are in STANDBY/PRIMARY.

```
show role instance-id 1
result "STANDBY"

show role instance-id 2
result "PRIMARY"
```

On Rack-2

1. Verify that roles of both the instances on Rack-2 are in STANDBY_ERROR.

```
show role instance-id 1
result "STANDBY_ERROR"

show role instance-id 2
result "STANDBY_ERROR"
```

2. Initiate reset role for both instances on Rack-2 to STANDBY. This step transitions the roles from STANDBY_ERROR/STANDBY_ERROR to STANDBY/STANDBY.

```
geo reset-role instance-id 1 role standby
geo reset-role instance-id 2 role standby
```

3. Verify that the roles of both the instances move to STANDBY on Rack-2.

```
show role instance-id 1
result "STANDBY"
```

```
show role instance-id 2
result "STANDBY"
```

4. Initiate switch role for instance-id 2 on Rack-1 to STANDBY. This step transitions roles of Rack-1 from PRIMARY/PRIMARY to PRIMARY/STANDBY_ERROR and Rack-2 from STANDBY/STANDBY to STANDBY/PRIMARY.

   ```
   geo switch-role instance-id 2 role standby [failback-interval 0]
   ```

5. Verify that roles of instances on Rack-1 are in PRIMARY/STANDBY_ERROR mode.

   ```
   show role instance-id 1
   result "PRIMARY"

   show role instance-id 2
   result "STANDBY_ERROR"
   ```

6. Verify that roles of instances on Rack-2 are in STANDBY/PRIMARY mode.

   ```
   show role instance-id 1
   result "STANDBY"

   show role instance-id 2
   result "PRIMARY"
   ```

7. Initiate reset role for instance-id 2 on Rack-1 to STANDBY. This step transitions the roles of Rack-1 from PRIMARY/STANDBY_ERROR to PRIMARY/STANDBY.

   ```
   geo reset-role instance-id 2 role standby
   ```

8. Verify that roles of instances on Rack-1 are in PRIMARY/STANDBY.

   ```
   show role instance-id 1
   result "PRIMARY"

   show role instance-id 2
   result "STANDBY"
   ```

Key Performance Indicators (KPIs)

The following section describes KPIs.

ETCD/Cachepod Replication KPIs

The following table lists ETCD/Cachepod Replication KPIs.

Table 399: geo_replication_total KPIs

KPI Name	Description	Labels	Possible Values
geo_replication _total	This KPI displays total number of replication requests/responses for various Sync types and Replication types.	ReplicationRequest Type	Request / Response
		ReplicationSync Type	Immediate / Deferred / Pull
		ReplicationNode	ETCD / CACHE_POD / PEER
		ReplicationReceiver	Local / Remote
		status	True / False
		status_code	Error code/description

Geo Rejected Role Change KPIs

The following table lists Geo Rejected Role Change KPIs.

Table 400: Geo Rejected Role Change KPIs

KPI Name	Description	Labels	Possible Values
geo_RejectedRole Changed_total	This KPI displays the total number of rejected requests/calls received for STANDBY instance. After the count, the same instance is moved to PRIMARY.	RejectedCount	Number value indicating rejected calls/requests received for standby instance.
		GRInstance Number	1 / 2

Monitoring KPIs

The following table lists monitoring KPIs.

Table 401: geo_monitoring_total KPIs

KPI Name	Description	Labels	Possible Values
geo_monitoring_total	This KPI displays the total number of successful / failure messages of different kinds such as, heartbeat / remoteNotify / TriggerGR and so on.	ControlAction Type	AdminMonitoring ActionType / AdminRemote MessageAction Type / AdminRole ChangeActionType
		ControlAction NameType	MonitorPod / MonitorBfd / RemoteMsgHeartbeat / RemoteMsgNotifyFailover / RemoteMsgNotify PrepareFailover / RemoteMsgGetSiteStatus / RemoteClusterPodFailure / RemoteSiteRole Monitoring / TriggerGRApi / ResetRoleApi
		Admin Node	Any string value. For example, GR Instance ID or instance key / pod name
		Status Code	0 / 1001 / 1002 / 1003 / 1004 / 1005 / 1006 / 1007 / 1008 / received error code (1206, 1219, 2404, …)
		Status Message	

KPI Name	Description	Labels	Possible Values
			Success (0) / STANDBY_ERROR => STANDBY/STANDBY => PRIMARY (0) / Pod Failure (0) / CLI (0) / BFD Failure (0) / Decode Failure (1001) / remote status unavailable (1002) / target role does not support (1002) / Pod Failure (1002) / CLI (1002) / BFD Failure (1002) / site is down (1003) / Pod Failure (1003) / CLI (1003) / BFD Failure (1003) / Traffic Hit (1004) / Pod Failure (1004) / CLI (1004) / BFD Failure (1004) / current role is not STANDBY_ERROR/ STANDBY to reset role (1005) / resetRole: Key not found in etcd (1006) / monitoring threshold per pod is breached (1007) / Retry on heartbeat failure (1008) / received error message (No remote host available for this request / Selected remote host <remotehostname> has no client connection / Sla is expired for transaction / …)

Table 402: geo_replication_finalpull_total KPIs

KPI Name	Description	Label Names	Possible Values
geo_replication _finalpull_total	This KPI displays the total number of geo replications present in the final pull of the feature messages.	**MessageType**	It's a request or a response message type.
		TotalTimeTaken	It's the total time taken to process the request.
		GRInstanceNumber	It's the GR Instance ID in number from the list of the following: • 1 • 2 • Instance.1 • Instance.2

BFD KPIs

The following table lists BFD KPIs.

Table 403: BFD KPIs - 1

KPI Name	Description	Labels	Possible Values
bgp_speaker _bfd_status	This KPI displays BFD link status on BGP Speaker.	status	STATE_UP / STATE_DOWN
geo_bfd_ status	This KPI displays BFD link status on Geo POD.	status	STATE_UP / STATE_DOWN

Table 404: BFD KPIs - 2

KPI Name	Description	Gauge
bgp_speaker _bfd_status	This KPI displays BFD link status on BGP Speaker.	1 (UP) or 0 (DOWN)
geo_bfd_ status	This KPI displays BFD link status on Geo POD.	1 (UP) or 0 (DOWN)

GR Instance Information

Table 405: GR Instance Information KPI

KPI Name	Description	Labels	Possible Values
gr_instance_ information (Type – Guage)	This KPI displays the current role of the GR instance in the application.	gr_instance_id	Configured GR instances value (numerical value)

Geo Maintenance Mode

Table 406: Geo Maintenance Mode KPI

KPI Name	Description	Labels	Possible Values
geo_MaintenanceMode_ info (Type – Guage)	This KPI displays the current state of maintenance mode for the rack.	MaintenanceMode	0: false 1: true

Bulk Statistics

The following section provides details on GR-specific bulkstats.

```
bulk-stats query GR-BGP-Incoming-Failed-Routes
 expression "sum(bgp_incoming_failedrouterequest_total) by (namespace, interface, service_IP,
 next_hop, instance_id)"
 labels     [ instance_id interface next_hop service_IP ]
 alias      gr-bgp-routes-in
exit
bulk-stats query GR-Geo-Monitoring-Failure
 expression "sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover|
RemoteMsgNotifyPrepareFailover|MonitorVip',status!~'success|monitoring.*'}) by (namespace,

AdminNode, ControlActionType, ControlActionNameType,  pod, status, status_code)"
 labels     [ pod AdminNode ControlActionNameType status status_code ]
 alias      gr-geo-monitoring-failure
exit
bulk-stats query GR-Geo-Monitoring-Success
 expression "sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover|
RemoteMsgNotifyPrepareFailover',status=~'success|monitoring.*'}) by (namespace, AdminNode,

ControlActionType, ControlActionNameType,  pod, status)"
 labels     [ pod AdminNode ControlActionNameType status ]
 alias      gr-geo-monitoring
exit
bulk-stats query GR-Geo-Monitoring-Total
 expression "sum(geo_monitoring_total{ControlActionNameType=~'MonitorPod|RemoteMsgHeartbeat|
RemoteMsgGetSiteStatus|RemoteSiteRoleMonitoring|RemoteClusterPodFailure|RemoteMsgNotifyFailover
|RemoteMsgNotifyPrepareFailover|MonitorVip'})
by (namespace, AdminNode, ControlActionType, ControlActionNameType,  pod, status)"
 labels     [ pod AdminNode ControlActionNameType status ]
 alias      gr-geo-monitoring
exit
```

```
bulk-stats query GR-Geo-Replication-Failure
 expression
"sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER',status!='success',
ReplicationRequestType='Response'}) by (namespace, ReplicationNode, ReplicationSyncType,
ReplicationReceiver,ReplicationRequestType,status,status_code)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType status status_code ]
 alias      gr-geo-replication-failure
exit
bulk-stats query GR-Geo-Replication-Success
 expression "sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER',
status='success',ReplicationRequestType='Response'}) by (namespace, ReplicationNode,
ReplicationSyncType,ReplicationReceiver,ReplicationRequestType,status)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType status ]
 alias      gr-geo-replication-success
exit
bulk-stats query GR-Geo-Replication-Total
 expression "sum(geo_replication_total{ReplicationNode=~'CACHE_POD|ETCD|PEER'})
by (namespace, ReplicationNode, ReplicationSyncType,ReplicationReceiver,
ReplicationRequestType,pod)"
 labels     [ pod ReplicationNode ReplicationReceiver ReplicationRequestType
ReplicationSyncType ]
 alias      gr-geo-replication-total
exit
bulk-stats query GR-Trigger-ResetRole-Api
 expression "sum(geo_monitoring_total{ControlActionNameType=~'TriggerGRApi|ResetRoleApi'})

by (namespace, AdminNode, ControlActionType, ControlActionNameType,  pod, status,
status_code)"
 labels     [ pod AdminNode ControlActionNameType status status_code ]
 alias      gr-api
exit
bulk-stats query GR-CDL-Index-Replication
 expression "sum(consumer_kafka_records_total) by (pod, origin_instance_id)"
 labels     [ origin_instance_id pod ]
 alias      gr-cdl-index-replication
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Failures
 expression "sum(datastore_requests_total{local_request='0',errorCode!='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Success
 expression "sum(datastore_requests_total{local_request='0',errorCode='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Inter-Rack-Replications-Total
 expression "sum(datastore_requests_total{local_request='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-inter-rack-replications
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Failures
 expression "sum(datastore_requests_total{local_request='1',errorCode!='0'}) by
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Success
 expression "sum(datastore_requests_total{local_request='1',errorCode='0'}) by
```

```
(operation,sliceName,errorCode)"
 labels     [ sliceName operation errorCode ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Intra-Rack-Operations-Total
 expression "sum(datastore_requests_total{local_request='1'}) by
(operation,sliceName,errorCode)"
 labels     [ errorCode operation sliceName ]
 alias      gr-cdl-intra-rack-operations
exit
bulk-stats query GR-CDL-Session-Count-Per-Slice
 expression
sum(avg(db_records_total{namespace=~'$namespace',session_type='total'})by(systemId,sliceName))by(sliceName)

 labels     [ sliceName ]
 alias      gr-cdl-session-count-per-slice
exit
bulk-stats query GR-CDL-Session-Count-Per-System-ID
 expression sum(avg(db_records_total{namespace=~'$namespace',session_type='total'})
by(systemId,sliceName))by(systemId)
 labels     [ systemId ]
 alias      gr-cdl-session-count-per-system-id
exit
bulk-stats query GR-CDL-Slot-Records-Per-Slice
 expression "sum(slot_records_total{pod=~'.*',systemId!=''}) by (pod, sliceName)"
 labels     [ pod sliceName ]
 alias      gr-cdl-slot-records-per-slice
exit
bulk-stats query GR-CDL-Slot-Records-Per-System-ID
 expression "sum(slot_records_total{pod=~'.*',systemId!=''}) by (pod, systemId)"
 labels     [ pod systemId ]
 alias      gr-cdl-slot-records-per-system-id
exit
bulk-stats query GR-CDL-Total-Session-Count
 expression "sum(db_records_total{namespace=~'$namespace',session_type='total'}) by
(systemId,sliceName)"
 labels     [ sliceName systemId ]
 alias      gr-cdl-total-session-count
exit
```

For more information on GR-related statistics, see the following:

- In RADIUS statistics, you can filter GR-specific statistics using grInstId label.

  For more information, see the *UCC 5G Session Management Function - Metrics Reference*.
- In GTP Endpoint statistics, you can filter GR-specific statistics using gr_instance_id label.

  For more information, see the *UCC 5G Session Management Function - Metrics Reference*.
- In SMF statistics, you can filter GR-specific statistics using gr_instance_id label.

  For more information, see the *UCC 5G Session Management Function - Metrics Reference*.
- In REST Endpoint statistics, you can filter GR-specific statistics using gr_instance_id label.

  For more information, see the *UCC 5G Session Management Function - Metrics Reference*.
- In IPAM-related statistics, you can filter GR-specific statistics using grInstId label.

  For more information, see the *UCC 5G Session Management Function - Metrics Reference*.

Alerts

The following section provides details on GR alerts.

BFD Alerts

The following table list alerts for rule group BFD with *interval-seconds* as 60.

Table 407: Alert Rule Group - BFD

Alert Rule	Severity	Duration (in mins)	Type
BFD-Link-Fail	critical	1	Communication Alarm
	Expression: sum by (namespace,pod,status) (bgp_speaker_bfd_status{status='BFD_STATUS'}) == 0 **Description:** This alert is generated when BFD link associated with BGP peering is down.		

GR Alerts

The following table list alerts for rule group GR with *interval-seconds* as 60.

Table 408: Alert Rule Group - GR

Alert Rule	Severity	Duration (in mins)	Type
Cache-POD-Replication-Immediate-Local	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of CACHE_POD sync type:Immediate and replication receiver:Local is below threshold value.		

Alert Rule	Severity	Duration (in mins)	Type
Cache-POD-Replication-Immediate-Remote	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of CACHE_POD sync type:Immediate and replication receiver:Remote is below threshold value.		
Cache-POD-Replication-PULL-Remote	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='PULL',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='CACHE_POD', ReplicationSyncType='PULL',ReplicationReceiver='remote', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of CACHE_POD sync type:PULL and replication receiver:Remote is below threshold value.		
ETCD-Replication-Immediate-Local	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of ETCD sync type:Immediate and replication receiver:Local is below threshold value.		

Alert Rule	Severity	Duration (in mins)	Type
ETCD-Replication-Immediate-Remote	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'}[1m]))/sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of ETCD sync type:Immediate and replication receiver:Remote is below threshold value.		
ETCD-Replication-PULL-Remote	critical	1	Communication Alarm
	Expresion: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='ETCD', ReplicationSyncType='PULL',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'}[1m]))/ sum by (namespace) (increase(geo_replication_total {ReplicationNode='ETCD',ReplicationSyncType='PULL', ReplicationReceiver='remote',ReplicationRequestType= 'Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of ETCD sync type:PULL and replication receiver:Remote is below threshold value.		
Heartbeat-Remote-Site	critical	-	Communication Alarm
	Expression: sum by (namespace) (increase(geo_monitoring_total{ControlActionNameType= 'RemoteMsgHeartbeat',status!='success'}[1m])) > 0 **Description:** This alert is triggerd when periodic Heartbeat to remote site fails.		
Local-Site-POD-Monitoring	critical	-	Communication Alarm
	Expression: sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='MonitorPod'}[1m])) > 0 **Description:** This alert is triggerd when local site pod monitoring failures breaches the configured threshold for the pod mentioned in Label:{{$labels.AdminNode}}.		

Alert Rule	Severity	Duration (in mins)	Type
PEER-Replication-Immediate-Local	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='PEER', ReplicationSyncType='Immediate',ReplicationReceiver='local', ReplicationRequestType='Response',status='success'} [1m]))/sum by (namespace) (increase(geo_replication_total {ReplicationNode='PEER',ReplicationSyncType= 'Immediate',ReplicationReceiver='local', ReplicationRequestType='Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of PEER sync type:Immediate and replication receiver:Local is below threshold value.		
PEER-Replication-Immediate-Remote	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(geo_replication_total{ReplicationNode='PEER', ReplicationSyncType='Immediate',ReplicationReceiver='remote', ReplicationRequestType='Response',status='success'} [1m]))/sum by (namespace) (increase(geo_replication_total {ReplicationNode='PEER',ReplicationSyncType='Immediate', ReplicationReceiver='remote',ReplicationRequestType= 'Request'}[1m])))*100 < 90 **Description:** This alert is generated when the success rate of PEER sync type:Immediate and replication receiver:Remote is below threshold value.		
RemoteCluster-PODFailure	critical	-	Communication Alarm
	Expression: sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='RemoteClusterPodFailure'}[1m])) > 0 **Description:** This alert is generated when pod failure is detected on the Remote site for the pod mentioned in Label:{{$labels.AdminNode}}.		

Alert Rule	Severity	Duration (in mins)	Type
RemoteMsg NotifyFailover	critical	1	Communication Alarm
	Expression: sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='RemoteMsgNotifyFailover',status!='success'}[1m])) > 0 **Description:** This alert is generated when transient role RemoteMsgNotifyFailover has failed for the reason mentioned in Label:{{$labels.status}}.		
RemoteMsg NotifyPrepare Failover	critical	1	Communication Alarm
	Expression: sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='RemoteMsgNotifyPrepareFailover',status!='success'}[1m])) > 0 **Description:** This alert is generated when transient role RemoteMsgNotifyPrepareFailover has failed for the reason mentioned in Label:{{$labels.status}}.		
RemoteSite-RoleMonitoring	critical	-	Communication Alarm
	Expression: sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='RemoteSiteRoleMonitoring'}[1m])) > 0 **Description:** This alert is generated when RemoteSiteRoleMonitoring detects role inconsistency for an instance on the partner rack and accordingly changes the role of the respective instance on local rack to Primary. The impacted instance is in Label:{{$labels.AdminNode}}.		
ResetRoleApi -Initiated	critical	-	Communication Alarm
	Expression: sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='ResetRoleApi'}[1m])) > 0 **Description:** This alert is generated when ResetRoleApi is initiated with the state transition of roles mentioned in Label:{{$labels.status}}.		
TriggerGRApi -Initiated	critical	-	Communication Alarm
	Expression: sum by (namespace,status) (increase(geo_monitoring_total{ControlActionNameType ='TriggerGRApi'}[1m])) > 0 **Description:** This alert is generated when TriggerGRApi is initiated for the reason mentioned in Label:{{$labels.status}}.		

Alert Rule	Severity	Duration (in mins)	Type
VIP-Monitoring -Failures	critical	-	Communication Alarm
	Expression: sum by (namespace,AdminNode) (increase(geo_monitoring_total{ControlActionNameType ='MonitorVip'}[1m])) > 0 **Description:** This alert is generated when GR is generated upon detecting VIP monitoring failures for the VIP and Instance mentioned in the Label:{{$labels.AdminNode}}.		

CDL Alerts

The following table list alerts for rule group CDL with *interval-seconds* as 60.

Table 409: Alert Rule Group - CDL

Alert Rule	Severity	Duration (in mins)	Type
GRPC-Connections-Remote-Site	critical	1	Communication Alarm
	Expression: sum by (namespace, pod, systemId) (remote_site_connection_status) !=4 **Description:** This alert is generated when GRPC connections to remote site are not equal to 4.		
Inter-Rack -CDL-Replication	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(datastore_requests_total{local_request=\"0\", errorCode=\"0\"}[1m]))/sum by (namespace) (increase(datastore_requests_total{local_request=\"0\"} [1m])))*100 < 90 **Description:** This alert is generated when the Inter-rack CDL replication success rate is below threshold value.		
Intra-Rack -CDL-Replication	critical	1	Communication Alarm
	Expression: (sum by (namespace) (increase(datastore_requests_total{local_request=\"1\", errorCode=\"0\"}[1m]))/sum by (namespace) (increase(datastore_requests_total{local_request=\"1\"} [1m])))*100 < 90 **Description:** This alert is generated when the Intra-rack CDL replication success rate is below threshold.		

Inter-site Geographic Redundancy

Inter-site geographic redundancy is the practice of implementing redundancy and failover mechanisms across multiple sites or locations. The purpose of inter-site redundancy is to ensure that critical services and applications remain available even in the event of a catastrophic failure at one site.

Feature Description

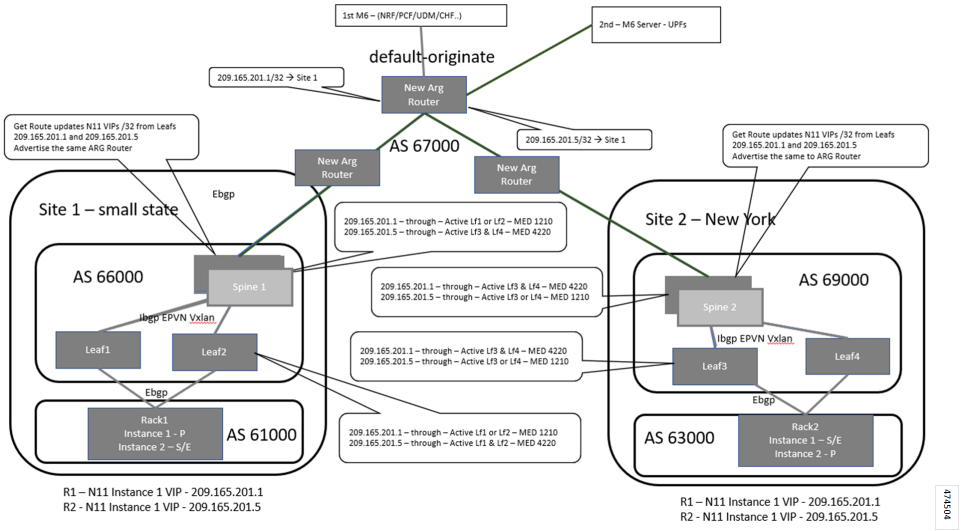
Mobile operators set up the redundant data centers in different geographical locations, so that if one data center goes down, the other can take over. This feature allows to extend the existing inter-rack solution to the inter-site solution. The current notation of HA inside a rack continues to work in conjunction with inter-site redundancy to provide a more comprehensive high availability solution.

Note Inter-site and inter-rack solution cannot co-exist together, so customer need to select any one of the solutions.

Architecture

The SMF implements the 1:1 model of inter-site redundancy, also known as active:active model. This model is a type of redundancy configuration in which all sites in a network are actively processing traffic simultaneously, and each site is capable of taking over the full load of the network in case of a failure at another site.

The following topology diagram describes about the inter-site redundancy deployment architecture.



Prerequisites

Following is the list of the minimum site requirements for the 1:1 deployment model for each site:

- Two leaves

- Two spines
- One K8 cluster with logical SMF containing two GR instances

Note Each GR instance is the set of unique EPC, RADIUS, and N11 endpoints with same configuration in both the sites.

- UPF would be deployed in 1:1 configuration

Note Active and standby UPF instances are associated with GR instances, and UPF carries only N4 address of both the GR instances in control plane profile.

General Guidelines

The configuration for the various modules in the inter site redundancy remains the same as inter rack redundancy. See the following for details of the various modules configurations:

- Configuring BGP Speaker, on page 1210
- Configuring Endpoint Instance Awareness, on page 1203
- Configuring ETCD/Cachepod Replication, on page 1214
- Configuring Inter-Rack Redundancy Instance, on page 1202
- Configuring IPAM, on page 1212
- Pod Monitoring, on page 1215

How It Works

Most of the configurations for the inter-rack and inter-site are same, except for the configurations that are required for managing and monitoring redundancy events, and replicating sessions across the sites.

Following are the guidelines to achieve the seamless communication between the sites in the inter-site redundancy implementation:

- Prepend the autonomous systems (AS) path in the BGP (Border Gateway Protocol) route advertisement configuration. For more information, see Configuration for Inter-site Deployment, on page 1269.
- L3 routing of the Geo-pod, CDL-ep (s), and CDL-Kafka-servers.

BGP Route Advertisement

In the inter-site redundancy deployment, the Multi-exit Discriminator (MED) attribute, which is a non-transitive BGP attribute, is used to inform the neighboring routers of the best path to reach the active service VIP. However, MED values are not shared beyond neighboring routers to their eBGP peers.

In the inter-rack deployment model, AS-path prepending technique is used in BGP to influence the path selection of routes advertised to other BGP routers. AS-path prepending technique makes a certain route more favorable over another by manipulating the AS-path in the BGP route advertisement. The difference in the number of AS-paths getting prepended by software logic helps to provide guidance to upstream routers to choose the best routable path.

Following table captures the number of AS-path prepend required for various combination of service VIP and interface bonding status.

GR Role	Bonding interface active	VIP present	MED value	Local Preference	AS-Path Prepend (Number of times)
Primary Role (active)	Yes	Yes	1210	2220	3
	Yes	No	1220	2210	3
	No	Yes	1215	2215	3
	No	No	1225	2205	3
Standby Role	Yes	Yes	2210	1220	6
	Yes	No	2220	1210	6
	No	Yes	2215	1215	6
	No	No	2225	1205	6
Standby-Error Role	NA	NA	3220	220	9

KPI

prepend_as_path_count” label is added in the following existing metrics.

- bgp_outgoing_failedrouterequest_total
- bgp_outgoing_routerequest_total

The above metrics are populated when routes are advertised.

BGP Outgoing Failed Route Request KPI

KPI Name	Description	Labels	Possible Values
bgp_outgoing_failedrouterequest_total	This Key Performance Indicator (KPI) represents the total number of failed outgoing routes.	app_name	Application Name
		cluster	Local
		data_center	DC
		instance	1
		instance_id	1
		interface	bd2.nrf.2275
		local_pref	320
		med	3220
		next_hop	50.50.50.50
		prepend_as_path_count	"9->STANDBY_ERROR"
		service_IP	10.10.10.10
		service_name	bgpspeaker-pod
		vrf	Default

BGP Outgoing Route Request Total KPI

KPI Name	Description	Labels	Possible Values
bgp_outgoing_routerequest_total	This Key Performance Indicator (KPI) represents the total number of outgoing routes.	app_name	Application Name
		cluster	Local
		data_center	DC
		instance	1
		instance_id	1
		interface	bd2.nrf.2275
		local_pref	320
		med	3220
		next_hop	50.50.50.50
		prepend_as_path_count	"9->STANDBY_ERROR"
		service_IP	10.10.10.10
		service_name	bgpspeaker-pod
		vrf	Default

Note The above metrics are populated when routes are advertised.

Values for As-Path metrics:

New label "prepend_as_path_count" includes the following values based on RoleInfo:

- Inter Rack/Prepend CLI disabled:
  - prepend_as_path_count="Not-Applicable"
- Prepend CLI enabled/Primary, Traffic_Hit reason:
  - prepend_as_path_count="0->PRIMARY,TRAFFIC_HIT"
- Prepend CLI enabled/Primary, Non Traffic_Hit reason:
  - prepend_as_path_count="3->PRIMARY"
- Prepend CLI enabled/STANDBY:
  - prepend_as_path_count="6->STANDBY"
- Prepend CLI enabled/STANDBY_ERROR:
  - prepend_as_path_count="9->STANDBY_ERROR"

Configuration for Inter-site Deployment

To enable the inter-site deployment, you must configure the AS-path prepend flag in the BGP configuration.

Following is the sample configuration:

```
config
  router local_as_number
    bfd bfd_configuration
    interface bgp_local_interface
    prepend as-path { false | true }
    exit
   exit
```

NOTES:

- **interface** *bgp_local_interface*: Specify BGP local interface.
- **prepend as-path { false | true }**: Select **true** to enable the Inter-site deployment. By default this option is disabled.

  If this option is set to **false**, the logical SMF deployment follows the inter-rack model.

Configuration Verification

To verify the configuration, use the following show command:

```
smf# show running-config router
router bgp 63200
 learnDefaultRoute false
 prepend as-path true  ——————————————> as-path
 bfd interval 250000 min_rx 250000 multiplier 3
 interface enp216s0f0.2119
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 101.101.172.254 remote-as 63100 fail-over bfd
 exit
 interface enp216s0f0.2129
  vrf vrf_papn1
  bondingInterface enp216s0f0
  bondingInterface enp94s0f1
  neighbor 101.101.174.254 remote-as 63100 fail-over bfd
 exit
 interface enp216s0f0.2139
  vrf vrf_papn2
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 101.101.178.254 remote-as 63100 fail-over bfd
 exit
```

Following is the sample ouput of the bgp-advertised routes corresponding to the GR role.

```
[smf] smf# show role instance-id 1
result "PRIMARY"
[smf] smf# show bgp-advertised-routes
bgp-route

-----bgpspeaker-pod-0 ----
   Network              Next Hop                AS_PATH          Age        Interface
    Vrf                       Attrs
*> 209.165.200.228    209.165.200.229       63000 63000 63000   00:00:47      ens161
   Default      [{Origin: e} {LocalPref: 2205} {Med: 1225}]
```

L3 Routing of Pods

In the inter-rack solution, leaf and spine servers were incorporated into the same AS-path to enable the utilization of VxLAn techniques. This deployment model allows for the support, monitoring, and exchange of redundancy data and events among various pods, while remaining reachable across racks. Specifically, the external IP address of the Geo-pod on both racks were integrated into a common subnet, enabling data exchange without the need for route discovery as they shared the same VLAN. Additionally, communication between racks remained within the boundaries of the leaf and spine servers, without the need for packets to traverse beyond them.

The following PODs require external connectivity between the sites:

- Geo-pod
- CDL-ep (s)
- CDL-Kafka-server(s)

Unlike service VIPs, these IP addresses do not require floating across sites. A routing decision needs to be made only once during production deployment. Therefore, static routing was used instead of advertising these external IP addresses through BGP.

Static routes are added to the local K8S cluster protocol nodes for reaching remote CDL/Kafka/Geo Networks. The leafs automatically advertise all connected local CDL/Kafka/Geo Networks to the spines. The spines redistribute those routes to the Arg router. The Arg routers know how to reach both Sites' CDL/Kafka/Geo

Networks. If a packet is destined for a remote CDL/Kafka/Geo network, the local K8S protocol node has a static route that points to the local leaf. The packet then goes to the spine. The spines have a default route that points to the Arg router. The Arg routers have proper routes to send packets to the remote site.

In addition, the Arg routers are configured with the "default-originate" keyword, which designates the ARG routers as the default gateway for the spines. Consequently, the spines redirect all traffic for which a routing path is not available in the spines to the Arg routers.

Inter-site Redundancy Scenarios

This section describes that how the inter-site redundancy deployment works in the different scenarios:

In a scenario with two sites and both operational, each site have one primary/active GR (Gateway Router) instance. The endpoint configured on each site carries traffic corresponding to its active instance. It is possible that the Aggregation Router (ARG) may not be directly connected to the sites, and there could be multiple autonomous systems between the ARG and sites. The ARG router is responsible for the convergence of the routes from both sites.

Following are the various scenarios for the site redundancy:

- During sunny weather conditions, Site A advertises the best route for GR1 and a less favorable route for the endpoint associated with GR2.

  On the ARG, following are the routes:

  - Routes from Site A
    - 209.165.200.225 AS-Path 65000 65000 65000 65000
    - 209.165.200.235 AS-Path 65000 65000 65000 65000 65000 65000 65000

  - Routes from Site B
    - 209.165.200.225 AS-Path 64000 64000 64000 64000 64000 64000
    - 209.165.200.235 AS-Path 64000 64000 64000 64000

  - Best Path:
    - Site-A 209.165.200.225 AS-path 65000 65000 65000 65000
    - Site -B 209.165.200.235 AS-path 64000 64000 64000 64000

Now if the Site A goes down:

The BGP session on the ARG routers goes down after the BGP convergence time, resulting in the withdrawal of routes learned from Site A. The current state of routes at ARG is as follows.

- Routes from Site B:
  - 209.165.200.225 AS-Path 64000 64000 64000 64000 64000 64000 64000
  - 209.165.200.235 AS-Path 64000 64000 64000 64000

  Now the traffic for both the endpoints 209.165.200.225 and 209.165.200.225 is being sent towards site B.

- The traffic monitoring feature at site B has identified traffic for the IP address 209.165.200.225. Once the packet threshold for this IP address is exceeded, the GeoReplication pod triggers the transition of the GR-1 instance from standby mode to active mode.
- After the Geo-pod notifies the BGPSpeaker-pod of the transition of GR1 to the primary instance, the BGPSpeaker-pod readvertises the routes for the GR1 endpoint using the most favorable routing path.
- Now the routes in the ARG are updated with following information:
  - Routes from site B:
    - 209.165.200.225 AS-Path 64000 64000 64000 64000
    - 209.165.200.235 AS-Path 64000 64000 64000 64000

Split Brain

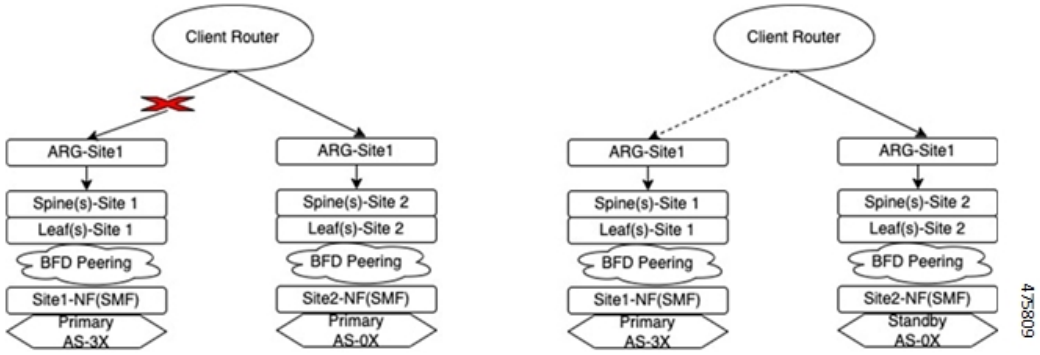
When deploying across multiple sites, the failure domain expands. Failures that occur within the leaf/spine architecture and rack are well-managed, and the state of the GR instances during these failures is well-defined and follows the same mechanism as the Inter-Rack solution. However, if there are failures outside the data center, such as link fluctuations on external routers, there is no mechanism for the rack with an active GR instance in cases where communication with the peer rack is lost.

If the link between the Client Router and Data Center Router goes down, connectivity between the racks is lost. The Client Router then sends incoming data traffic to the next preferred site, which is Site 2 in this case. Site 2 has traffic monitoring enabled, which detects the traffic, and once the incoming traffic threshold is met, the GR instance is transitioned from Standby to Primary. At this point, both Site 1 and Site 2 are active for this GR instance. If the link between ARG-Site1 and the Client Router is restored, a dual-active or split-brain scenario occurs.

This instance leads to the following scenarios:

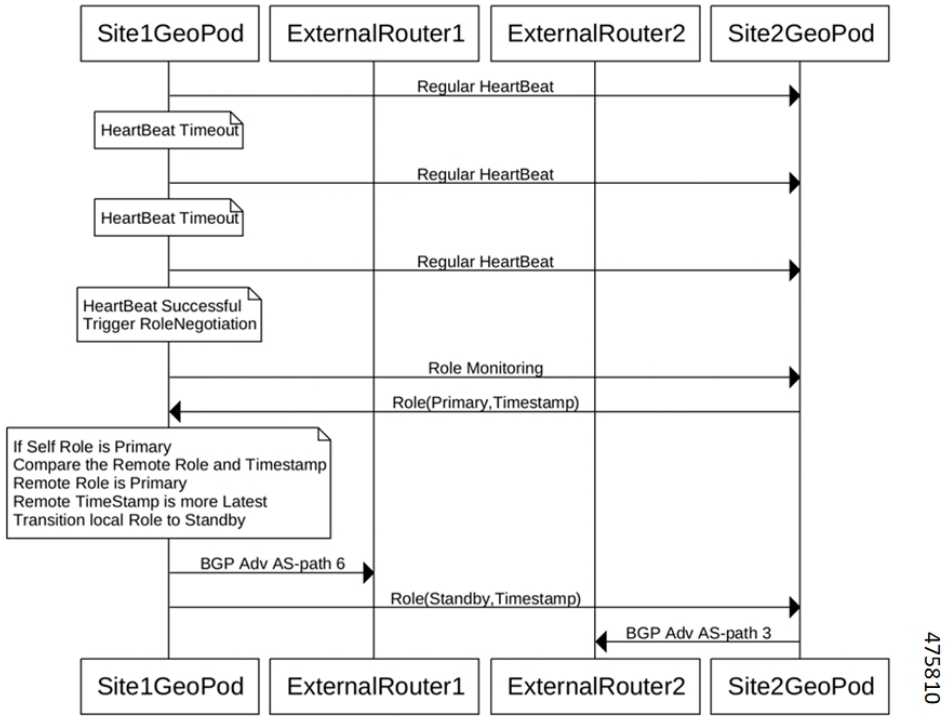
1. If the Client Router distributes traffic between ARG-Site1 and ARG-Site2, it results in call loss and disruptions in customer service.
2. Post external link recovery, which site to consider primary and how to move the other site to standby.

To address the issue of traffic being distributed between the two sites, solution is to not prepend any AS-path when the GR instance transitions from standby to Primary due to traffic monitoring. The new Primary site then performs the BGP readvertising without any explicit local AS path pre-pending, making this site the most preferred even if the peer site comes back online. This approach ensures that traffic is directed to the Primary site until the Secondary site is restored and fully operational.



To address the issue of Site Role transition after external link recovery, solution is to keep a timestamp for every role transition. When the link is restored, communication occurs between the Site-1/Geo-Pod and Site-2/Geo-Pod, during which both the pods exchange the role state and timestamp on which the transition occurred. The site with the older timestamp then transitions from Primary to Standby, ensuring that the most recent Primary site maintains its role after the link is restored.

Note The timestamp update happens only when there is a change in the role. If there is a change in the reason, the timestamp remains unchanged. When detecting the initial split brain, the preference is given for the Site/Rack combination with the role primary and the reason traffic-hit.



KPI

As part of this feature, the following Key Performance Indicators (KPIs) are associated with split brain support.

Geo Split Brain Detection Total KPI

KPI Name	Description	Labels	Possible Values
geo_split_brain_detection_total	This Key Performance Indicator (KPI) represents the overall count of Split Brain Detection instances.	GRInstanceNumber	It's the GR Instance ID and value can be any one from the following: • instance.1 • instance2.
		LocalSiteRole	This is local site's role as a number. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role) • 6 (for Standby-error role)
		LocalSiteReason	This is local site's reason's string value: • "CLI" • "BFD Failure" • "POD Failure" • "TRAFFIC Hit" • "UPGRADE" • "STARTUP" • "STUCKED Role" • "SITE Notification" • "REMOTE Monitoring" • "SPLITBRAIN Recover" • "DELETE Notification" • "HEARTBEAT Recover"
		LocalSiteTimeStamp	Local site's timestamp when role was last updated.
		RemoteSiteRole	This is remote site's role as a number. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role) • 6 (for Standby-error role)
		RemoteSiteReason	

KPI Name	Description	Labels	Possible Values
			This is remote site’s reason’s string value: • "CLI" • "BFD Failure" • "POD Failure" • "TRAFFIC Hit" • "UPGRADE" • "STARTUP" • "STUCKED Role" • "SITE Notification" • "REMOTE Monitoring" • "SPLITBRAIN Recover" • "DELETE Notification" • "HEARTBEAT Recover"
		RemoteSiteTimeStamp	Remote site’s timestamp when role was last updated.

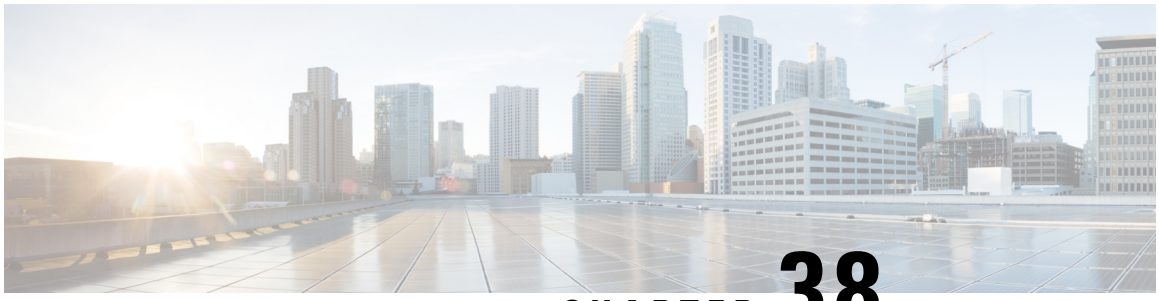
Geo Split Brain Resolution Total

KPI Name	Description	Labels	Possible Values
geo_split_brain_resolution_total	This Key Performance Indicator (KPI) represents the overall count of split brain resolution instances.	GRInstanceNumber	It's the GR Instance ID and value can be any one from the following: • instance.1 • instance2.
		LocalSiteRole	This is local site's role as a number. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role) • 6 (for Standby-error role)
		LocalSiteReason	This is local site's reason's string value: • "CLI" • "BFD Failure" • "POD Failure" • "TRAFFIC Hit" • "UPGRADE" • "STARTUP" • "STUCKED Role" • "SITE Notification" • "REMOTE Monitoring" • "SPLITBRAIN Recover" • "DELETE Notification" • "HEARTBEAT Recover"
		LocalSiteTimeStamp	Local site's timestamp when role was last updated.
		RemoteSiteRole	This is remote site's role as a number. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role)
		RemoteSiteReason	

KPI Name	Description	Labels	Possible Values
			This is remote site's reason's string value: • "CLI" • "BFD Failure" • "POD Failure" • "TRAFFIC Hit" • "UPGRADE" • "STARTUP" • "STUCKED Role" • "SITE Notification" • "REMOTE Monitoring" • "SPLITBRAIN Recover" • "DELETE Notification" • "HEARTBEAT Recover"
		RemoteSiteTimeStamp	Remote site's timestamp when role was last updated.
		OldRole	The role before split-brain resolution. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role)
		NewRole	The new role after split-brain resolution. This can be any one of below values: • 3 (for Standby role) • 6 (for Standby-error role)

Geo Role Reason Change Total

KPI Name	Description	Labels	Possible Values
geo_role_reason_change_total	This Key Performance Indicator (KPI) represents the overall count of the total number of times the role reason has been changed to HEARTBEAT Recover.	GRInstanceNumber	It's the GR Instance ID and value can be any one from the following: • instance.1 • instance2.
		LocalSiteRole	This is local site's role as a number. This can be any one of below values: • 2 (for Primary role) • 3 (for Standby role) • 6 (for Standby-error role)
		oldReason	This is local site's reason's string value before HEARTBEAT Recover: • "HEARTBEAT Recover"
		NewReason	This is local site's reason's string value: • "HEARTBEAT Recover" **Note** Currently, this transition occurs exclusively based on Traffic Hit.



CHAPTER 38

Roaming Support

- Feature Summary and Revision History, on page 1281
- Feature Description, on page 1282
- Local Breakout Roaming Support, on page 1283
- Home Routed Roaming Support, on page 1291
- N3 and N9 User Plane Separation, on page 1328
- Allowed PLMN List Support, on page 1332
- Inter-plmn Roaming Mobility Support, on page 1332
- Roaming Status on N4 Interface, on page 1342
- Troubleshooting Information, on page 1343

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 410: Revision History

Revision Details	Release
SMF supports the following Roaming functionalities: • N3 and N9 Separation for Homer and Roamer calls • Support for Allowed PLMN list and Requester PLMN list through CLI configuration • Roaming status on N4 messages • SMF supports the failure handling for N16 hSMF or vSMF and SEPP.	2023.03.0
The following enhancements were introduced: • Home Routed (HR) Roaming Support • Security Edge Protection Proxy (SEPP) Support • Handover Support in HR Roaming	2021.02.3
First introduced.	2021.01.0

Feature Description

This chapter provides an overview of the roaming features that are supported on SMF. Mobile network operators form roaming partnerships to provide seamlessl services to subscribers in geographies beyond network reach. PLMN designates the operator network boundaries. hPLMN denotes the home network of subscribers. vPLMN denotes the visited network from where the services are rendered.

Roaming support for SMF can be classified as follows:

- LBO (local breakout) roaming – vPLMN locally provides packet core services and access to data network.
- HR (home routed) roaming – vPLMN provides packet core services and hPLMN provides access to data network.

Local Breakout Roaming Support

Feature Description

Important The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

VPLMN provides packet core services and access to data network. This feature enables the SMF to support the flavour of routing that is termed as the local breakout (LBO) roaming.

This feature provides the following functionalities:

- Roaming for 5G sessions connected via NR
- Roaming for 4G and Wi-Fi sessions connected via E-UTRAN
- LI support
- Deployment model without SEPP

For more details on the serving PLMN, see Multiple PLMN Support, on page 855 chapter.

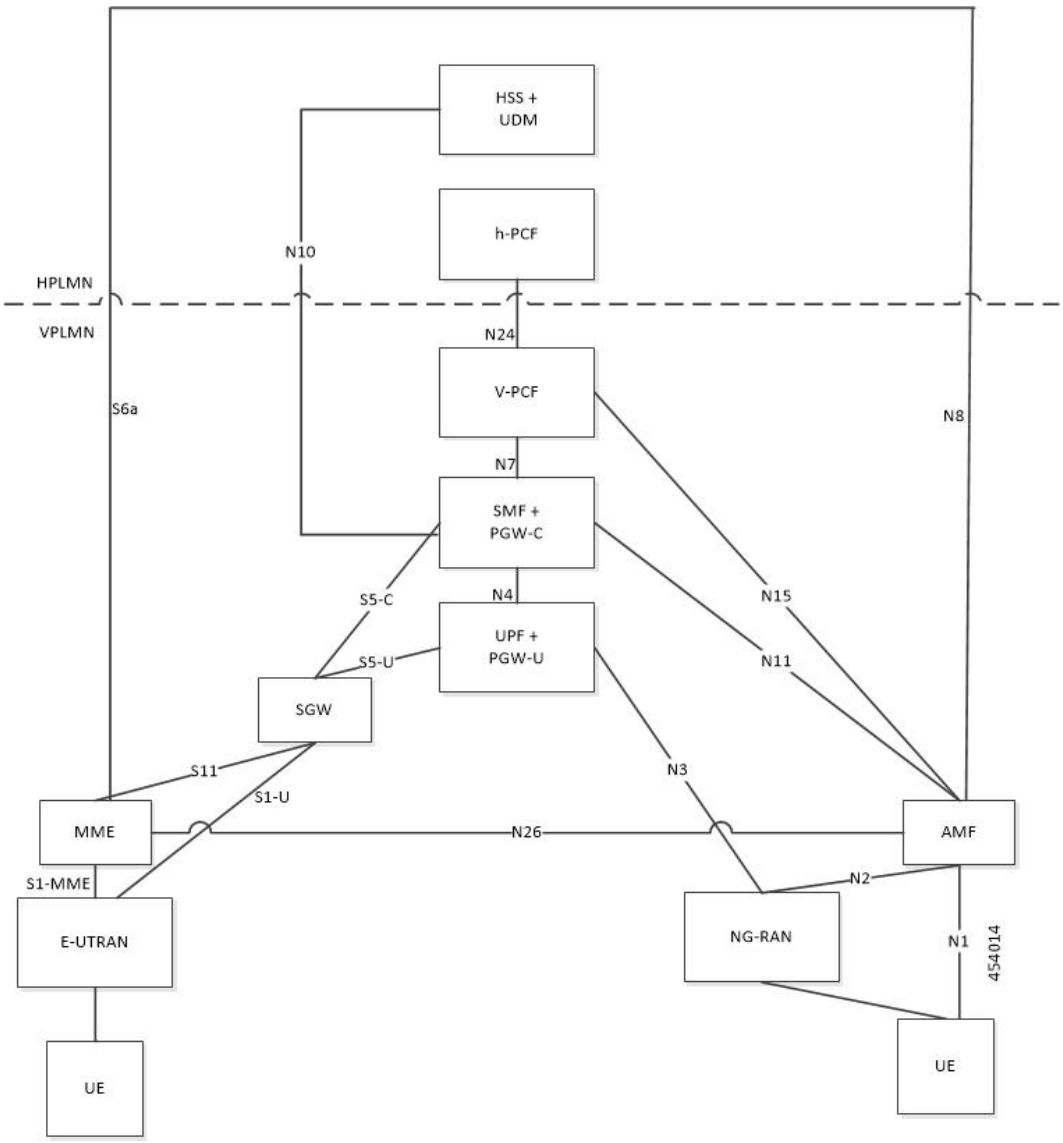
Architecture

This section describes the architecture for the LBO roaming feature.

EPC LBO Scenario

The following diagram shows the LBO roaming architecture for the 4G sessions connected to the SMF and PGW-C in EPC.

Figure 233: Local Breakout Roaming Architecture for 4G Sessions

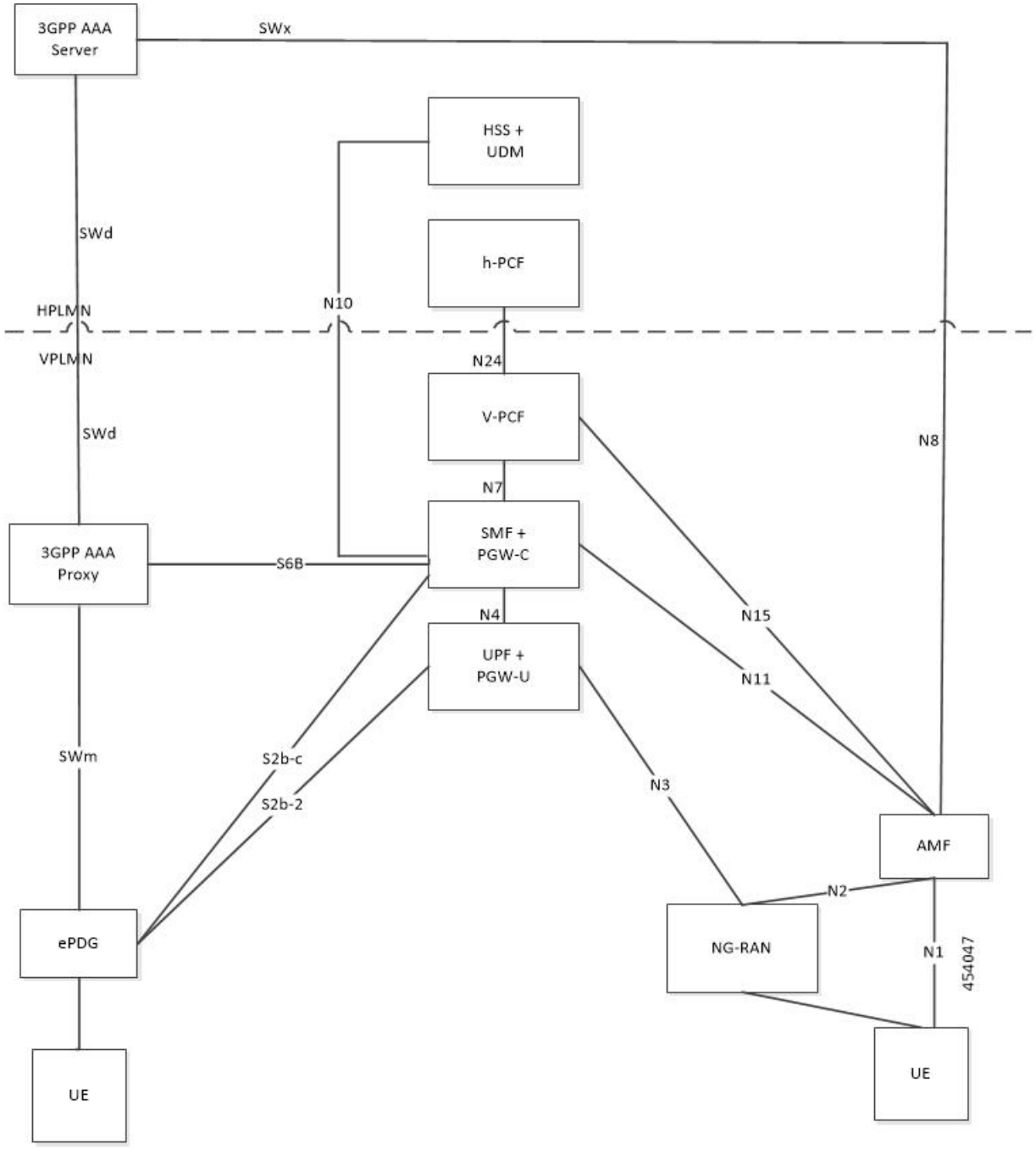


During LBO roaming for 4G sessions, the SGW and the SMF with PGW-C both reside in VPLMN. The SGW and SMF exchange messages through S5-C interface. All northbound SBI interfaces are common for 4G and 5G. The SMF interacts with vPCF, vCHF, and UDM.

ePDG LBO Scenario

The following diagram shows the LBO roaming architecture for the Wi-Fi sessions connected to the SMF and PGW-C in EPC.

Figure 234: Local Breakout Roaming Architecture for Wi-Fi Sessions

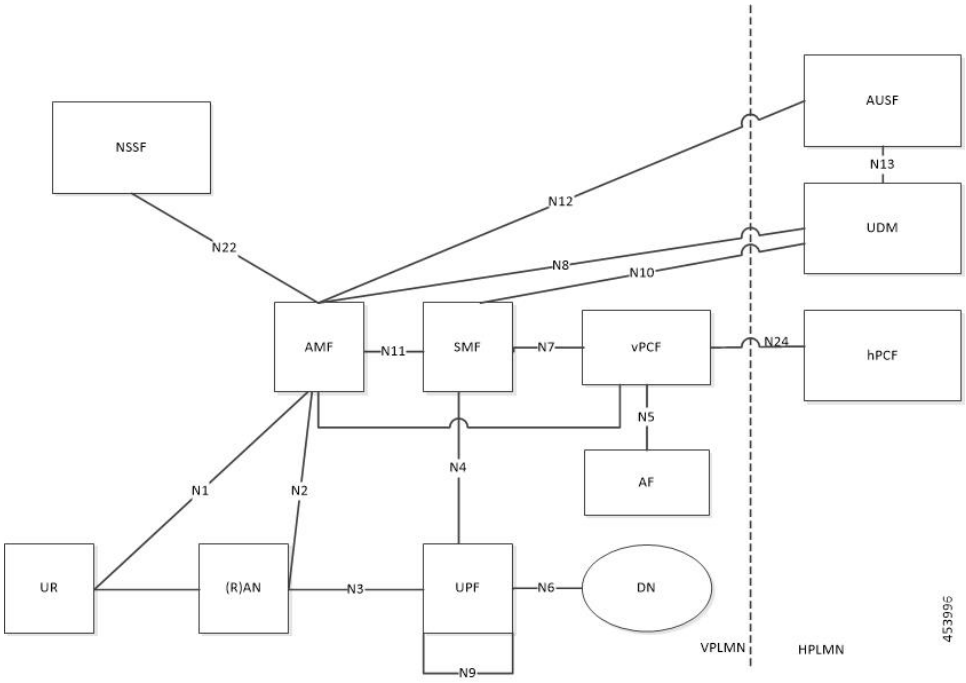


SMF resides in VPLMN and interacts with vPCF, vCHF, and UDM. SMF doesn't support S6b toward the 3GPP AAA server, but uses the N10 interface.

5G NR LBO Scenario

The following diagram shows the LBO roaming architecture for the 5G sessions connected through NR.

Figure 235: LBO Roaming Architecture for 5G Sessions



As shown in the preceding diagram, the SMF resides in the VPLMN. Only AUSF and UDM are the NFs in the HPLMN. The PCF in the VPLMN communicates with PCF in the HPLMN over N24 interface. The PCFs communicate with each other to get the policies related to the subscriber session and pass them to SMF.

SMF Functionalities During LBO

The SMF supports the following functionalities related to LBO for in-roamers.

- Detection of in-roamers based on local configuration and MCC and MNC in the SUPI received
- N11
  - Determination of LBO for the in-roamers
  - If the SMF receives the session setup request for a visitor without the support for LBO, then the SMF sends an error to the AMF. Then, the AMF reattempts the session setup with the SMF that supports Home Routed (HR) roaming.
  - Support of PCF ID that is vPCF from the AMF
- N2
  - The SMF provides Single Network Slice Selection Assistance Information (S-NSSAI) of VPLMN in the N2 SM Information.
- N7
  - Selection of PCF in VPLMN
  - vPCF interacts with AF in HPLMN for PCC rule generation (for example, IMS). However, PCC rules are generated using roaming policies and the subscribed policies in HPLMN are inaccessible

by vPCF. Also, vPCF doesn't interact with CHF for spending limits. The PCC rules in LBO have limited capabilities.

- N40
  - Selection of CHF in VPLMN. vSMF considers additional parameters of the HPLMN ID that CHF has to service the roamer status (in-roamer) of the UE.
- N10
  - Selection of UDM in HPLMN
- NRF
  - The SMF uses the **chf-supported-plmn** query parameter while discovering the vCHF servicing HPLMN.
  - During EPS procedures, if the SMF supports more than one S-NSSAI and the APN is valid for more than one S-NSSAI, then it performs the Nnssf_NSSelection_Get service operation. This operation is in effect before the SMF provides an S-NSSAI to the UE. This operation helps to retrieve the mapping of the subscribed S-NSSAIs to the serving PLMN S-NSSAI values.
- Emergency services on SMF are supported only in LBO model. For LBO roaming, the SMF does not register with UDM for an emergency session.

  For emergency calls, the SMF ignores the UE PLMN ID and relays the serving PLMN ID across all the interfaces.

Network Slicing

The SMF supports the following functionalities related to network slicing:

- The SMF can be configured with a list of allowed NSSAI.
- When the SMF acts as a vSMF during roaming, the S-NSSAI of the UE used in the VPLMN must be the value that is configured on the SMF.
- In the case of LBO, the SMF performs mapping of S-NSSAI received from UDM to the NSSAI of HPLMN received during PDU connection setup. The received NSSAI must be configured on vSMF as the supported NSSAI.

Node Selection Considerations

The following criteria are applied for selecting the nodes in the LBO roaming:

- When roaming is enabled, each SMF registers the inter-PLMN FQDN value with the NRF. This operation helps the AMF to select the hSMF in a different PLMN.
- The SMF treats **target-plmn-list** and **requester-plmn-list** as the query parameters.
- The NRF in the serving PLMN handles all the discovery requests from the NFs.

PDU Establishment During LBO

The following conditions are considered for PDU session establishment in LBO roaming case:

- If the SMF receives the session setup request for a visitor without support for LBO, then the SMF sends SM Context Create error to the AMF with the cause HOME_ROUTED_ROAMING_REQUIRED. Then, the AMF reattempts the session setup with the SMF that supports Home Routed (HR) roaming. An example scenario is when the NAS PDU Session Establishment Request has requested SSC mode as 3 and the allowed SSC mode in vSMF does not support the SSC mode 3.
- The SMF receives both HPLMN S-NSSAI and S-NSSAI. The SMF uses S-NSSAI to validate NSSAI against the vSMF supported NSSAI.
- On N40 interface:
  - vSMF sends the roamerInOut attribute to CHF through the CDR message. The roamerInOut attribute includes PDUSessionChargingInformation and userInformation. This attribute value is either IN_BOUND for in-roamers or OUT_BOUND for out-roamers.
  - vSMF sends the PDUSessionInformation and chargingCharacteristicsSelectionMode IE with appropriate value (HOME_DEFAULT, ROAMING_DEFAULT, and VISITING_DEFAULT) for non-roaming and roaming cases.
  - The hPlmnId and servingCNPlmnId fields in the PDUSessionInformation IE carry the value as per the roaming status of the UE.
- During N1N2 Message Transfer, the S-NSSAI provided in N2 content should be the same as the VPLMN S-NSSAI.
- For LBO roaming scenario, the PDU Session Establishment Accept message includes the S-NSSAI from the allowed NSSAI for the VPLMN. It also includes the corresponding S-NSSAI of the HPLMN from the mapping of allowed NSSAI that the SMF received from AMF.
- The SMF uses HPLMN for UDM discovery during LBO roaming.

PDN Establishment During LBO

The S-GW sends Serving Network IE to the PGW-C with the PLMN ID where the S-GW belongs. The SMF uses that PLMN as VPLMN for validation, node selection, and passing on the VPLMN to other north bound interfaces.

The N40 interface related requirements and the emergency session-related requirements applicable for 5G session creation, also apply for the 4G and Wi-Fi sessions.

PLMN Usage

The following table shows an example of how the PLMN values configured in SMF service profile are relayed across all the interfaces.

Interface	Attribute	Homer	In-roamer (LBO)	Out-roamer (HR)	In-roamer (HR)
	UE PLMN	310-240	262-06	310-310	302-610
NRF	plmn-list in nrf Discover to discover UDM (queryParam = target-plmn)	UE PLMN	UE PLMN	UE PLMN	Not applicable

Interface	Attribute	Homer	In-roamer (LBO)	Out-roamer (HR)	In-roamer (HR)
NRF	plmn-list in nrf Discover to discover PCF/CHF(queryParam = target-plmn)	UE PLMN	Serving PLMN	UE PLMN	Serving PLMN
N10	PLMN in smfRegistration IE in N10 registration	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable
N10	PLMN in GET subscription URI	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable
N10	PLMN in sdmSubscription IE in N10 subscribe ToNotification	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable
N40	PLMN in NfConsumer identification IE in N40 charging data request	Primary home PLMN	Primary home PLMN	Primary home PLMN	Primary home PLMN
N40	hPlmnId in PDUSession Information IE in pduSession Charging Information in chargingData Request	UE PLMN	UE PLMN	UE PLMN	UE PLMN
N40	Serving PLMN in PDU Session Information IE in pduSession ChargingInformation in chargingData Request	Serving PLMN	Serving PLMN	Primary home PLMN	Serving PLMN

Interface	Attribute	Homer	In-roamer (LBO)	Out-roamer (HR)	In-roamer (HR)
N7	PLMN in PCF notify for AC_TY_CH/ SAREA_CH/ RAT_TY_CH trigger	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable
N7	PLMN in create request to PCF	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable
RADIUS	PLMN in 3GPP UE location IE RADIUS authentication	Serving PLMN	Serving plmn	Not applicable	
RADIUS	PLMN in 3GPP GGSN MCC MNC in RADIUS authentication	Primary home PLMN	Primary home PLMN	Not applicable	
N4	PLMN in X-header of N4 requests	Serving PLMN	Serving PLMN	Primary home PLMN	Not applicable

Roaming Status Determination

The SMF extracts the UE PLMN from SUPI. The SMF compares the UE PLMN and the serving PLMN with the configured PLMN list. The SMF determines the roaming status of subscribers based on the HPLMN values.

If the UE PLMN and the serving PLMN both belong to the PLMN list configured in SMF, then it is a home subscriber. If the UE PLMN does not belong to the configured PLMN list and the serving PLMN belongs to the configured PLMN list, then it is a visitor. If the UE PLMN belongs to the configured PLMN list and the serving PLMN does not belong to the configured PLMN list, then it is a roamer.

Handover Scenarios

Once the roaming status is determined, there will be no change to the status even if the configuration of PLMN values changes after the handover (HO).

Local Policies

In HO scenarios, vSMF supports local policy to enable vPLMN operators to override the signaled parameter from hPLMN domain as per the roaming agreements. The SMF uses the local policies to—

- allow always-on session requests.
- perform paging policy differentiation

- allow PDU session setup in HR or LBO mode
- support subscriber QoS as per the roaming agreement
- allow ARP priority levels 1-8 for HO roaming sessions.

Other Procedures

Paging Policy Differentiation (PPD)

The SMF needs a configuration per PLMN to allow different PPD profiles for different roaming partners. The vSMF picks the appropriate configuration for the HPLMN and applies the same for the roaming session.

PCF and UDM Selection

During roaming, the AMF selects both vPCF and hPCF and sends the vPCF ID and hPCF ID to the SMF and vPCF respectively during policy association. The SMF selects the PCF using the received vPCF ID. During AMF relocation, target AMF selects a new vPCF and hPCF. The SMF receives a redirection indication with PCF ID from the existing PCF for the PDU session. The SMF terminates the current SM Policy Control association and reselects a PCF based on the received PCF ID. The SMF then establishes an SM Policy Control association with the reselected PCF.

For selection of PCF and UDM based on local configuration, the locally configured addresses map to the VPLMN and HPLMN respectively since the PCF is in VPLMN and the UDM is in HPLMN for roaming with LBO case.

For NRF-based discovery of PCF and UDM, the query criteria includes VPLMN for PCF discovery and HPLMN for UDM discovery. The AMF sends the UDM group ID to enable the SMF to select UDM. The S-NSSAI used by SMF to select PCF should be the VPLMN S-NSSAI received from AMF.

Lawful Interception

During roaming scenario, the SMF uses S-NSSAI of the VPLMN to generate IRI events. The S-NSSAI information is sent to the mediation device through the IRI event message.

Home Routed Roaming Support

Feature Description

The VPLMN provides access network services and packet routing to the packet core, whereas the HPLMN provides data network access to the subscriber. This feature enables the SMF to support the flavour of routing that is termed as the Home Routed (HR) roaming.

This feature provides the following functionalities:

- Support home routed roaming traffic for 5G sessions connected through NR.
- Support QoS flow Based Charging (QBC) on the UPF.

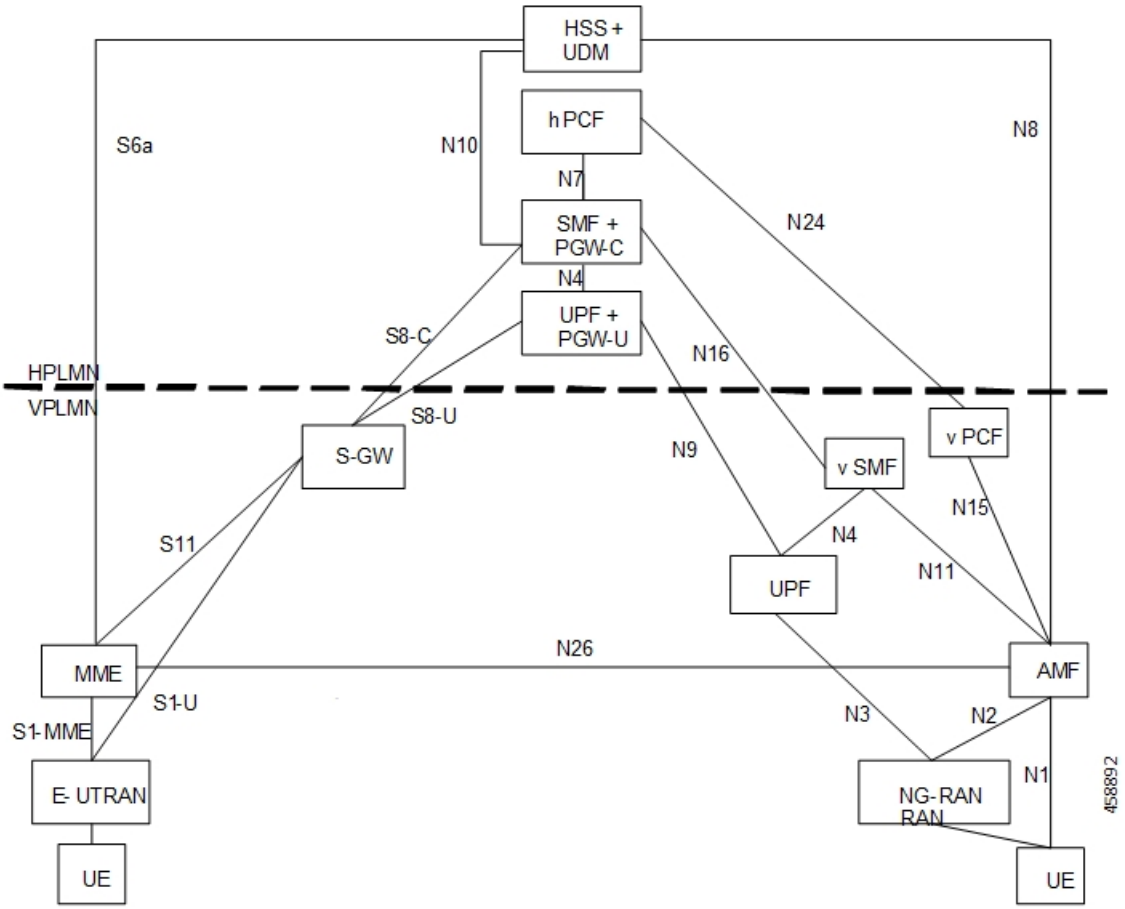
Architecture

This section describes the architecture for the HR roaming support feature.

EPC HR Roaming Scenario

The following diagram shows the architecture for an EPC HR roaming scenario.

Figure 236: EPC HR Roaming Architecture



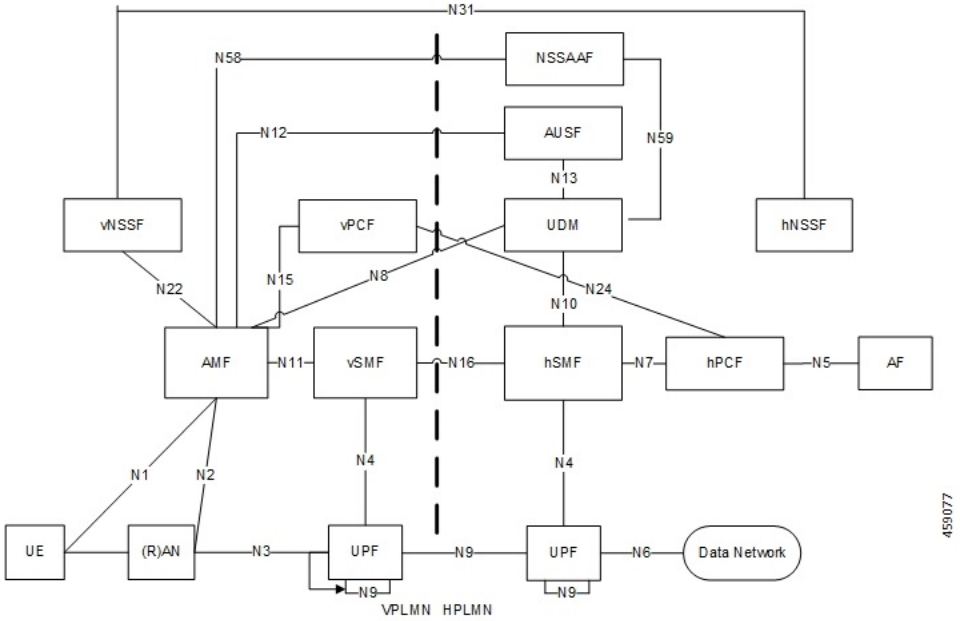
The 3GPP reference point for nodes in the VPLMN and HPLMN in an EPC HR roaming scenario, are as follows:

- SMF+IWK resides in the HPLMN.
- SMF-IWK interacts with the hPCF, hCHF and UDM.
- SMF-IWK supports S8-C with the S-GW (in VPLMN).
- vSMF interacts with the vCHF.

5G NR HR Roaming Scenario

The following diagram shows the architecture for a 5G NR HR roaming scenario.

Figure 237: 5G NR HR Roaming Architecture



The 3GPP reference point for nodes in the VPLMN and HPLMN in a 5G NR HR roaming scenario, are as follows:

- SMF resides in both the VPLMN and HPLMN.
- vSMF and hSMF support the N16 interface.
- hSMF interacts with UDM, h-PCF and h-CHF.
- vSMF interacts with the vCHF.
- When SEPP appears in the network, vSMF communicates to cSEPP for hSMF messaging.
- When SCP appears in the home network, hSMF communicates to SCP for UDM, hPCF and hCHF messaging.

vSMF

The SMF supports the following functionalities related to HR roaming for visitors:

- N1
  - The NAS SM information is of two parts, one is visible to vSMF (for example, PDU session type, Session AMBR, UE address). The other one that is not visible to vSMF (for example, SSC Mode, PCO, QoS rules, and so on), which it transparently relays to the hSMF.
  - The vSMF transfers the NAS signalling messages information, which is not visible to the vSMF, in a container toward the hSMF.
  - The vSMF transfers the NAS signalling messages information, which it does not comprehends, these are unknown IEs or IEs with an unknown value not set to "reserved" according to the release to which the vSMF complies, in a different container toward the hSMF.

- The vSMF appends unknown NAS signalling messages information received in the N16 container at the end of the NAS signalling message it sends to the UE.

- N40
  - Assignment and transfer of Charging ID of VPLMN to the hSMF.
  - Negotiation of roaming charging profile.
  - When NRF is used, the vCHF is selected based on the UE identified as an in-bound roamer and the PLMN id of the HPLMN.

- N4
  - V-CN-Tunnel lifecycle management.

- N16
  - Support for the N16 interface (between vSMF and hSMF).
  - Support for Always-on PDU Session Granted indication.

- EPS interworking procedures for home routed roaming, are as follows:
  - Caching of EPS bearer IDs and mapped QoS parameters received in hSMF. AMF retrieves the PDN contexts from the vSMF during the 5G to 4G handover. Also, the vSMF supports the release PDN context and not the forward to hSMF context.
  - During the 4G to 5G handover.
  - Support for indirect data forwarding tunnels.

- Does not interact with PCF or UDM.

hSMF

The SMF supports the following functionalities related to HR roaming for roamers:

- N1
  - The entire NAS SM information must be interpreted by the hSMF.
  - The hSMF transfers NAS SM information which the vSMF does not need to interpret in one container toward the vSMF.

- N10
  - Registers with UDM with the S-NSSAI value defined in the HPLMN.

- N4
  - User-plane inactivity detection is not performed during roaming (does not provide inactivity timer to hUPF).
  - H-CN-tunnel lifecycle management.

- N40

- Negotiation of “roaming charging profile.
- Generate a "home provided charging identifier"
- When the NRF is used, the hCHF is selected based on a UE identified as an out-bound roamer and the PLMN ID of the VPLMN.

- N7
  - N7 interaction for the hSMF is similar to the non-roaming case.
- N16
  - Support for the N16 interface (between vSMF and hSMF).
- If the UE uses IPv6, IPv4v6, it generates router advertisements Secondary authorization or authentication.

Network Slicing

The SMF supports the following functionalities related to network slicing:

- The SMF can be configured with a list of allowed NSSAI.
- When the SMF acts as a vSMF during roaming, the S-NSSAI sent by the UE used in the VPLMN must be the value that is configured on the SMF.
- In HR, the vSMF sends the PDU Session Establishment Request message to the hSMF along with NSSAI valued used in HPLMN.

Node Selection Considerations

The following criteria are applied for selecting the nodes in the HR roaming:

- When roaming is enabled, each SMF registers the interPlmnFqdn value with the NRF. This helps the AMF to select the hSMF in a different PLMN.
- The SMF supports **target-plmn-list** and **requester-plmn-list** query parameters.
- The NRF in the serving PLMN handles all the discovery requests from the NFs.

Lawful Intercept

The SMF provides the IRI-POI functions in the following network topology cases:

- Non-roaming case.
- Roaming case, in VPLMN.
- Roaming case, in HPLMN.

The SMF generates the following IRI events during the roaming scenarios:

- PDU session establishment
- PDU session modification
- PDU session release

- Start of interception with an established PDU session

Session Management

With roaming considerations, the SMF sessions are categorized into the following flavors:

- Non-roaming
- LBO
- vSMF-HO
- hSMF-HO

How it Works

This section provides details about the session create, release, modify procedures, and the different call handover scenarios for both vSMF and hSMF.

vSMF Create Session Procedure

This section provides details about the create session procedure for vSMF.

Figure 238: vSMF Create Session Call Flow

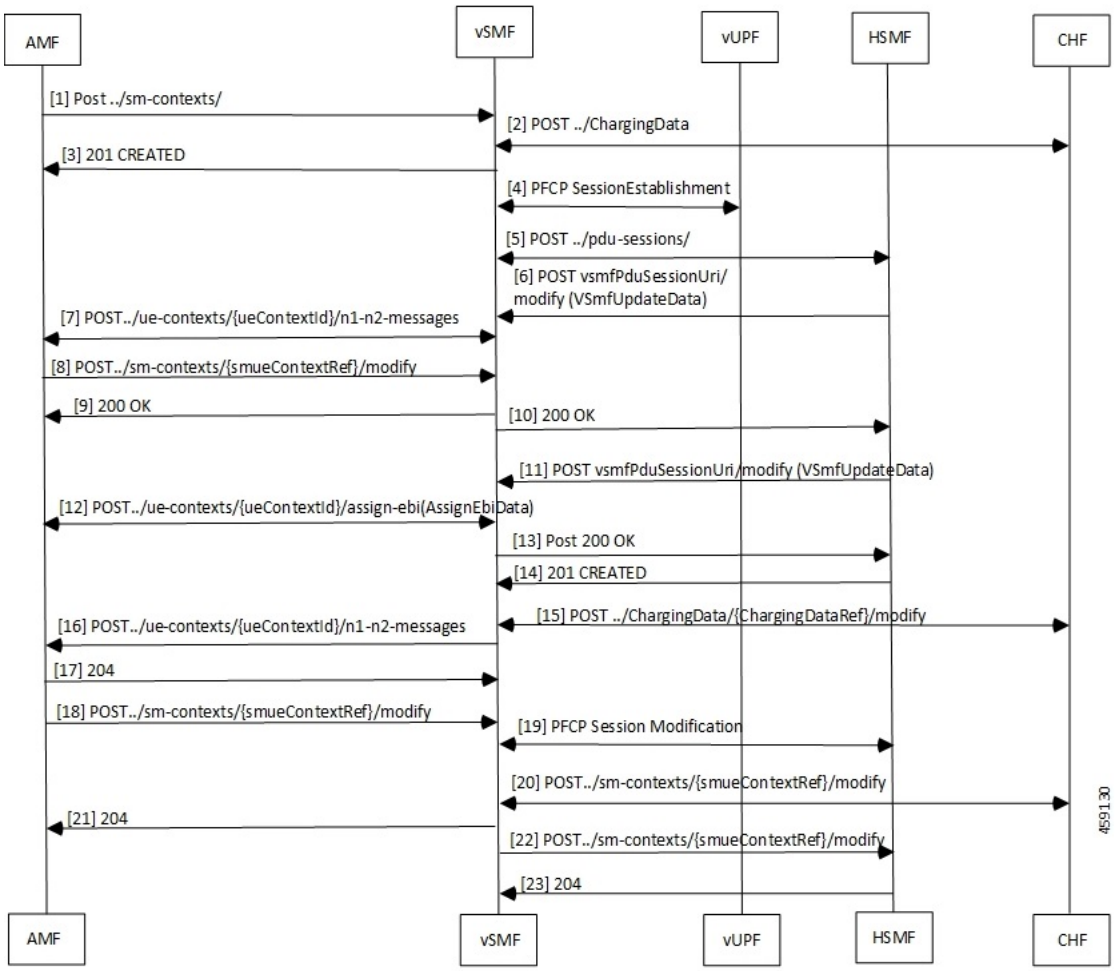


Table 411: vSMF Create Session Call Flow Description

Step	Description
1	The AMF receives a request from a UE. Based on the local configuration, the AMF locates a vSMF and a list of possible hSMFs to handle the UE request. It creates a **CreateSmContext** request, and POSTs the message to the vSMF. In the vSMF, based on the presence of an hSMF URI that is not its own, and the SUPI policy configuration of , the vSMF creates a PDU Context for valid UE requests.
2	The vSMF locates and creates a charging association with the appropriate CHF.
3	The vSMF responds to the AMF request with a reference to the created PDU Session.
4	The vSMF sends a PFCP Session Creation request to the vUPF. The vUPF responds with the CN tunnel Information of the created tunnel.

Step	Description
5	The vSMF creates a PDU Session Create Request to send to the hSMF. The CN tunnel information of the vUPF is an IE that is sent to the hSMF. Most of the request parameters from the AMF are copied on to the request to the hSMF. The following parameters from the N1 Message are removed from the request before it's sent to the hSMF: • **Always-On Indication** - If the UE requested an Always-On PDU session, and by policy the vSMF is ready to provide this service, this indication is set in the PDU Session Create request. • Any IE that is not identified by the vSMF is stripped off from the message and sent in a different payload to the hSMF. The UE request from the vSMF to the hSMF is sent asynchronously. This method enables the hSMF to start the EBI assignment procedures through the vSMF when it's processing the create request from the VSMF.
6	If a secondary authentication is required, the hSMF uses the callback URI for the vSMF session and the modify method to send an authentication request payload for the UE.
7	The vSMF sends this message to the AMF, and the AMF responds to the vSMF.
8	The UE responds to the authentication request, which is conveyed by the AMF to the vSMF.
9	The vSMF sends the update to the hSMF.
10	The vSMF responds to the AMF for the Modify Request.
11	If this session can be moved to EPC, the hSMF starts the EBI allocation procedure by invoking the modify method on the vSMF callback URI.
12	The vSMF invokes the assign-ebi method on the AMF, and the AMF sends back the assigned EPS bearer ID to the vSMF.
13	The vSMF responds to the hSMF.
14	If the request is acceptable to the hSMF, it responds with a 201 Created response which includes the subscription information required for the setup of the PDU session in the GNB. The response also contains an N1 payload.
15	The SMF updates the CHF with the parameters from the response from hSMF, including the charging profile setup by the hSMF.
16	The vSMF creates an N1N2MessageTransferRequest to the AMF. • The N2 payload is created by the using the parameters that are sent in the PDU Session Created Data, and the CN tunnel information from the vUPF. • The N1 payload is created by using the binary payload from the hSMF. The always-on indicator is set based on the value that is received in the PDU Session Created Data.
17	The AMF responds to the N1N2MessageTranfer Request.
18	The GNB responds with an N2 response to the ERAB RESOURCE SETUP REQUEST to the AMF, which the AMF sends in an SmContext Update message to the vSMF.

Step	Description
19	The vSMF requests the vUPF to update the tunnel information of the GNB, the tunnel and other information sent by the hSMF in step 6. The vUPF responds to the vSMF.
20	If required, the vSMF updates the CHF with any additional information.
21	The vSMF responds to the Update request from the AMF.
22	If there are any flows that have failed to setup, the vSMF notifies the hSMF accordingly.
23	The hSMF responds to the vSMF.

hSMF Create Session Procedure

This section provides details about the create session procedure for hSMF.

Figure 239: hSMF Create Session Call Flow

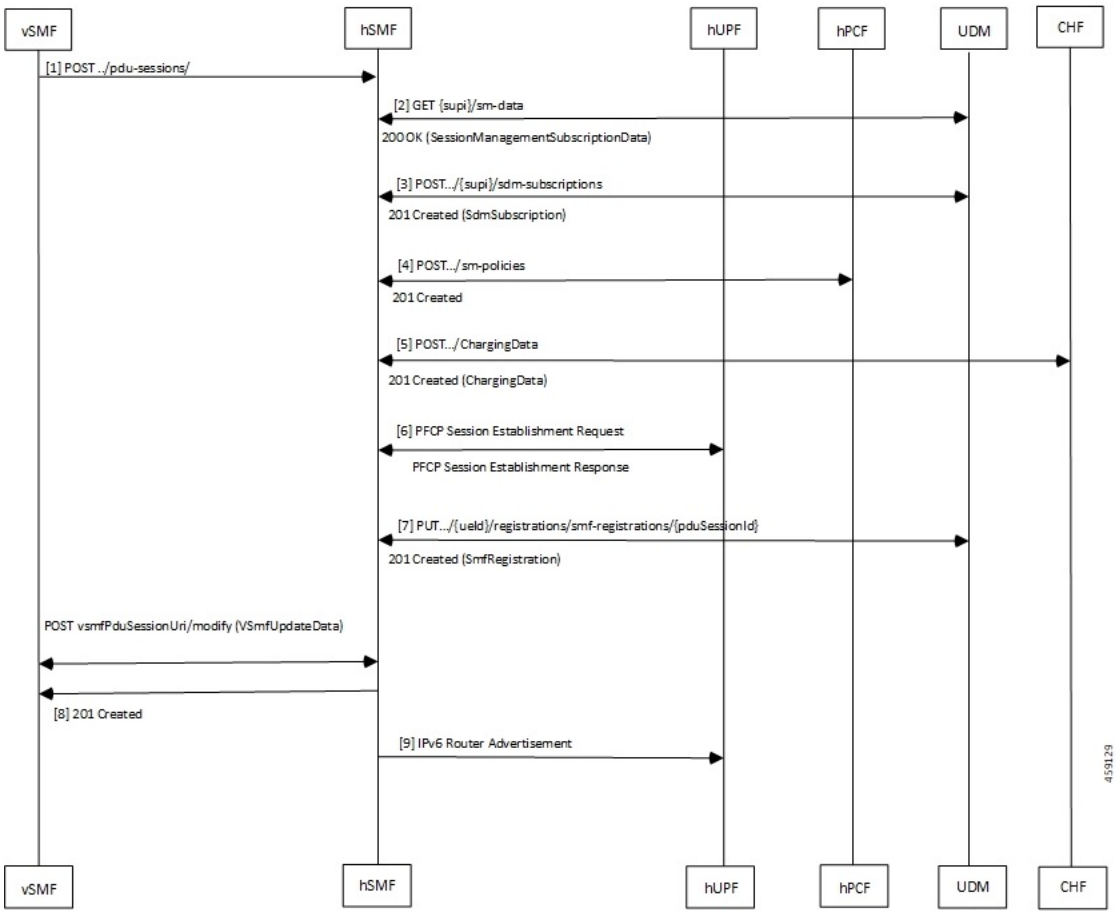


Table 412: hSMF Create Session Call Flow Description

Step	Description
1	The hSMF receives a request to create a PDU Session from the vSMF. The request has a JSON part and also a binary part, which has the list of IEs that the vSMF did not process, or could not process.
2	The hSMF retrieves the subscription data for the UE from the UDM.
3	If based on the subscription data, the session can be established, then the SMF subscribes to changes for the subscription data to the UDM.
4	The hSMF creates a policy association with the PCF. The PCF can either be one that has been selected by the AMF and signaled to the hSMF, or an NRF based or policy based selection on the hSMF.
5	A Charging Data association is created with the CHF.
6	Using the CN tunnel information provided by the vSMF in step 1, the hSMF creates CN tunnels on the hUPF. The hUPF responds with the CN tunnel information on the hUPF.
7	The hSMF registers with the UDM for any notifications for the UE in this DNN.
8	The hSMF responds to the request from the vSMF, with the CN tunnel information of the hUPF, and N1 information elements that need to be sent to the UE. If the UE has requested always-on session, and this is acceptable to the hSMF, then it's indicated to the vSMF in the response.
9	If IPV6 router advertisements are required to be transmitted, then the hSMF requests the UPF to perform that task.

vSMF Modify Session Procedure

This section provides details about the modify session procedure for vSMF.

Figure 240: vSMF Modify Session Call Flow

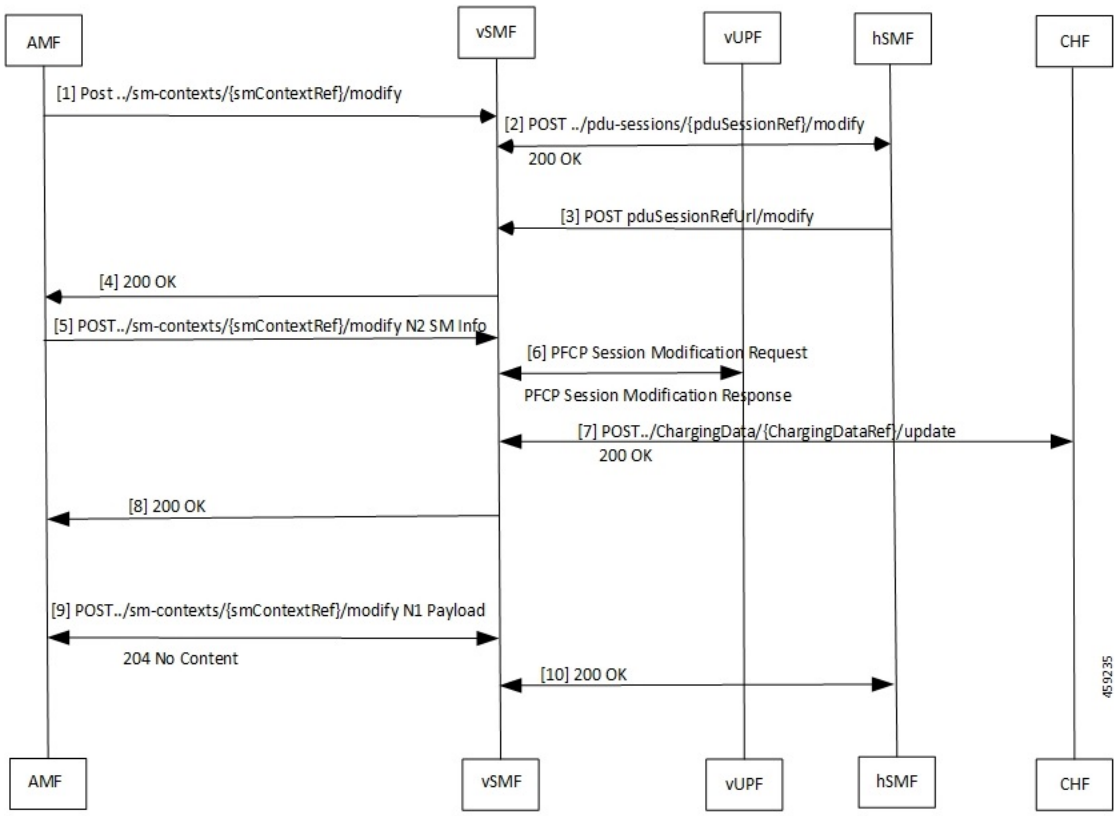


Table 413: vSMF Modify Session Call Flow Description

Step	Description
1	The AMF sends the request from the UE as an Sm Context Update message to the vSMF.
2	The vSMF uses the reference that the hSMF returned during creation of the message. It posts the relevant parts of the message to the hSMF. The hSMF responds to the message.
3	The hSMF sends an update request to the vSMF. This message contains the N1 and N2 messages that is sent to the gNB or UE as a part of the request message.
4	The vSMF combines the information from the hSMF and creates the N1 and N2 payloads for the UE and gNB. It then adds these to the response for the original request from the AMF.
5	The AMF relays the N2 response to the gNB.
6	If there are changes to the UPF due to the modification requested by the UE and accepted by the network, for example, addition or deletion of flows, the vSMF updates the UPF with these changes.
7	The vSMF notifies the CHF of any charging triggers for the changes applied to the UPF.
8	The vSMF acknowledges the N2 message from the AMF with a 200 OK message.

Step	Description
9	The AMF transfers the N1 payload from the UE and the vSMF acknowledges it.
10	The vSMF responds to the request from the hSMF for session modification.

hSMF Modify Session Procedure

This section provides details about the modify session procedure for hSMF.

Figure 241: hSMF Modify Session Call Flow

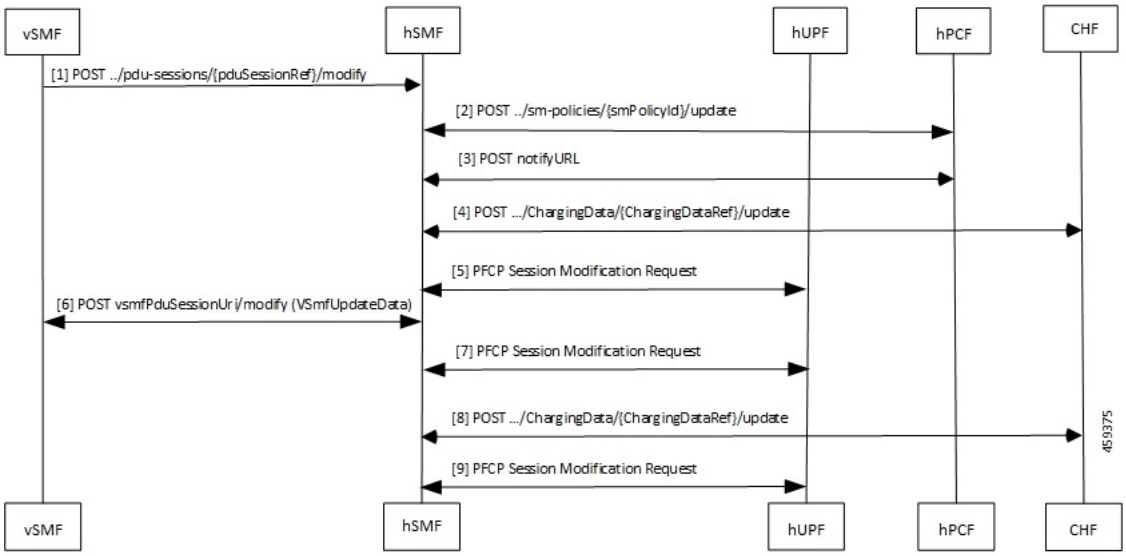


Table 414: hSMF Modify Session Call Flow Description

Step	Description
1	The UE request reaches the hSMF from the vSMF.
2	If any hPCF trigger criteria is met, the hSMF sends an update request to the hPCF.
3	The hSMF responds to the UE request and handles any exceptions.
4	The vSMF notifies the CHF of any charging triggers for the changes applied to the UPF.
5	If there are changes to the UPF due to the modification requested by the UE and accepted by the network, for example, addition or deletion of flows, the vSMF updates the UPF with these changes.
6	The UE request to update the PDU session reaches the hSMF from the vSMF..
7	If there are changes to the UPF due to the modification requested by the UE and accepted by the network, for example, addition or deletion of flows, the vSMF updates the UPF with these changes.
8	The vSMF notifies and updates the CHF of any charging triggers for the changes applied to the UPF.

Step	Description
9	If there are changes to the UPF due to the modification requested by the UE and accepted by the network, for example, addition or deletion of flows, the vSMF updates the UPF with these changes.

vSMF Release Session Procedure

This section provides details about the release session procedure for vSMF.

Figure 242: vSMF Release Session Call Flow

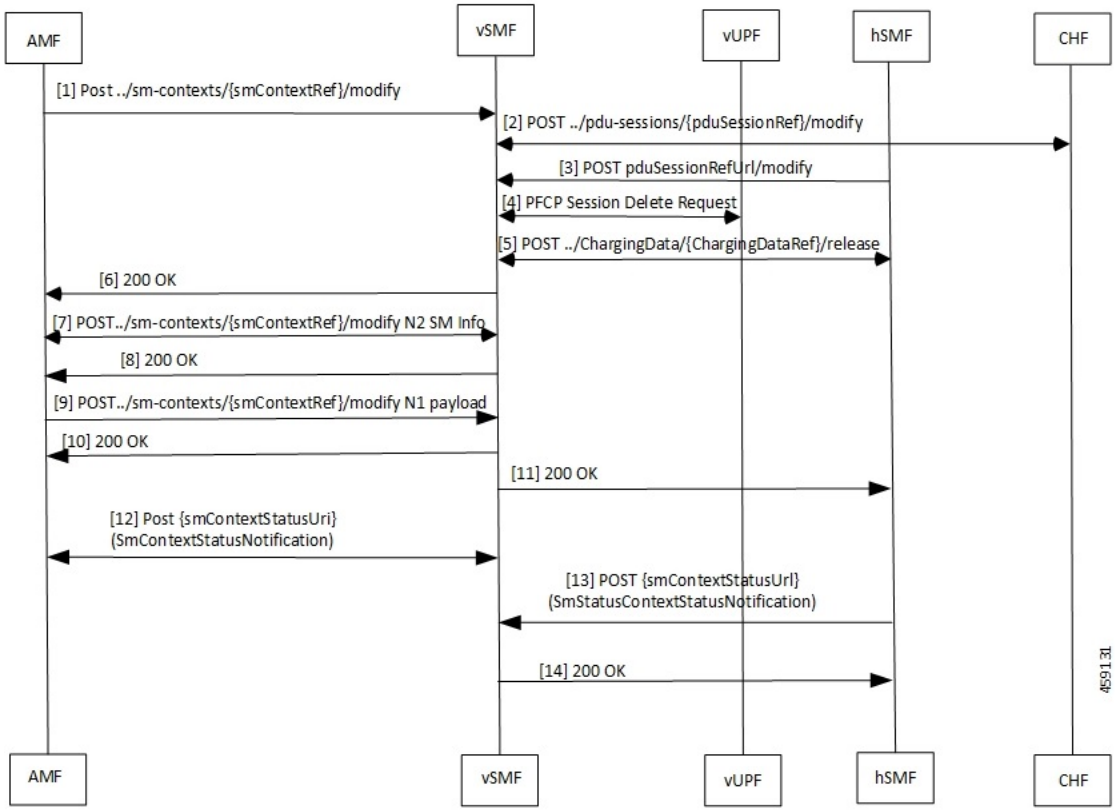


Table 415: vSMF Release Session Call Flow Description

Step	Description
1	The UE will initiate a release of the PDU session.
2	The vSMF receives the release request response from the hSMF.
3	The hSMF responds with a request to release the request in the form of a modify request with release indication set to true.
4	The vSMF releases the PFCP session.
5	The vSMF releases the charging session.

Step	Description
6	The vSMF responds to the AMF with a 200 OK response message.
7	The AMF responds with an N2 modification request.
8	The vSMF responds to the request with a 200 OK response message.
9	The AMF sends an N1 modification request to the vSMF.
10	The vSMF responds with a 200 OK message.
11	The vSMF responds to the hSMF PDU session modification request.
12	The vSMF forwards this notification to the AMF.
13	The hSMF sends an Sm context status notification that the release is complete.
14	The vSMF acknowledges the receipt of the notification.

hSMF Release Session Procedure

This section provides details about the release session procedure for hSMF.

Figure 243: hSMF Release Session Call Flow

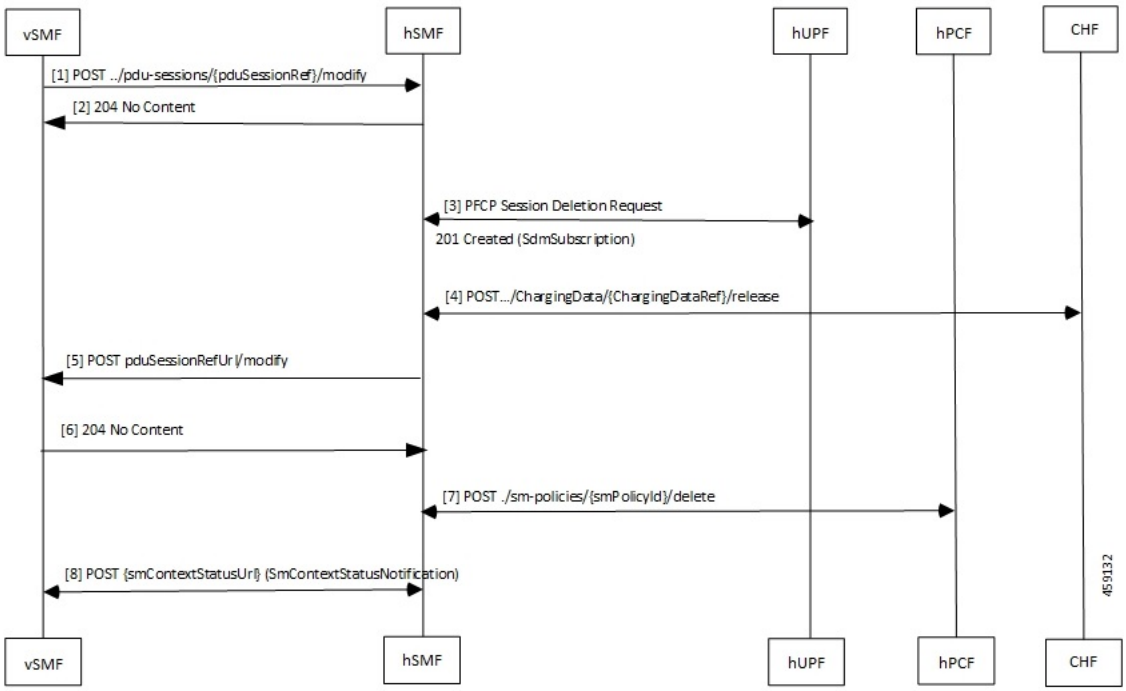


Table 416: hSMF Release Session Call Flow Description

Step	Description
1	The vSMF forwards the release request to the hSMF.

Step	Description
2	The hSMF responds with a 204 No Content message.
3	The hSMF releases the PFCP session.
4	The hSMF releases the charging session.
5	The hSMF sends a request to vSMF to release the request in the form of a modify request with release indication set to true.
6	The vSMF responds with a 204 No Content message.
7	The hSMF releases the associated Sm policies.
8	The hSMF forwards this notification to the vSMF.

vSMF Clear Subscriber Release Session Procedure

This section provides details about the release session procedure for vSMF by using an Ops Center.

Figure 244: vSMF Clear Subscriber Release Session Call Flow

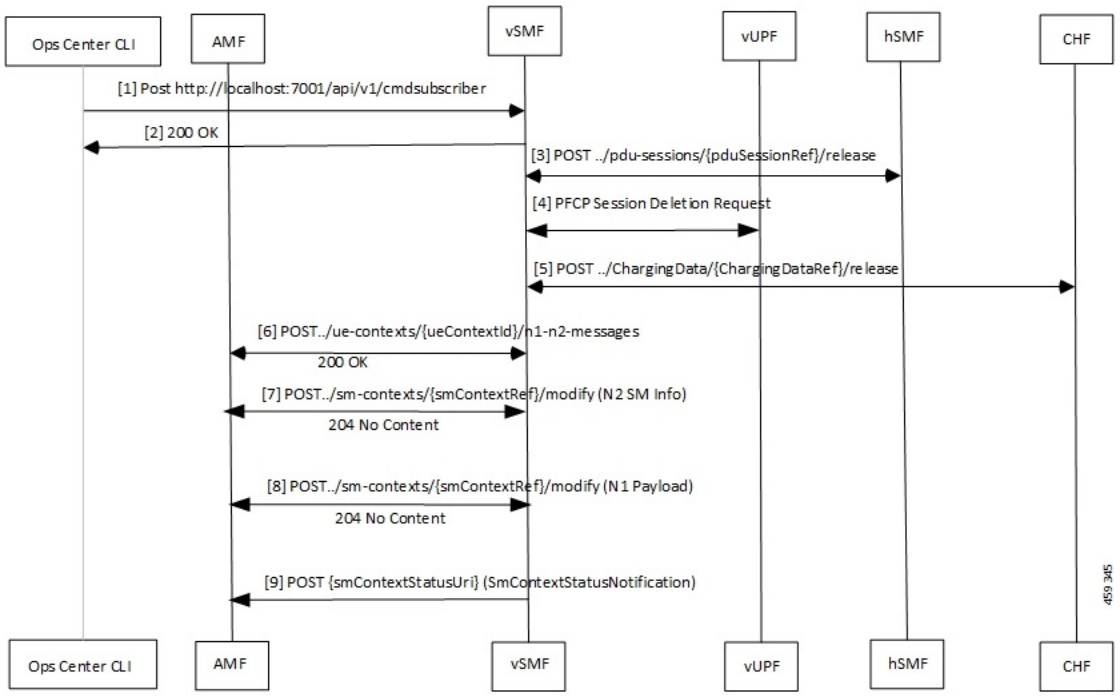


Table 417: vSMF Clear Subscriber Release Session Call Flow Description

Step	Description
1	The Ops Center or the vUPF issues a clear subscriber release request.
2	The vSMF acknowledges the receipt of the message.

Step	Description
3	The vSMF receives a release request response from the hSMF.
4	The vSMF releases the PFCP session for the vUPF.
5	The vSMF releases the charging session and updates the CHF.
6	The AMF receives an N1/N2 transfer request.
7	The vSMF receives information regarding the N2 status and acknowledges with a 204 No Content message.
8	The vSMF receives an N1 release complete notification from the AMF and responds with a 204 No Content message.
9	The vSMF updates the AMF with an Sm Context Status Notification message, which indicates that the session is released.

EPS to 5G Handover Using N26 Interface

This section describes the call flow for the EPS to 5G handover procedure using the N26 interface.

Figure 245: Call Flow for the EPS to 5G Handover Using the N26 Interface

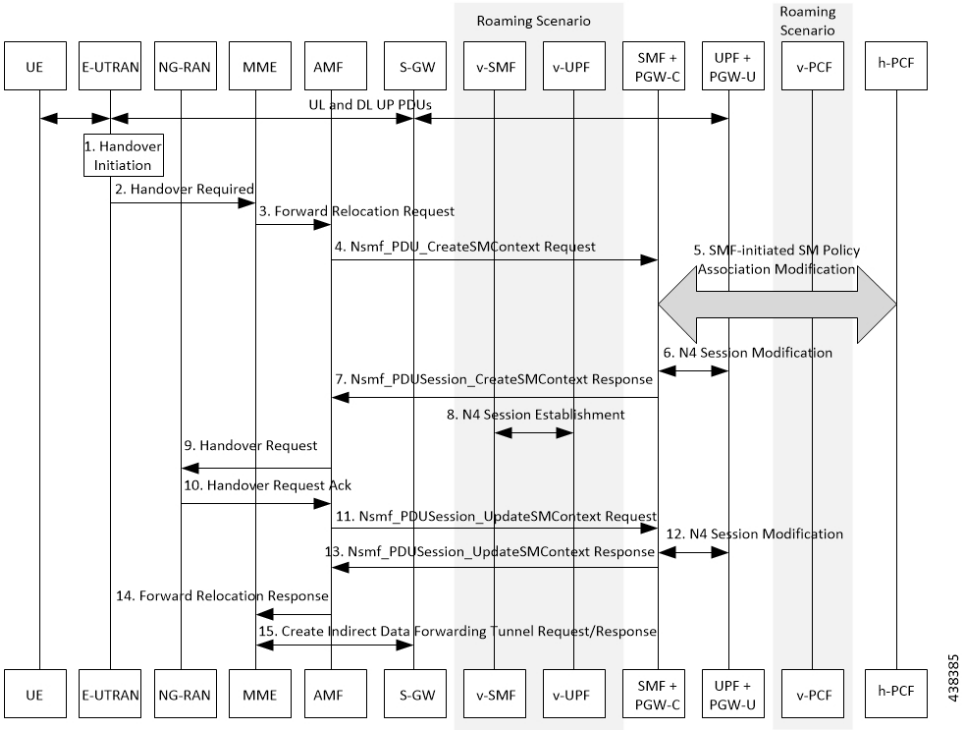


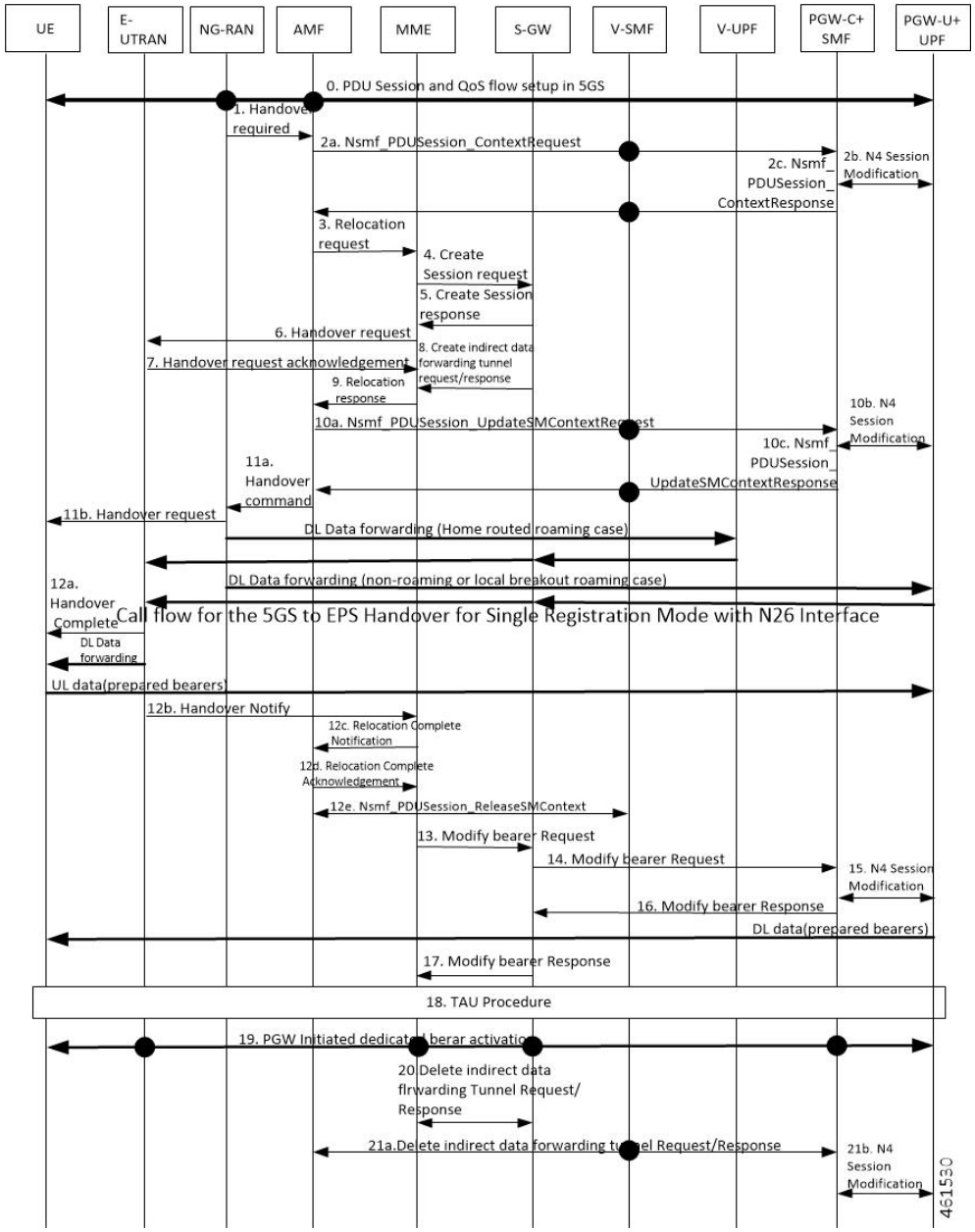
Table 418: Call Flow Description for the EPS to 5G Handover Using the N26 Interface

Step	Description
1	Call handover initiation starts from UE and E-UTRAN toward each other, proceeds from E-UTRAN to the S-GW. Then for roaming calls, call handover initiation proceeds from S-GW to the UPF+P-GW-U.
2	The E-UTRAN sends the Handover Call Request to the MME.
3	The MME forwards the Relocation Request to the AMF.
4	The AMF invokes the NsmfPDUSessionCreateSMContext service operation on SMF. The PGW-C+SMF address identifies this service operation. The service operations can be UE EPS PDN Connection, AMF ID, or Direct Forwarding Flag. The AMF then indicates the handover preparation to avoid switching the UP path. The SMF searches for the corresponding PDU session that is based on EPS Bearer Contexts. The AMF includes Direct Forwarding Flag to inform the SMF of the applicability of indirect data forwarding.
5	If you have deployed the dynamic PCC, the SMF+PGW-C initiates the SMF-initiated SM Policy Modification toward the PCF.
6	The PGW-C+SMF sends the N4 Session Modification to PGW-U+UPF to establish the CN tunnel for a PDU Session. The PGW-U+UPF receives the uplink packets from NG-RAN. This step involves creating uplink PDRs and FARs for the 5G session along with the QFIs that are mapped from the existing 4G bearers.
7	The PGW-C+SMF sends a NsmfPDUSessionCreateSMContext Response to the AMF. This response includes PDU Session ID, S-NSSAI, and N2 SM Information. The N2 SM Information includes PDU Session ID, S-NSSAI, QFIs, QoS Profiles, EPS Bearer Setup List, mapping between EBIs and QFIs, CN Tunnel information, and cause code details. The SMF includes mapping between EBIs and QFIs as the N2 SM Information container. If the P-GW-C+SMF determines that session continuity from EPS to 5GS is not supported for the PDU session, then the P-GW-C+SMF does not provide the Session Manager information for the corresponding PDU session. However, the P-GW-C+SMF includes the cause code details for rejecting the PDU session transfer in the N2 SM information.
8	The V-SMF and V-UPF establish an N4 session with each other.
9	The AMF sends the Handover Request to NG-RAN.
10	The NG-RAN sends an acknowledgment for the received Handover Request to the AMF.
11	The AMF sends a NsmfPDUSessionUpdateSMContext Request, T-RAN SM N3 forwarding information list message to the SMF for updating the N3 tunnel information. The NsmfPDUSessionUpdateSMContext request includes a PDU Session ID, S-NSSAI, and N2 SM Information. The tunnel information exists in the NGAP IE DL Forwarding UP TNL Information of the Handoff Request Acknowledgment that is received from NG-RAN.
12	The SMF+PGW-C performs the N4 session modification toward UPF+PGW-U to create the indirect tunnel to forward the DL data from eNodeB to NG-RAN. This step includes creating UL PDRs for the redirected DL data and associating FARs with them to forward the FARs to NG-RAN. The mapping of these PDRs and FARs is based on QFI and the corresponding bearer ID.

Step	Description
13	The PGW-C+SMF sends the NsmfPDUSessionUpdateSMContext Response to the AMF. This response includes PDU Session ID, EPS Bearer Setup List, and CN tunnel information for data forwarding. At this point, the indirect tunnels are established for DL data forwarding.
14	The AMF sends the Forward Relocation Response to the MME.
15	The MME sends the creation request for the indirect data forwarding tunnel to the S-GW. The S-GW sends the response for the indirect data forwarding tunnel to the MME.

5GS to EPS Handover for Single Registration Mode with N26 Interface

Figure 246: Call flow for the 5GS to EPS Handover for Single Registration Mode with N26 Interface



Call flow for the 5GS to EPS Handover for Single Registration Mode with N26 Interface

Important The IP address preservation cannot be supported if PGW-C+SMF in the HPLMN doesn't provide the mapped QoS parameters.

Table 419: Call Flow Description for the 5GS to EPS Handover for Single Registration Mode with N26 Interface

Step	Description
1	The NG-RAN sends a Handover Required (Target eNB ID, Source to Target Transparent Container, inter-system handover indication) message to the AMF.
2a	AMF sends Nsmf_PDUSession_ContextRequest requests the V-SMF to provide SM Context that also includes the mapped EPS Bearer Contexts. **Note** The AMF knows the MME capability to support non-IP PDN type or not through local configuration. **Note** In a home routed roaming scenario, the UE's SM EPS Contexts is obtained from the V-SMF.
2b	The PGW-C+SMF send N4 Session modification to PGW-U+UPF to establish the CN tunnel for each EPS bearer and provide EPS Bearer Contexts to AMF.
2c	PGC+SMF sends Nsmf_PDUSession_ContextResponse requests the V-SMF to provide SM Context that also includes the mapped EPS Bearer Contexts.
3	The AMF sends a Forward Relocation Request with modifications and clarifications.
4	MME sends Create_Session_Request to S-GW.
5	S-GW sends Create_Session_Response to MME.
6	MME sends Handover Request(may contain information Handover Restriction List with information about PLMN IDs) to E-UTRAN.
7	E-UTRAN sends Handover Request Acknowledgment to MME.
8	Creates indirect data forwarding tunnel request or response between MME and S-GW.
9	MME sends Relocation Response to AMF.
10a	AMF sends the Nsmf_PDUSession_UpdateSMContext Request (Serving GW Addresses and Serving GW DL TEIDs for data forwarding) to the PGW-C+SMF, for creating indirect data forwarding tunnel.
10b	N4 Session modification request is sent between PGW-C+SMF and PGW-U+UPF.
10c	The PGW-C+SMF returns an Nsmf_PDUSession_UpdateSMContext Response (Cause, CN tunnel Info for Data Forwarding, QoS flows for Data Forwarding) to AMF for creating indirect data forwarding. Based on the correlation between QFIs and Serving GW Addresses and TEIDs for data forwarding, the PGW-U+UPF maps the QoS flows into the data forwarding tunnels in EPC.
11a	The AMF sends the Handover Command to the source NG-RAN.
11b	The NG-RAN sends the Handover Command to the source UE.
12a	The UE sends the Handover Complete Command to the source UE NG-RAN.
12b	The E-UTRAN sends the Handover Notify to the source UE MME.
12C	The MME sends Relocation Complete Notification to AMF.

Step	Description
12d	The AMF acknowledges MME with Relocation Complete Acknowledge message. A timer in AMF is started to supervise when the resources in the NG-RAN and PGW-C+SMF are released.
13	MME sends Modify Bearer Request to S-GW.
14	S-GW sends Modify Bearer to PGW-C+SMF.
15	The PGW-C+SMF initiates a N4 Session Modification procedure in the direction of UPF+PGW-U to update the User Plane path downlink User Plane, for the indicated PDU Session is switched to E-UTRAN. The PGW-C+SMF releases the resource of the CN tunnel for PDU Session in UPF+PGW-U.
16	PGW-C+SMF sends Modify Bearer Response to S-GW.
17	S-GW sends Modify Bearer Response to MME.
18	The UE initiates a Tracking Area Update procedure(TAU).
19	The PGW-C+SMF initiates dedicated bearer activation procedure for non-GBR QoS Flows.
20	Indirect Data Forwarding Tunnel Request and Response deleted in MME and S-GW
21a	Indirect Data Forwarding Tunnel Request and Response deleted in AMF and PGW-C+SMF.
21b	N4 Session modification request is sent between PGW-C+SMF and PGW-U+UPF.

EPS to 5G Handover Without Using N26 Interface

This section describes the call flow for the EPS to 5G handover procedure without using the N26 interface.

Figure 247: Call Flow for the EPS to 5G Handover Without Using the N26 Interface

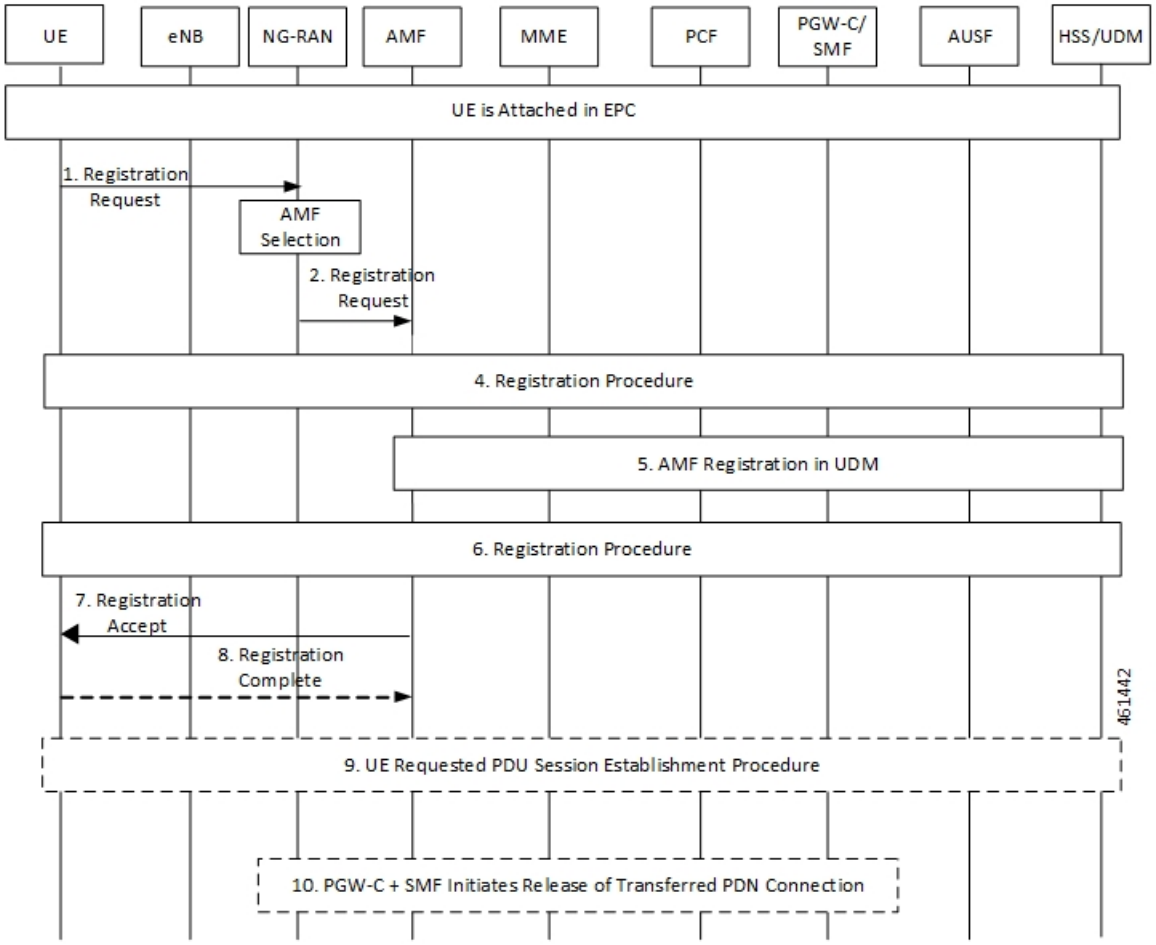


Table 420: Call Flow Description for the EPS to 5G Handover Without Using the N26 Interface

Step	Description
1	The UE initiates a registration request to the NG-RAN.
2	The NG-RAN selects an AMF.
3	The NG-RAN forwards the Registration Request with the N2 message parameters to the new AMF.
4	Refer to the General Registration procedure in TS 23.502.
5	The new AMF registers with the UDM using Nudm_UECM_Registration for the access to be registered.
6	Refer to the General Registration procedure in TS 23.502.

Step	Description
7	The new AMF sends the Registration Accept message to the UE. The AMF includes an "Interworking without N26" indicator to the UE.
8	The UE responds with a Registration Complete message to the new AMF.
9	The UE initiates a PDU Session establishment procedure.
10	The PGW-C+SMF performs release of the resources in EPC for the PDN connections(s) transferred to 5GS by performing the PDN GW initiated bearer deactivation procedure.

5G to EPS Handover Without Using N26 Interface

This section describes the call flow for the 5G to EPS handover procedure without using the N26 interface.

Figure 248: Call Flow for the 5G to EPS Handover Without Using N26 Interface

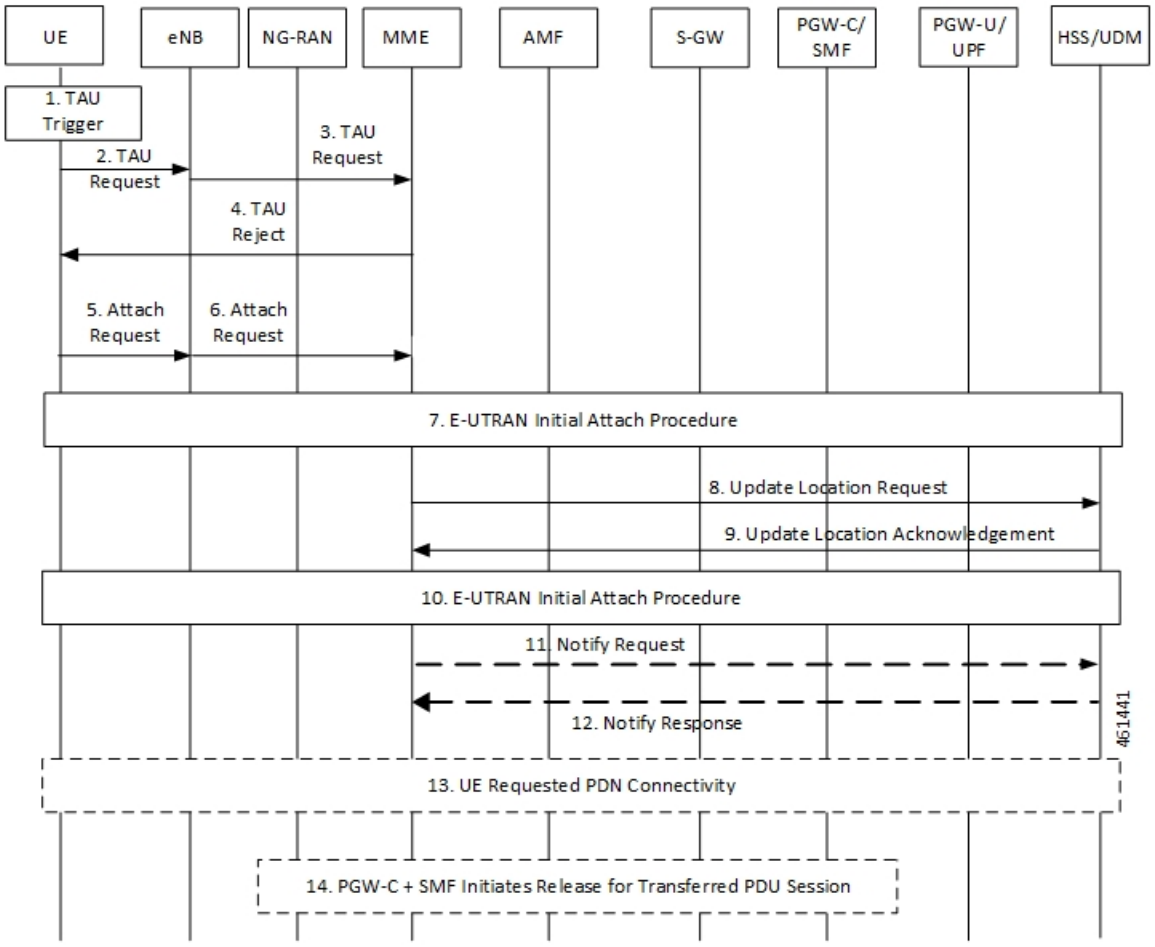


Table 421: Call Flow Description for the 5G to EPS Handover Without Using N26 Interface

Step	Description
1 - 2	The UE initiates the TAU procedure by sending, to the eNodeB, a TAU Request.
3	The eNodeB forwards the TAU Request message to the new MME.
4	If the MME determines that the old node is an AMF based on UE's GUTI mapped from 5G-GUTI and the MME is configured to support 5GS-EPS interworking without N26 procedure, the MME sends a TAU Reject to the UE.
5	The UE initiates an Attach Request to the eNodeB.
6	The eNodeB relays the Attach Request to the new MME.
7	Refer to the E-UTRAN Initial Attach procedure in TS 23.401.
8	If the MME has changed since the last detach, or if there is no valid subscription context for the UE in the MME, or if the UE provides an IMSI or the UE provides an old GUTI which doesn't refer to a valid context in the MME, or for some network sharing scenario if the PLMN-ID of the TAI supplied by the eNodeB is different from that of the GUTI in the UE's context, the MME sends an Update Location Request message to the HSS.
9	The HSS acknowledges the Update Location message by sending an Update Location Ack (IMSI, Subscription data) message to the new MME.
10	Refer to the E-UTRAN Initial Attach procedure in TS 23.401.
11	After the MME receives the Modify Bearer Response (EPS Bearer Identity) message, it sends a Notify Request including the APN and PDN GW identity to the HSS for mobility with non-3GPP accesses. The message includes information that identifies the PLMN in which the PDN GW is located.
12	In the case of non-emergency services, the HSS stores the APN and PDN GW identity pair. In the case of emergency services, the HSS stores the "PDN GW currently in use for emergency services". The HSS then sends a Notify Response to the MME.
13	If the UE has remaining PDU Sessions in 5GS, which it wants to transfer to EPS and maintain the same IP address/prefix, the UE performs the UE requested PDN Connectivity Procedure and sets the Request Type to "handover". UE provides an APN and the PDU Session ID corresponding to the PDU Session it wants to transfer to EPS.
14	The PGW-C+SMF initiates release of the PDU Session(s) in 5GS transferred to EPS.

Standards Compliance

The Home Routing roaming support feature complies with the following standards:

- *3GPP TS 23.501 v15.4.0*
- *3GPP TS 23.502 v15.4.0*
- *3GPP TS 23.503 v15.4.0*
- *3GPP TS 33.501 v15.4.0*
- *3GPP TS 33.128 v15.4.0*

- *3GPP TS 33.127 v15.4.0*
- *3GPP TS 32.240 v15.4.0*
- *3GPP TS 29.244 v15.4.0*
- *3GPP TS 32.291 v15.3.0*
- *3GPP TS 29.500, Version 16.8.0*
- *3GPP TS 29.502, Release 16*
- *3GPP TS 29.502 v15.7.0, April 2020*

Limitations

In this release, the Home Routing roaming support feature has the following limitations:

- No support for unknown NAS SM information (unknown IE).
- VPLMN-ID is not embedded within the Charging-ID.

Charging Support for HR Roaming

This section describes the charging support for the HR roaming feature.

This feature supports the following functionalities:

- QBC charging.
- Roaming QBC profiles configuration.
- Relay roaming QBC profiles to the CHF.
- Receive roaming QBC profiles from the CHF.
- Relay roaming QBC profiles from the vSMF to hSMF.
- hSMF relays roaming vSMF QBC profiles to hCHF.
- vSMF relays roaming hSMF QBC profiles to vCHF.
- In the vSMF, UPServ in collaboration with charging, creates PDRs for QFI on the N4 interface and associated corresponding URR, which are derived from the roaming QBC profile.
- Relay URR usage reports derived from the QBC profile to the respective CHF in QFi containers, which are meant for QosFlow reporting.
- Disable QBC for the sessions for which the corresponding QBC charging profiles could not be identified.
- Support Fail-Open from the CHF.
- Configuration to enable QBC on the hSMF, vSMF and non-roaming SMF.

Using the Roaming QBC Profile

The SMF determines the QBC profile based on the local interface. The QBC URR is created based on the limits present in the profile.

The following triggers are applicable for HR charging:

- Triggers armed at Session Level
  - Reports the QBC in the session level URR.
  - Reports the QBC for the CC events.
- Triggers armed at the QBC profile
  - Limits are used in QBC URRs.
  - Reports all the QBC URRs for an event armed at the QBC profile.

The following sample code shows the different triggers and their corresponding values.

```
Sess trigger []
Vol  100
time  100
RAT

Rg X trigger[]
Vol  10
time  10
PLMN

RoamignQbcprofile trigger[]
Vol    20
time  20
ULI


Sess URR
Vol 100
tim 100

RGX_URR
vol  10
tim 10

QBCURR1
Vol 20
tim 20

QBCURR2
Vol 20
tim 20



When RTA happens
Query all RG and all QBC urr

when PLMN change
Query RG X URR


when ULI changes
Query all QBC
```

Accounting Static or Predefined URR Usage to Session Level URR

In the previous release, the CHF driven session limits were controlled by the PCF, dynamic in nature and applicable for the online and offline charging service. As a result, all the dynamic URRs were reported when a session level URR was reported. Also, the offline URR associated with the static or predefined rules were reported when a separate URR was met.

In the current release, the reporting mechanism is streamlined on the N4 interface for the session limits to report the following URRs:

- The online and offline URRs associated with dynamic rules.
- The offline URR associated with static or predefined rules.
- All the QBC URRs.

NOTES:

- In this release, the SMF does not report the online static or predefined URRs when a session limit is met.
- In this release, rulebase ECGDR configuration is not required to get the static or predefined accumulated report for offline services.

  When QBC is enabled, the SMF associates SessLevelUrr to the default UL or DL PDR, which carries the rulebase name. The UPF associates this URR to every SDF PDR or URR for all the static predefined rules.
- During setup, the Sess Urr is associated with the default PDR. If the SMF does not have input during the setup time for creating the Sess level URR and later post setup, the CHF sets limits. These URRs are not honored.

MaxChangeinCC, MaxDeferredUrr and OOO Config

MaxChangeinCC

The HR roaming feature supports reporting of the QBC usage data when Max CC is met.

The MaxCC value can be controlled at the config level apart from it coming from the CHF. The priority order of selecting the MaxCC values, are as follows:

- The CHF armed MaxCC.
- The ChargingProfile when it's associated to a session.
- If a session is enabled for QBC charging, use QbcProfile .

MaxDeferredUrr

The local config is used to configure the MaxDeffered value present in Charging-Profile. This is extended to ChargingQbcProfile. The priority order of selecting, are as follows:

- The ChargingProfile when it's associated to a session.
- If a session is enabled for QBC charging, use QbcProfile .

The MaxDeferred count is met when the combined value of UUC and QFIContainer crosses the configured threshold value.

OOO Config

The OOO config is referred from Charg-Profile, which is associated to a session.

If it's not associated to a session, then it's referred from the QBC profile on the condition that the QBC charging is enabled for the session.

Configure Charging for HR Roaming

This section describes how to configure the charging for the HR roaming feature.

Configure the QBC Charging Profile

Use the following sample code to configure the QBC charging profile:

```
[unknown] smf(config)# profile charging-qbc test
[unknown] smf(charging-qbc-test)# ?
Possible completions:
  limits       List of threshold
  triggers       List of Triggers to be configured

[unknown] smf(charging-qbc-test)# limits ?
Possible completions:
  duration       Duration threshold for Charging, range [60..40000000]
  volume         Volume threshold for Charging, range [10000..4000000000]

[unknown] smf(charging-qbc-test)#  limit duration ?
Description: Duration threshold for Charging, range [60..40000000]
Possible completions:
  <unsignedInt, 60 .. 40000000>

[unknown] smf(charging-qbc-test)#  limit volume ?
Possible completions:
  downlink    in bytes, range [10000..4000000000]
  total       in bytes, range [10000..4000000000]
  uplink      in bytes, range [10000..4000000000]

[unknown] smf(charging-qbc-test)#  triggers ?
Description: List of Triggers
Possible completions:
  3gpp-ps-change
  ambr-change
  max-number-of-changes-in-charging-conditions
  plmn-change
  qos-change
  rat-change
  serv-node-change
  ue-pra-change
  ue-time-change
user-loc-change
```

Associate the QBC Charging Profile to Charging Characteristics

Use the following sample code to configure and associate the QBC charging profile to the Charging-Characteristics profile:

```
[unknown] smf(config)# profile charging-characteristics 16
[unknown] smf(config-charging-characteristics-16)# ?
Possible completions:
  charging-profile                 Charging Profile configuration
  network-element-profile-list     Network element profile list
  charging-qbc-profile    Associate said QBC ChargignProfile

[unknown] smf(config-charging-characteristics-16)#associate-qbc-charg-profile test
```

Associate the QBC Charging Profile to DNN Profile

Use the following sample code to configure and associate the QBC charging profile to the DNN-Profile:

```
unknown] smf(config)# profile dnn test
[unknown] smf(config-dnn-test)# ?
Possible completions:
  ---
  ---
  charging-profile                                        Charging Profile configuration

  charging-qbc-profile                                    QBC ChargignProfile
```

Configure the QoS Profile

The QoS profile is enhanced to configure per qi5 arp combination for the flow parameters, MFBR and GFBR.

Use the following sample code to configure the QoS profile:

```
[smf] smf(config-qos-abc)# qosflow?
Possible completions:
  qosflow   Configure Qosflow params for 5QI/Arp values
[smf] smf(config-qos-abc)# qosflow ?
Possible completions:
  qi5   Standard 5QI value (range 1 to 255)
[smf] smf(config-qos-abc)# qosflow qi5 ?
Possible completions:
  <qci-value:unsignedInt, 1 .. 255>  range
[smf] smf(config-qos-abc)# qosflow qi5 1 ?
Possible completions:
  arp-priority-level   Configures the ARP Priority Level [1-255]
  flow-parameter
  <cr>
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter ?
Possible completions:
  gfbr   Guaranted Bit Rate (GFBR)
  mfbr   Maximum Bit Rate (MFBR)
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter gfbr ?
Possible completions:
  dl   GFBR Downlink threshold
  ul   GFBR Uplink threshold
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter gfbr dl ?
Description: GFBR Downlink threshold
Possible completions:
  <string>
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter mfbr ?
Possible completions:
  dl   MFBR Downlink threshold
  ul   MFBR Uplink threshold
[smf] smf(config-qos-abc)# qosflow qi5 1 flow-parameter mfbr

[smf] smf(config-qos-abc)# qosflow qi5 1 arp-priority-level 1 flow-parameter ?
Possible completions:
  gfbr   Guaranted Bit Rate (GFBR)
  mfbr   Maximum Bit Rate (MFBR)
[smf] smf(config-qos-abc)# qosflow qi5 1 arp-priority-level 1 flow-parameter
```

Default DNN Support in HR Roaming

In the HR roaming scenario, the vSMF supports the use of default DNN to avoid listing or configuring all the DNNs used by the roaming partners.

The DNN validation is disabled for the visitor-hr calls received by the vSMF. From the default DNN profile, the virtual DNN configuration is used toward vCHF, vUPF, and RMGR for vUPF selection.

To configure the default DNN profile, use the following CLI configuration:

```
config
  policy dnn policy_name
    profile profile_name
  exit
exit
```

To configure the virtual DNN name, use the following CLI configuration:

```
config
  profile dnn profile_name
    dnn virtual_dnn_name network-function-list [ chf | rmgr | upf ]
  exit
exit
```

IPv6 RS/RA Support in HR Roaming

In this release, the Home Routed roaming feature supports the mechanism for vSMF to receive the IPv6 interface ID from the hSMF using the N16 interface as per *3GPP TS 29.502, Release 16, CR 202206*.

In the HR roaming scenario, the Router Solicitation (RA) and Router Advertisement (RA) is handled by the hUPF or hSMF, where the vUPF relays in both directions for RA to properly function. In CR 202206, the hSMF sends the IPv6 interface ID to the vSMF and then the vSMF relays the same to UE in the N1 payload.

For inter-operability, even if the vSMF does not receive the IPv6 interface ID from the hSMF on the N16 interface, it still relays based on the Virtual Mac configuration in the DNN profile to the UE.

SEPP Support

Feature Description

The Security Edge Protection Proxy (SEPP) is used to protect Control Plane traffic that is exchanged between different 5G PLMNs (Public Land Mobile Networks). The SEPP performs message filtering, policing and topology hiding for all API messages at the PLMN boundaries.

The SMF supports the Failure Handling template for SEPP to identify the source of failure through SEPP or Peer.

How it Works

The SEPP protects the communication pathways and performs topology hiding for every Control Plane message in an inter-PLMN signalling, acting both as a service relay between the actual service producer and the service consumer. For both the service producer and consumer, the result of the service relaying is equivalent to a direct service interaction.

For HR roaming, each SEPP communicates with the respective SMF in the VPLMN and HPLMN by using the N16 interface.

Note The SEPP is only used on inter-PLMN boundaries, and is not used between nodes in the home domain, for example, between the hSMF and the hUDM.

SEPP Selection

The SEPP is selected through local configuration. The current set of NF nodes are extended to allow for SEPP selection. Both the vSMF and hSMF use the same configuration to select SEPP.

Failure Handling for SEPP and hSMF/vSMF

The SMF supports failure handling (FH) for hSMF or vSMF and SEPP. The client SMF detects the originator of the failure response based on the 3GPP header message received in the HTTP response. The originator can be either peer SMF or SEPP.

Depending on the NF instance value in the header message, it selects either the SEPP FH profile or the N16 FH profile.

The N16 FH profile works similar to the existing N32 SEPP FH profile. But the N16 FH profile uses an AdditionalHsmfUri attribute instead of the Endpoint (EP) configuration available for other NFs.

Important AdditionalHsmfUri attribute is used only in the create session procedure.

When there is an error response from SMF, it includes the server header in the following format:

SMF-nf-instance-id

```
Example:
SMF-54804518-4191-46b3-955c-ac631f953ed8
 SEPP-35644518-9291-46b3-934c-ac5678f953ed
```

If the header has the SEPP NF instance value, the client SMF that receives the failure applies the SEPP failure handling configuration.

Note If the header has two SEPP server names, it deems the failure response as originated from the peer SMF.

Following is the sequence of failure handling steps taken during the PDU session creation procedure:

1. The vSMF selects the first SEPP based on the locally configured SEPP EPs and appends the “3gg-target-api-root” header with the hSMF URI.
2. If the first SEPP EP fails, vSMF selects the SEPP FHT and retries the procedure with another EP.
3. In the absence of SEPP FHT or exhaustion of retry count, the SMF terminates the session.
4. When the peer SMF fails, vSMF uses N16 FHT and selects the next EP from the AdditionalHsmfUri EPs.
5. If all the URIs defined in the AdditionalHsmfUri IE fail or the retry count exhaust, the vSMF terminates the procedure..

SEPP and SMF Failure Actions

During the PDU session lifecycle, the SMF checks for the hSMF and SEPP with the NF instance value. Depending on the HTTP status code configured in the FH profile, the SMF takes one of the following actions.

Table 422: Supported Actions in SEPP and SMF FHT

N16 Procedure	SEPP FHT Actions	SMF FHT Actions
Create	terminate retry-and-terminate	terminate retry-and-terminate
Release	terminate retry-and-terminate	terminate
HsmfPduSessionNotify	terminate retry-and-terminate	terminate

Note The SMF overwrites any other configured FH action with the default terminate action.

Call Flows

This section describes the call flow for selecting and using SEPP.

The following types of requests are sent from a client to a server:

- **Requests to API roots** - These requests are sent to the API root as defined in the YAML. The following headers are added to the request:
  - **3gpp-Sbi-Target-apiRoot** - The value of this header is the FQDN of the NF that services the request. For requests sent to the hSMF, this is the hSMF FQDN.
  - **Authority** - The value of this header is the server SEPP to which the request is sent to by the client. When the request is sent by the vSMF, the value is vSEPP, and when the request is sent by the hSMF, it's hSEPP.
- **Callback Requests** - These requests are callbacks that are invoked across PLMN boundaries. The values of the header field in such requests are defined in *3GPP TS 29.500, Annex B*.

Figure 249: Call Flow with SEPP

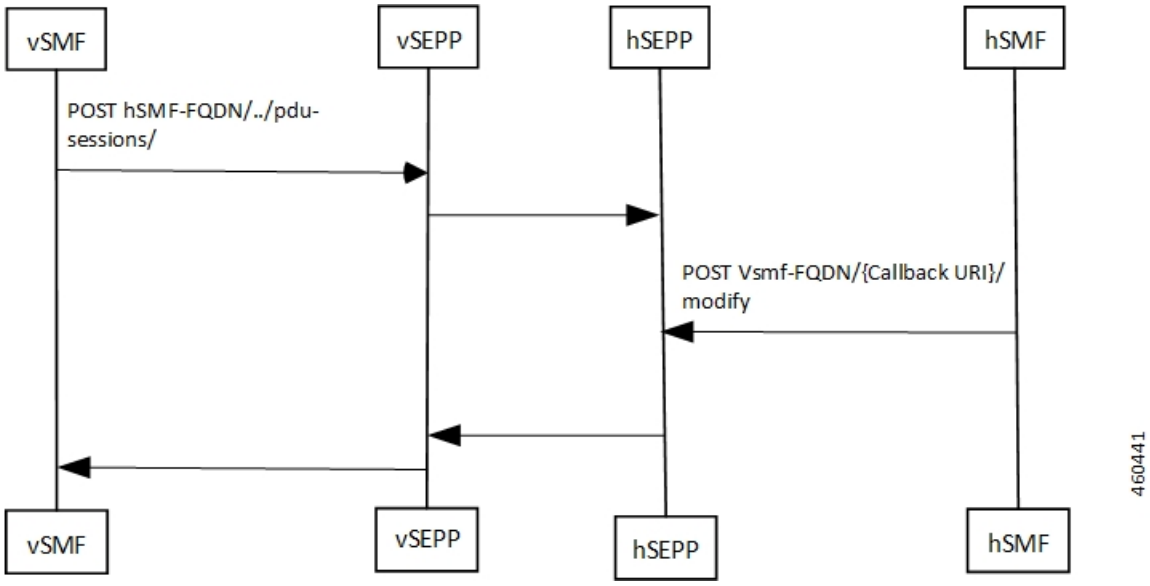


Table 423: Call Flow Description for Selecting a SEPP

Step	Description
1 - 2	The vSMF initiates the procedure by sending an indication to hSMF about using a SEPP and the address of the SEPP. The call flow sequence for this forward messaging is as follows: • The vSEPP and hSEPP encrypts and decrypts the messages sent from the vSMF to hSMF respectively. • The AMF sends the hSMF FQDN to smf-service, which in turn sends it to rest-ep in all the messages. • The vSMF selects the vSEPP by reading the locally configured IP address and port number for the vSEPP and uses it to send messages to hSMF. • The rest-ep updates the 3gpp-Sbi-Target-apiRoot headers with the hSMF URI and Authority header with the IP address and port number of the vSEPP and then, sends the messages to vSEPP, which is further communicated to the hSEPP. • The hSEPP resolves the DNS (if required), decrypts the message and transmits it to the hSMF.

Step	Description
3 - 4	The hSMF responds with a callback header value. The call flow sequence for this return messaging is as follows: • The hSEPP and vSEPP encrypts and decrypts the messages sent from the hSMF to vSMF respectively. • The smf-service gets the FQDN for the vSMF from the notification URI that is received as apart of message from the vSMF and updates the 3gpp-Sbi-Target-apiRoot headers. The smf-service updates the 3gpp-sbi-callback enum value in all the messages. • The smf-service forwards the message to the rest-ep. The rest-ep updates the 3gpp-sbi-callback and 3gpp-Sbi-Target-apiRoot header values. • The rest-ep updates the Authority (pseudo header) with the locally configured IP address and port number of the hSEPP and forwards the message to the hSEPP, which is further communicated to the vSEPP. • The vSEPP resolves the DNS (if required), decrypts the message and transmits it to the vSMF.

Configuring the SEPP

This section describes how to configure SEPP.

The following conditions are applicable when you configure SEPP:

- It's configured in the same way how you configure the other NFs, like, for example, UDM, CHF, or PCF.
- As it's an Edge proxy and not a proper NF, it must have service lists, which are supported by a peer SMF.
- It supports failure handling functionality using the existing nf-client failure templates, similar to the other NFs.

Configuring the SEPP nf-client

To configure a SEPP nf-client, use the sample CLI configuration only as a reference.

```
profile nf-client nf-type sepp
 sepp-profile SEPP1
  locality LOC1
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   50
     priority   50
     uri-scheme http
     endpoint-name sepp-ep-1
      priority 50
      capacity 50
      primary ip-address ipv4 xx.xx.xx.xx
      primary ip-address port xxxx
     exit
    exit
   exit
  exit
 exit
exit
```

Configuring the Network Element Profiles for a SEPP

To configure the network element profiles linked to a SEPP nf-client, use the sample CLI configuration.

```
profile network-element sepp nrf-nf-sepp-1
 nf-client-profile SEPP1
exit
```

Configuring the DNN Profile for a SEPP

To configure the DNN profile for a SEPP, use the sample CLI configuration only as a reference.

```
network-element-profile sepp nrf-nf-sepp-1 is linked to dnn

profile dnn intershatRoamer
 network-element-profiles sepp nrf-nf-sepp-1
exit
```

Configuring the Failure Handling for a SEPP

The SEPP supports the existing failure handling template for all the HTTP error response codes. To configure failure handling for a SEPP, use the sample configuration only as a reference.

```
profile nf-client-failure nf-type sepp
 profile failure-handling FH-SEPP
  service name type nsmf-pdusession
   message type VsmfPduSessionCreate
    status-code httpv2 504
     retry  2
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

Note In the current release, only the retry-terminate option is supported for all the messages.

Configuring the Failure Handling Template for hSMF/vSMF and SEPP

The peer SMF and SEPP support the failure handling template for all the HTTP error response codes. To configure failure handling for a peer SMF message, use the sample configuration only as a reference.

The following is a sample configuration for hSMF:

```
profile nf-client-failure nf-type sepp
 profile failure-handling FHSEPP
  service name type nsmf-pdusession
   responsetimeout 4000
   message type VsmfPduSessionUpdate
    status-code httpv2 500-599
     retry  3
     action retry-and-terminate
    exit
   exit
   message type VsmfPduSessionNotify
    status-code httpv2 400-599
     retry  3
     action retry-and-terminate
```

```
    exit
   exit
  exit
 exit
exit
```

The following is a sample configuration for vSMF:

```
profile nf-client-failure nf-type sepp
 profile failure-handling sepp
  service name type nsmf-pdusession
   responsetimeout 4000
   message type HsmfPduSessionCreate
    status-code httpv2 400-599
     retry  3
     action retry-and-terminate
    exit
   exit
   message type HsmfPduSessionUpdate
    status-code httpv2 500-599
     retry  3
     action retry-and-terminate
    exit
   exit
   message type HsmfPduSessionRelease
    status-code httpv2 504
     retry  3
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
```

Note The sample configurations use the nf-type SEPP. You can use the same for nf-type SMF.

Configuring the Failure Handling Template with Alternate hSMF

If there is failure from a primary hSMF, vSMF tries the alternate hSMF. SMF service sends the alternate hSMF details to Rest Endpoint (rest-ep) and SMF gets alternate HSM details from AMF. Based on the N26 failure handling configuration, an alternate hSMF is selected.

Alternate hSMF is selected only if retry is configured for.**pduSessionCreate**

Note smf-service includes list**alternate-hsmf** in the **discoveryParams** to Rest Endpoint.

Based on the N26 failure handling configuration, an alternate hSMF is selected.

Rest-ep or NfLib sends the selected alternate hSMF back to service and vSMF sends this back to AMF. vSMF displays **SelectedSmfId** in smContextCreatedData.

Configuration Example:

The following is an example configuration:

```
[smf] smf(config)# profile nf-client-failure nf-type n16smf
```

```
smf] smf(config-n16smf)# profile failure-handling fh
[smf] smf(config-failure-handling-fh)# service name type nsmf-pdusession
[smf] smf(config-type-nsmf-pdusession)# message type [ PduSessionCreate  ] status-code
httpv2 <0-599>
[smf] smf(config-httpv2-400)# action [continue  retry-and-continue  retry-and-ignore
retry-and-terminate  terminate]
[smf] smf(config-httpv2-400)# retry <1-10>
```

Configuring the SMF NRF Registration

To configure the SMF NRF registration, use the sample configuration only as a reference.

```
profile smf smf1 instances
            instances 1 fqdn 5gc.mnc456.mnc123.3gppnetwork.org
            instances 1 inter-plmn-fqdn 5gc.mnc456.mnc123.3gppnetwork.org
            instances 1 supported-features [ vsmf ]
```

Note In the current release, for the SMF to register with an NRF, the **inter-plmn-fqdn** and vsmf-supported IEs are included for the SMF discovery. The configuration for **vsmfSupportIndicator** must be added on vSMF along with **inter-plmn-fqdn**. This configuration is required for vAMF to find a vSMF, which supports roaming.

To undo the configuration for **vsmfSupportIndicator**, use the following sample configuration:

```
smf] smf(config-smf-smf1)# no instances 1 supported-features
[smf] smf(config-smf-smf1)# commit
```

OAM Support

Bulk Statistics Support

This feature introduces "failed_nf_type" label in the "smf_restep_http_msg_total" statistics to indicate the target NF from where the failure response code is sent.

Following are the example queries for peer SMF and SEPP create session procedure failure responses.

- Create session procedure success:

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="201",service_name="rest-ep",sess_type="", failed_nf_type=""} 1
```

- Create session procedure failure response from SMF:

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="400",service_name="rest-ep",sess_type="", failed_nf_type="smf"} 1
```

- Create session procedure failure response from SEPP:

```
smf_restep_http_msg_total{api_name="smf_pdu_session_create",app_name="SMF",
cluster="SMF",data_center="DC",dnn="",gr_instance_id="1",
instance_id="0",message_direction="outbound",message_type="",
nf_type="smf",nf_uri="",proc_name="",rat_type="",req_cause="",response_cause="",
response_status="400",service_name="rest-ep",sess_type="", failed_nf_type="sepp"} 1
```

For more information on the bulk statistics, see the *UCC 5G SMF Metrics Reference*.

N3 and N9 User Plane Separation

Users prefer to keep the N3 and N9 network separately in a 5G network on SMF or UPF that handles both non-roaming subscribers and home routed subscribers.

If the UPF does not detect whether an UE is an outbound roamer or a homer, the SMF passes information to the UPF about the interface to use for the subscriber. To overcome this scenario, SMF allows N3 interface on one network and S5-U/S8-U and N9 interface on another network, to allow users to maintain a separate RAN network from core network especially on the data path.

The SMF populates source interface type IE (3GPP interface type) in PDI IE in N4 messages while creating PDR with an appropriate interface type. The format of IE is as below:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 160 (decimal)							
3 to 4	Length = n							
5	Spare				Interface Type Value			
6 to n+4	These octets are present only if explicitly specified							

Following table describes the 3GPP Interface type and its values.

Interface Value	Values (Decimal)
S1-U	0
S5 /S8-U **Note** If there is separation of roaming and non-roaming traffic, this value should only used for the S5-U interface and "S8-U" (decimal 19) should be used for the S8-U interface.	1
S4-U	2
S11-U	3
S12	4

Gn/Gp-U **Note** If there is separation of roaming and non-roaming traffic, this value should only be used for the Gn-U interface and "Gp-U" (decimal 20) should be used for the Gp-U interface.	5
S2a-U	6
S2b-U	7
eNodeB GTP-U interface for DL data forwarding	8
eNodeB GTP-U interface for UL data forwarding	9
SGW/UPF GTP-U interface for DL data forwarding	10
N3 3GPP Access	11
N3 Trusted Non-3GPP Access	12
N3 Untrusted Non-3GPP Access	13
N3 for data forwarding	14
N9 (or N9 for non-roaming **Note** If there is separation of roaming and non-roaming traffic, this value should only be used for N9 non-roaming interfaces and (decimal value "21") should be used for N9 roaming interfaces.	15
SGi	16
N6	17
N19	18
S8-U	19
Gp-U	20
N9 for roaming	21
Iu-U	22
N9 for data forwarding	23
Sxa-U	24

Sxb-U	25
Sxc-U	26
N4-U	27
SGW/UPF GTP-U interface for UL data forwarding	28
N6mb/Nmb9	29
N3mb	30
N19mb	31
Spare	32–63

How it Works

Following functions can occur during N3 and N9 User Plane Separation:

- SMF provides:
  - S5-U as source interface type in the Packet Detection Information (PDI) of uplinks PDRs for homers attaching via 4G RAT.
  - N3 3GPP Access as source interface type in the PDI of uplinks PDRs for homers attaching through 5G RAT.
  - S5-U as source interface type in the PDI of uplinks PDRs for homers attaching through Wi-Fi RAT. This is done as an optimization to avoid tunnel recreation during 4G < - > Wi-Fi handovers.
- During Hand Over (HO) scenarios:
  - **From 5G to 4G/Wi-Fi**: A Tunnel is recreated and N4 modification goes with uplink PDRs PDI having source interface type set to S5-U.
  - **Fron 4G/Wi-Fi to 5G**: A Tunnel is recreated and N4 modification goes with uplink PDRs PDI having source interface type set to N3.
  - Similarly, the uplink PDRs for dedicated flow/bearers get created with either N3 or S5-U source interface type depending on the RAT.
- UPF handles N4 messages without source interface type and allocates tunnel from interface, which is not associated to any interface for backward compatibility reasons.

Configuring Interface Types

To configure the UPF ingress interface type, use the following configuration:

```
configure
   context context_name
      user-plane-service service_name
```

```
[ no ] associate gtpu-service gtpu_service_name upf-ingress
end
```

NOTES:

- **associate gtpu-service** *gtpu_service_name*: Associates the GTP-U service with the user plane service.
- **upf-ingress**: Configures the interface type as UPF ingress.

The following is an example:

```
associate gtpu-service n3-upf-in upf-ingress
associate gtpu-service n3-upf-in upf-ingress interface-type S5-U | S8-U | 3 3Gpp Access |
n9-s5-s8
| N3 for data Forwarding | N9 | N6 | SGi
```

Homer Calls with N3 and N9 Separation

Following call flow process change happens in the Home routed calls.

- **vSMF Create Session Procedure**: During the 5G session creation procedure, SMF includes source interface type IE (3GPP interface type) in the PDI IE in N4 messages while creating a PDR with an appropriate interface type. For example, SMF includes source interface type= N3 3GPP Access in the Create uplink PDR in N4 messages and UPF allocates TEID from that interface based on the configuration. If no GTPU service is associated to N3 3GPP Access, then TEID is allocated from default (one without interface configuration).
- **4G Access Registration**: At the time of 4G access registration, SMF includes source interface type= S5-U in the Create uplink PDR in N4 messages and UPF allocates TEID from that interface based on the configuration. If no GTPU service is associated to S5-U, then TEID is allocated from default (one without interface configuration.

Dedicated Bearer Call Flow

Following call flow changes happen during:

- **Dedicated Bearer Flow Creation**: While creating dedicated bearer in 4G, SMF sends N4 modify with source interface type as S5-U in uplink PDR create.
- **Additional 5G Call Flow Creation**: While creating additional flows in 5G, SMF sends N4 modify with source interface type as “N3 3GPP Access” in the uplink PDR create.

Roamer Calls with N3 and N9 Separation

Following call flow process change happens during Roamer calls:

- For roamers, vSMF sends source interface type as N9 while creating downlink (DL) PDRs for N9 traffic and as “N3 3GPP Access” while creating Uplink (UL) PDRs for N3 traffic in N4 messages.
- The hSMF sends source interface type as N9 while creating UL PDRs for N9 traffic and as S5-U while creating UL PDRs (secondary PDR) for 4G traffic.
- The UPF allocates two different tunnels for the NR and 4G default bearer/flow.

Note To achieve further optimization, SMF can send N9 as source interface type while creating both 4G and 5G UL PDRs if required, without any changes on the UPF.

Allowed PLMN List Support

In networks, where non-roaming SMF and hSMF are in different nodes, AMF can select SMF based on the NRF discovery using query parameters such as NSSAI, PLMN-ID of SUPI, DNN, and so on. This selection might not provide correct results.

In such scenarios, SMF uses the NRF discovery service to register with NRF with the Allowed PLMN list. Either non-roaming SMF can register with list of home serving PLMNs or hSMF can register with partner serving PLMNs.

The SMF includes the configured allowed-plmn-list in allowedPlmns in a Network profile at the time of registering a network function to the NRF.

AMF discovers SMF using a requester-plmn-list in addition to the existing query parameters.

If allowed plmns is configured and SMF receives any SmContextCreate or SmContextUpdate with serving-plmn, which doesn't match with the configured allowed-plmn, then calls get rejected.

For more information about NF Discovery, refer to the *NF Discovery* chapter in the *UCC 5G SMF Configuration and Administration Guide*

Configuring the Allowed PLMN List

To configure the Allowed PLMN list for SMF use the following sample configuration.

```
config
  profile smf smf_profile_name
    allowed-plmn-list  [ mcc-mnc ]
    end
```

NOTES:

- **allowed-plmn-list [mcc-mnc]**: Configures the allowed plmn list.

Inter-plmn Roaming Mobility Support

The Inter-plmn roaming mobility is a feature that allows a UE to move from their home network (H-PLMN) to a partner network (V-PLMN) and vice versa while maintaining an ongoing seamless data transfer.

The SMF supports home-routed roaming Inter-plmn scenarios when the UE moves from the home network to the visitor network and vice versa.

SMF supports the following functionalities:

- Handovers from H-PLMN to V-PMLN and vice versa.
- Enabling and disabling of inter-plmn handover functionalities through a CLI.

- Advertises Deployments Topologies with specific SMF Service Areas (DTSSA) in supported features on N11 and N16 interfaces.
- Creates Secondary PDRs for secondary RATs for homer calls for efficient Inter-RAT handoffs.

During Inter-plmn mobility, vSMF:

- Selects operator policy based on the configured subscriber policy.
- Selects V-UPF and V-CHF based on the configuration.
- Uses roaming status that is configured under the Operator policy to override the HRT roaming request to treat the UE as Local Breakout (LBO).

N4 Changes

The SMF supports re-creating of PDRs rather than changing the associations.

- **5G roaming**: For 5G roaming, when the 5G UE moves from a homer to a roamer, and vice versa, N3 PDRs is created and deleted. The S5 and N9 Secondary PDRs get recreated with an existing FTEID.
- **4G roaming**: For 4G roaming, when the 4G UE moves from a homer to roamer and vice versa, S5 and N9 PDRs get recreated with existing FTEIDs. The N3 PDRs get freshly created and deleted.
- **Inter-RAT roaming**: The SMF deletes older RAT PDRs and creates new RAT PDRs for Inter-RAT scenarios. SMF also recreates the S5 and N9 PDRs with existing FTEIDs.

Limitations and Restrictions

During inter-plmn mobility, H-SMF or SMF has the following limitations:

- Does not reselect operator policy and the UPF.
- Northbound NF selection criteria do not change.
- Changes roaming status from/to homer/roamer

During inter-plmn mobility, V-SMF has the following limitations:

- Selects operator policy based on the subscriber policy configuration
- V-UPF and V-CHF are selected based on configuration.
- Roaming-status configured under the Operator policy is used to override the HRT roaming request to treat the UE as LBO.

Restrictions

SMF has the following restrictions:

- Intra-PLMN mobility where UE moves from one V-SMF to another in V-PLMN, V-SMF change is not supported.
- IDFT is not supported for Inter-plmn HO.
- If the inter-plmn CLI is not configured, ModifyBearerRequest with visitor PLMN is rejected.

- For inter-plmn scenarios, the Roaming QOS flow based charging profile configured in the H-SMF is given priority and the one received from the V-SMF is ignored.

Standards Compliance

The Inter-plmn Roaming Mobility features complies with the following standards:

- *3GPP TS 23.502,Version 16.6*
- *3GPP TS 29.502, Version 16.6*
- *3GPP TS 29.571, Version 16.6*
- *3GPP TS 29.244, Version 16.6*
- *3GPP TS 32.255, Version 16.6*

How it Works

This section describes call flows and procedures for Inter-plmn handover feature.

Call Flows

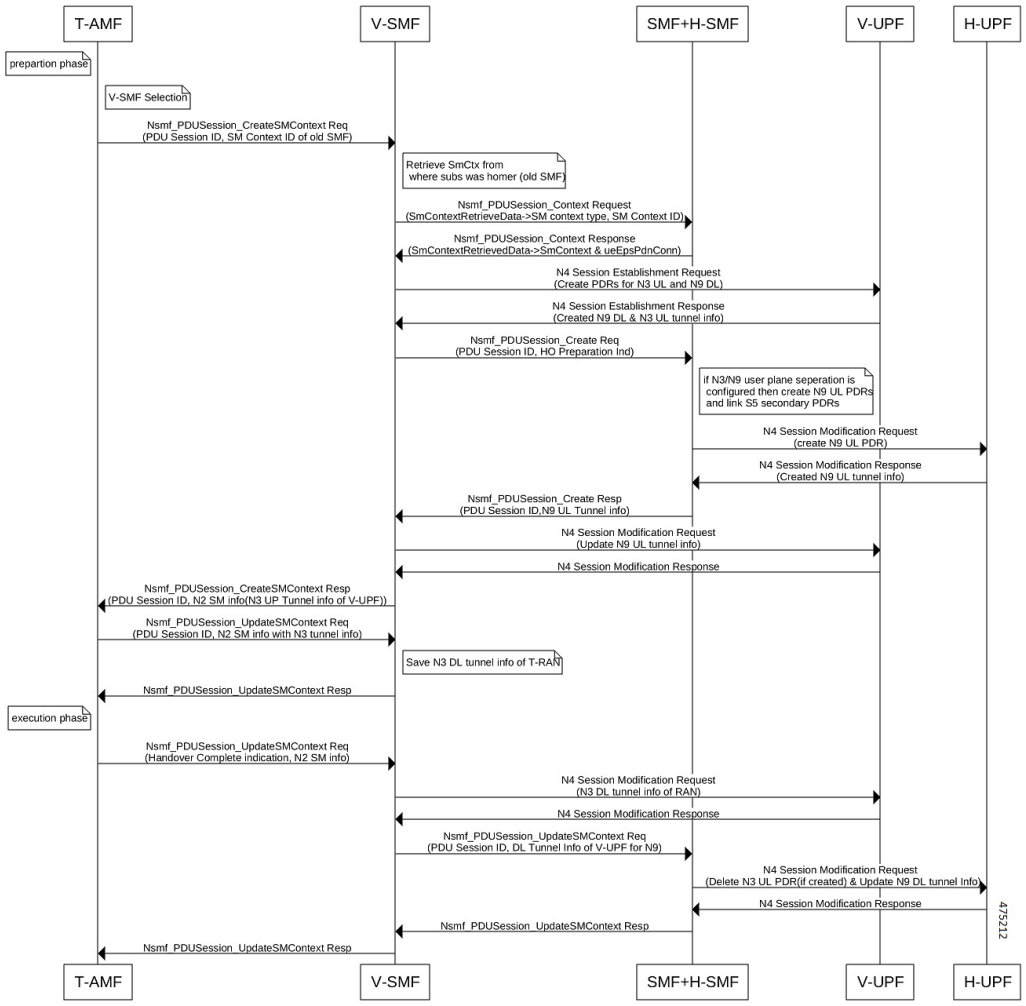
SMF supports the following call flows for various inter-plmn mobility functions:

- 5g homer to 5g roamer
- 5g roamer to 5g homer
- 5g roamer to 4g homer/roamer
- 4g roamer/homer to 5g roamer
- Intra PLMN roaming

Inter PLMN 5G Handover with Homer to Roamer

This section provides call flow and details about the Inter-plmn N2 HO procedure with v-SMF Insertion.

Figure 250: Call Flow for Inter-plmn N2 HO with v-SMF Insertion



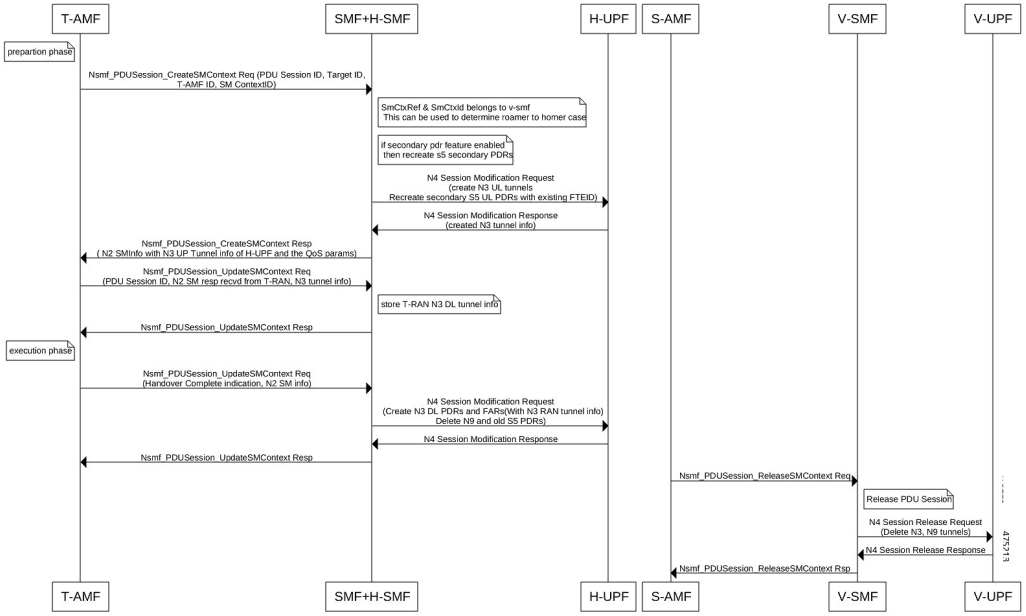
Procedure

- UE moves from being a homer in H-PLMN to a roamer in V-PLMN.
- V-SMF gets added.
- SMF transitions to the H-SMF.

Inter PLMN Handover from 5G Roamer to 5G Homer with v-SMF Deletion

This section provides call flow and details about the Inter-plmn N2 HO procedure with v-SMF deletion.

Figure 251: Call Flow for Inter-plmn N2 HO with v-SMF Deletion



Call Flow Description for Inter-plmn N2 HO with v-SMF Deletion:

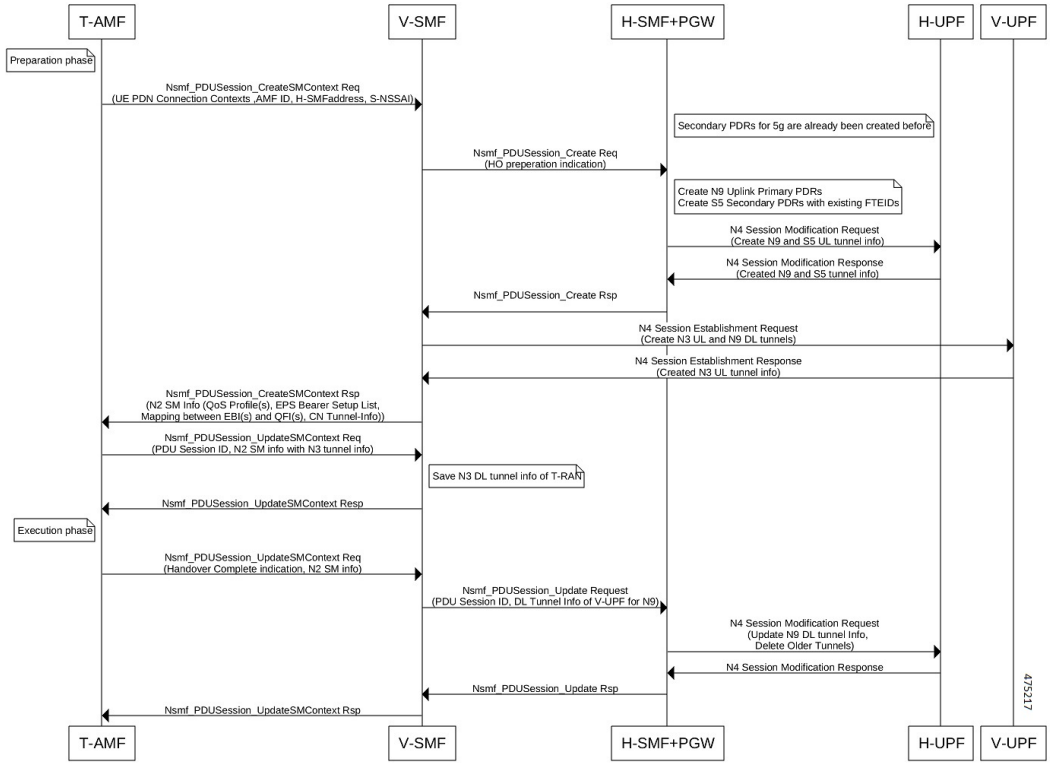
- UE moves from being a roamer in V-PLMN to a homer in H-PLMN.
- Deletes V-SMF.
- H-SMF transitions to SMF.

Inter PLMN and Inter-RAT Scenarios

Inter PLMN N26 Handover from 4G Homer to 5G Roamer

This section provides Call flow and details about the Inter-plmn N2 HO from 4G Homer to 5G Roamer.

Figure 252: Call Flow for Inter-plmn N26 HO from 4G Homer to 5G Roamer

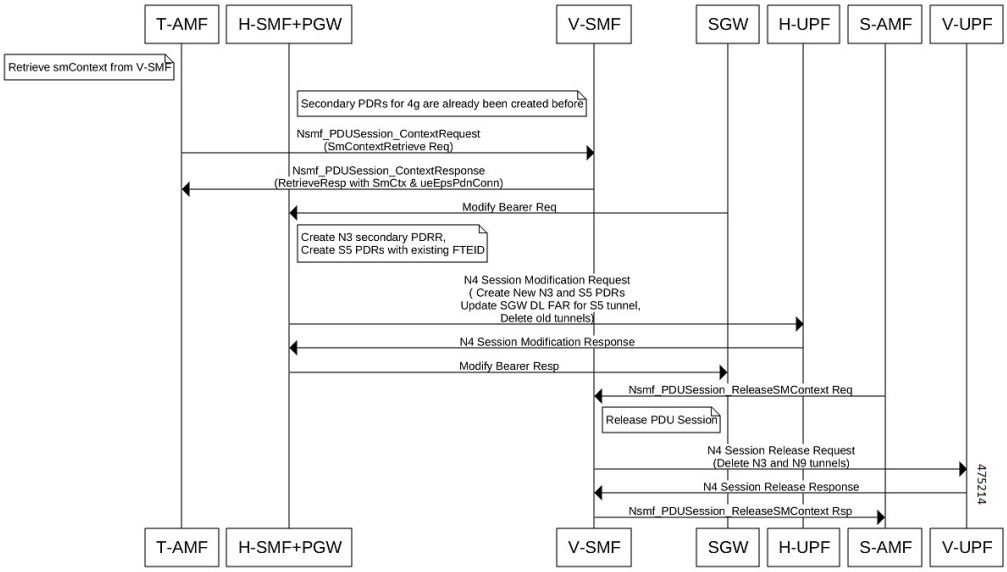


Call Flow Description for Inter-plmn N26 HO from 4G Homer to 5G Roamer: The UE moves from a 4G homer in H-PLMN or a roamer in V-PLMN to a 5G roamer in V-PLMN.

Inter PLMN Handover from 5G Roamer to 4G Homer or Roamer

This section provides call flow and details about the Inter-plmn HO from 5G Roamer to 4G Homer.

Figure 253: Call Flow for Inter-plmn HO from 5G Roamer to 4G Homer



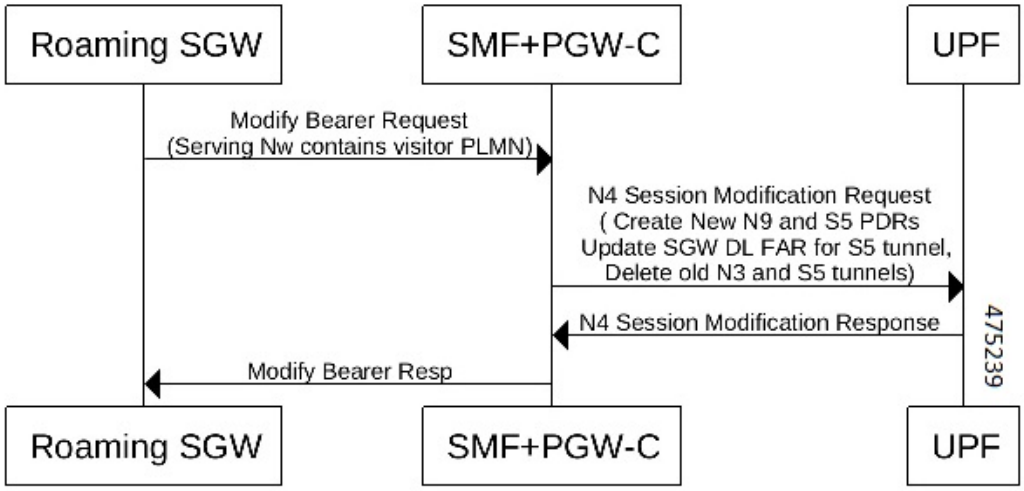
Call Flow Description for Inter-plmn HO from 5G Roamer to 4G Homer:

The UE moves from being a 5G roamer in V-PLMN to a 4G homer in H-PLMN or a 4G roamer in V-PLMN.

Inter PLMN Handover from 4G Homer to 4G Roamer

This section provides call flow and details about the Inter-plmn Handover (HO) procedure from 4G Homer to 4G Roamer.

Figure 254: Call Flow for Inter-plmn HO from 4G Homer to 4G Roamer



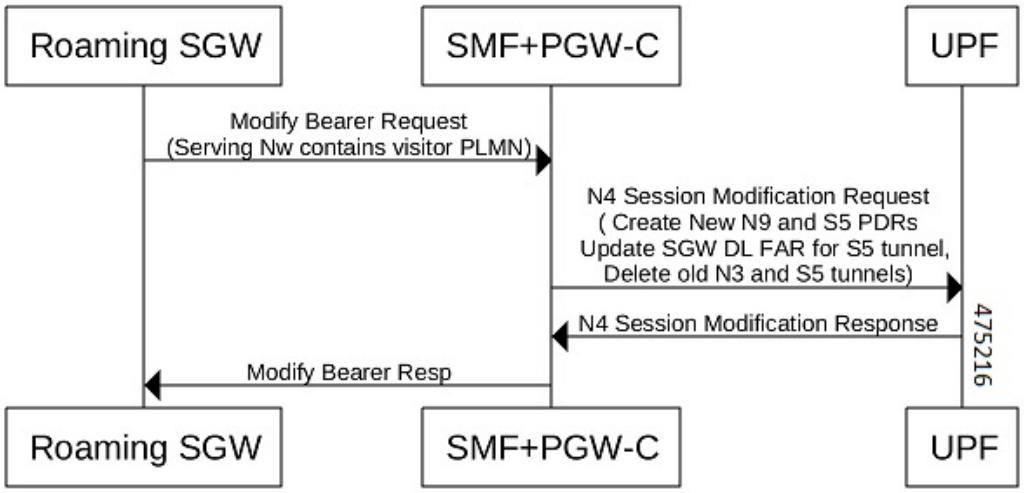
Call Flow Description for 4G Homer to 4G Roamer

- Receives the ModifyBearerRequest from a visitor S-GW.
- Determines roaming status during ModifyBearerRequest processing.
- Deletes N3 and creates N9 Secondary PDRs.
- Recreates S5 PDRs with existing FTEIDs.

Inter PLMN Handover from 4G Roamer to 4G Homer

This section provides call flow and details about the Inter-plmn N2 HO procedure from 4G Roamer to 4G Homer.

Figure 255: Call Flow for Inter-plmn N2 HO from 4G Roamer to 4G Homer



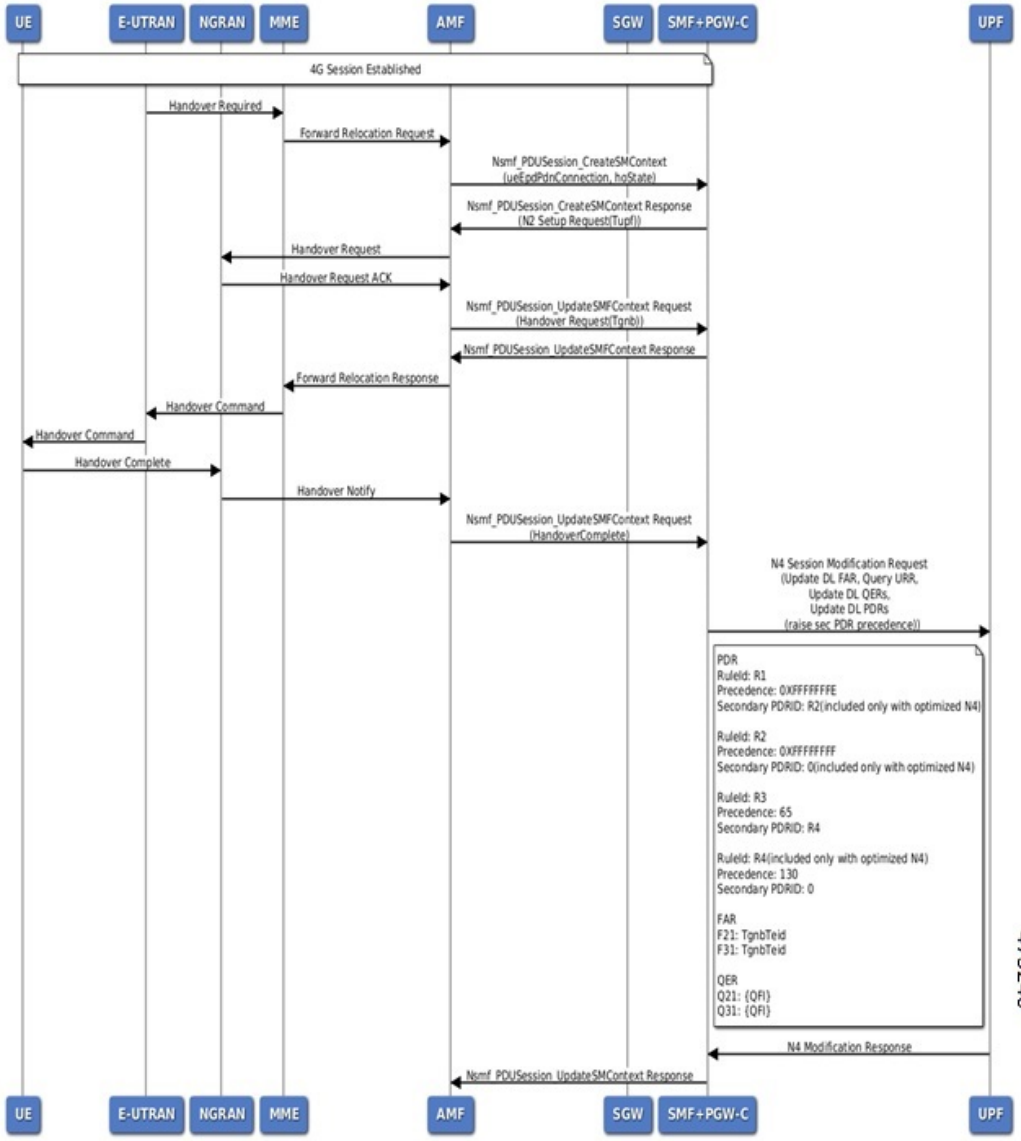
Call Flow Description for Inter-plmn N2 HO procedure from 4G Roamer to 4G Homer

- If the Subscriber is Roamer, SMF receives ModifyBearerRequest from the home S-GW.
- Determines roaming Status in ModifyBearerRequest messages.
- Deletes N9 and creates N3 Secondary PDRs
- Recreates S5 PDRs with an existing FTEID.

Inter PLMN Handover from 4G Roamer to 5G Homer

This section provides call flow and details about the Inter-plmn HO from 4G Roamer to 5G Homer.

Figure 256: Call Flow for Inter-plmn HO from 4G Roamer to 5G Homer



Call Flow Description for Inter-plmn HO from 4G Roamer to 5G Homer

- Deletes N9 secondary and creates N3 primary PDRs.
- Recreates S5 PDRs with existing FTEIDs.

Configuring the Inter PLMN Handover

Use the following sample configuration to enable or disable inter-plmn handover for roaming. You can use this configuration to disallow inter-plmn roaming for specific DNNs.

```
config
  profile dnn dnnprofile_name
     [ no ] supported-features [ inter-plmn-ho ]
```

NOTES:

- **supported-features [inter-plmn-ho]**: Enables inter-plmn handover for roaming.

Note If the inter-plmn CLI is not configured in PGW-C+SMF, MBR from a V-PLMN is rejected by PGW-C+SMF. To handle handovers from V-PLMN, configuring the inter-plmn-ho in the DNN profile is mandatory.

- **no**: Disables inter-plmn handover for roaming for a specific DNN.

Configuration for Creating Separate Tunnel for Secondary PDRs

Use the sample configuration to check whether N3and N9 interface separation is enabled or not at UPF. If n3-n9 interface-separation is enabled, then a separate tunnel is created for the Secondary RAT PDR else, the same tunnel is reused for the Secondary RAT.

```
config
  profile dnn dnnprofile_name
     [ no ] supported-features [ n3-interface-separation ]
```

NOTES:

- **supported-features [n3-interface-separation]**: Creates Separate Tunnel for Secondary PDRs.
- **no**: Creates same tunnel for Primary and Secondary PDRs.

Note If this config is not present, then SMF/PGW-C considers that the N3-N9 interface separation is disabled at UPF.

Sending DTSSA and ACSCR

SMF supports sending the DTSSA and ACSCR in supported-features in the following SmContextCreated, SmContextUpdated, PduSessionCreated, and PduSessionUpdated IEs on N11 and N16 interfaces.

This allows AMF to select an appropriate V-SMF and H-SMF for inter-plmn roaming.

Configuring DTSSA

To configure the DTSSA or ACSCR, use the sample configuration as a reference.

```
config
  profile smf profile_name instances instance-id supported-features
     [ vsmf dtssa acscr]
```

NOTES:

- **vsmf dtssa acscr**: Sends DTSSA and ACSCR in supported-features.

OAM Support

This section describes operations, administration, and maintenance information regarding support for interfaces in SMF.

Bulk Statistics Support

The following labels are added for the Inter-plmn mobility feature:

- interplmn_ho_not_configured
- dtssa_acscr_not_supported
- disc_vsmf_insert_dtssa_acscr_not_configured
- disc_vsmf_insert_interplmn_ho_not_configured
- disc_vsm_insert_hsmf_retrieve_failure
- disc_ro2ho_n2ho_interplmn_ho_not_configured
- disc_ro2ho_n4_modify_failed
- disc_ho2ro_n4_modify_failed
- disc_ho2ro_failure
- disc_ro2ho_failure
- ho2ro_invalid_state
- ro2ho_invalid_state
- disc_ro2ho_guard_timer_expiry
- disc_ho2ro_guard_timer_expiry
- disc_ro2ho_idft_timer_expiry
- smf_idft_inter_plmn_ro2ho_n2ho
- smf_dft_inter_plmn_ro2ho_n2ho
- smf_idft_inter_plmn_ho2ro_n2ho
- smf_dft_inter_plmn_ho2ro_n2ho

Roaming Status on N4 Interface

A **sub IE** option is added under the proprietary IE, in the **subscriber-params** N4 messages to allow the UPF know about the roaming status.

```
SUBSCRIBER PARAMS:
Type: 226
    roaming-status: homer/roamer/visitor-hr/visitor-lbo
```

The following sample output lists roaming statuses.

```
Homer- 1
Visitor-LBO - 2
Visitor-HR - 3
Roamer - 4
```

Troubleshooting Information

This section provides information on using the command line interface (CLI) commands, alerts, logs, and metrics for troubleshooting any roaming related issues that may arise during system operation.

Subscriber Details for Roaming-specific Information

The **show subscriber supi** *supi_id* **nf-service smf full** CLI command displays the roaming status of a UE.

Note In 2021.02 and later releases, the **namespace** keyword is deprecated and replaced with the **nf-service** keyword.

```
[unknown-smf] smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
…
        "authStatus": "Unauthenticated",
        "roamingStatus": "Vistor LBO",    <<< In-Roamer UE Roaming Status
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        }

…
     "authStatus": "Unauthenticated",
        "roamingStatus": "Roamer",      <<< Out-Roamer UE Roaming Status
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        }
…
        "authStatus": "Unauthenticated",
        "roamingStatus": "Homer",
        "uePlmnId": {
          "mcc": "123",
          "mnc": "456"
        }
```

Subscriber Details for Roaming-specific Information for hSMF

The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** CLI command displays the detailed subscriber information for roaming-specific use case as hSMF.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf psid
 5 full
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310210789012346",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "560"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "209.165.200.229",
    "nrLocation": {
      "ncgi": {
        "mcc": "310",
        "mnc": "560",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "310",
        "mnc": "560",
        "tac": "1820"
      }
    },
    "alwaysOn": "None",
    "dcnr": "None",
    "wps": "Non-Wps Session",
    "ratType": "NR",
    "ueType": "NR Capable UE",
    "sessTimeStamp": "2021-06-18 18:49:28.266245111 +0000 UTC",
    "callDuration": "20.549700502s",
    "ipPool": "poolv4",
    "commonId": 2097158,
    "snssai": {
      "sd": "Abf123",
      "sst": 2
    },
    "authStatus": "Unauthenticated",
    "roamingStatus": "Roamer",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "210"
    }
  },
  "accessSubData": {
    "amfID": "AFbe08",
    "amfPlmnId": {
      "mcc": "310",
      "mnc": "560"
    },
    "epsInterworkingIndication": "WITHOUT_N26"
  },
  "policySubData": {
    "TotalDynamicRules": 2,
    "TotalFlowCount": 2,
    "TotalNonGBRFlows": 1,
    "TotalGBRFlows": 1,
```

```
"pccRuleList": [
  {
    "pccRuleId": "PccRule-1",
    "qfi": 2,
    "gbrDl": 2000000000,
    "gbrUl": 1000000000,
    "mbrDl": 4000000000,
    "mbrUl": 3000000000,
    "flowInformation": [
      {
        "flowLabel": "flow",
        "spi": "2",
        "flowDirection": 3,
        "flowDescription": "permit out ip from 209.165.200.225 to 209.165.200.254",
        "tosTrafficClass": "8"
      }
    ],
    "chargingInformation": {
      "chargingId": "ChargingData-1",
      "meteringMethod": "Duration and Volume",
      "Type": "Online",
      "ratingGroup": 10,
      "serviceId": "20"
    }
  },
  {
    "pccRuleId": "defaultrule",
    "qfi": 1,
    "mbrDl": 125000000,
    "mbrUl": 100000000,
    "flowInformation": [
      {
        "flowDirection": 3,
        "flowDescription": "permit out ip from any to any"
      }
    ]
  }
],
"qosFlow": [
  {
    "qfi": 2,
    "GBRFlow": "True",
    "bindingParameters": {
      "x5Qi": 3,
      "arp": {
        "preemptCap": "NOT_PREEMPT",
        "preemptVuln": "PREEMPTABLE",
        "priorityLevel": 7
      }
    },
    "AggregatedULGFbr": 1000000000,
    "AggregatedDLGFbr": 2000000000,
    "AggregatedULMFbr": 3000000000,
    "AggregatedDLMFbr": 4000000000,
    "pccRuleList": "PccRule-1",
    "qosDescList": "QoS-1,"
  },
  {
    "qfi": 1,
    "GBRFlow": "False",
    "bindingParameters": {
      "x5Qi": 5,
      "arp": {
        "preemptCap": "NOT_PREEMPT",
```

```
            "preemptVuln": "NOT_PREEMPTABLE",
            "priorityLevel": 15
          },
          "priorityLevel": 1
        },
        "AggregatedULMFbr": 100000000,
        "AggregatedDLMFbr": 125000000,
        "pccRuleList": "defaultrule",
        "qosDescList": "default,"
      }
    ],
    "policyType": "Pcf",
    "pcfInteraction": "Pcf Interaction: ON",
    "ruleBase": "starent",
    "sessRuleList": [
      {
        "authDefaultQos": "&QosProfileKey{X5QI:5,Arp:{PreemptionCapability_NOT_PREEMPT
PreemptionVulnerability_NOT_PREEMPTABLE 15
true},Priority:1,MaxDataBurstVol:0,Qnc:false,AveragingWindow:,}",
        "authSessAmbr": {
          "downlink": 125000000,
          "uplink": 100000000
        },
        "sessRuleId": "default"
      }
    ],
    "presenceReporting": "Disabled"
  },
  "chargingData": {
    "invcSeqNo": 1,
    "pduChId": 2097158,
    "ccId": "1",
    "chargingIdRtgGrpMapInfo": {
      "rgId": "10",
      "chargingId": [
        "ChargingData-1",
        "l10of",
        "l10on"
      ]
    },
    "chargParmMapInfo": [
      {
        "ratingGrp": 10,
        "chargingId": "ChargingData-1",
        "online": "true",
        "offline": "true",
        "serviceID": 20,
        "pccRuleIds": [
          "PccRule-1"
        ],
        "linkedChrgId": [
          "l10of",
          "l10on",
          "sesslevelurr"
        ],
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingLevelOnline": "ReportingLevel_RAT_GR_LEVEL",
        "reportingLevelOffline": "ReportingLevel_RAT_GR_LEVEL",
        "configured": "false",
        "tightInterworkingMode": "false",
        "parent": "true",
        "reportingParm": "false",
        "limitParm": "false",
        "limitsChrgParamOnline": "l10on",
```

```
  "limitsChrgParamOffline": "l10of",
  "qosIds": [
    "QoS-1"
  ],
  "qfi": 2,
  "offlineConverted": "false"
},
{
  "ratingGrp": 10,
  "chargingId": "l10of",
  "online": "false",
  "offline": "true",
  "pccRuleIds": [
    "PccRule-1"
  ],
  "linkedChrgId": [
    "sesslevelurr"
  ],
  "meteringMthd": "MeteringMethod_DURATION_VOLUME",
  "reportingLevelOnline": "ReportingLevel_Dummy",
  "reportingLevelOffline": "ReportingLevel_RAT_GR_LEVEL",
  "configured": "false",
  "tightInterworkingMode": "false",
  "parent": "false",
  "reportingParm": "true",
  "limitParm": "true",
  "qosIds": [
    "QoS-1"
  ],
  "qfi": 2,
  "offlineConverted": "false"
},
{
  "ratingGrp": 10,
  "chargingId": "l10on",
  "online": "true",
  "offline": "false",
  "pccRuleIds": [
    "PccRule-1"
  ],
  "linkedChrgId": [
    "sesslevelurr"
  ],
  "meteringMthd": "MeteringMethod_DURATION_VOLUME",
  "reportingLevelOnline": "ReportingLevel_RAT_GR_LEVEL",
  "reportingLevelOffline": "ReportingLevel_Dummy",
  "configured": "false",
  "tightInterworkingMode": "false",
  "parent": "false",
  "reportingParm": "true",
  "limitParm": "true",
  "qosIds": [
    "QoS-1"
  ],
  "qfi": 2,
  "offlineConverted": "false"
},
{
  "chargingId": "sesslevelurr",
  "online": "false",
  "offline": "true",
  "pccRuleIds": [
    "PccRule-1"
  ],
```

```
      "meteringMthd": "MeteringMethod_DURATION_VOLUME",
      "reportingLevelOnline": "ReportingLevel_Dummy",
      "reportingLevelOffline": "ReportingLevel_Dummy",
      "configured": "false",
      "tightInterworkingMode": "false",
      "parent": "false",
      "reportingParm": "false",
      "limitParm": "true",
      "offlineConverted": "false"
    }
  ],
  "chTriggerInfo": {
    "sessionTriggerInfo": [
      {
        "triggerType": "VOLUME_LIMIT",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "TIME_LIMIT",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "AMBR_CHANGE",
        "triggerCategory": "IMMEDIATE_REPORT",
        "triglevel": 2
      },
      {
        "triggerType": "QOS_CHANGE",
        "triggerCategory": "DEFERRED_REPORT",
        "triglevel": 2
      }
    ],
    "rgTrgrList": [
      {
        "ratingGroup": 10,
        "rgTriggerInfo": [
          {
            "triggerType": "QUOTA_THRESHOLD",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          },
          {
            "triggerType": "VOLUME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          },
          {
            "triggerType": "TIME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          },
          {
            "triggerType": "QUOTA_EXHAUSTED",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 1
          }
        ]
      }
    ]
  },
  "chThresholdInfo": {
    "sessthresholdInformation": {
```

```
      "volumeThreshold": 45000,
      "durationThreshold": 90
    },
    "rgthresholdInformation": [
      {
        "volumeThreshold": 7000,
        "durationThreshold": 800
      }
    ],
    "quotaInformation": [
      {
        "quotaHoldingTime": -1,
        "timeQuotaThreshold": 10,
        "volQuotaThreshold": 1000,
        "downlinkVolume": 20000,
        "time": 100,
        "totalVolume": 35000,
        "uplinkVolume": 15000,
        "ratingGrp": 10
      }
    ]
  },
  "startTime": "2021-06-18T18:49:28Z",
  "rulebase": "starent",
  "chargingDisabled": "false",
  "dropTraffic": "false",
  "gtppGrp": "group1",
  "profileName": "chgprf1",
  "accountingEnabled": "false",
  "n40ChargingEnabled": "true",
  "QbcProfileName": "qbc_general",
  "qbcChargingEnabled": "True",
  "roamingQbcInfo": {
    "qfiTh": {
      "volTh": 30000,
      "durTh": 80
    },
    "qfis": {
      "rgTriggerInfo": [
        {
          "triggerType": "QOS_CHANGE",
          "triggerCategory": "IMMEDIATE_REPORT",
          "triglevel": 2
        },
        {
          "triggerType": "TIME_LIMIT",
          "triggerCategory": "IMMEDIATE_REPORT",
          "triglevel": 2
        },
        {
          "triggerType": "VOLUME_LIMIT",
          "triggerCategory": "IMMEDIATE_REPORT",
          "triglevel": 2
        }
      ]
    },
    "partialRecordMethod": "PartialRecordMethod_DEFAULT"
  },
  "qbcChargParam": [
    {
      "chargingId": "qfi1",
      "qfi": 1,
      "meteringMthd": "MeteringMethod_DURATION_VOLUME",
      "reportingParam": "True",
```

```
        "limitParam": "True",
        "parent": "True"
      },
      {
        "chargingId": "qfi2",
        "qfi": 2,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      }
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "True"
  },
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 9007228892966842,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "QoS-1@def#TC",
        "qerId": 2,
        "refcnt": 1
      },
      {
        "qosId": "default@def#TC",
        "qerId": 3,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "ChargingData-1",
        "urrId": 16
      },
      {
        "chargingId": "l10of",
        "urrId": 33
      },
      {
        "chargingId": "l10on",
        "urrId": 55
      },
      {
        "chargingId": "sesslevelurr",
        "urrId": 76
      },
      {
        "chargingId": "qfi1",
        "urrId": 82
      },
      {
        "chargingId": "qfi2",
        "urrId": 98
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
```

```
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 1001,
            "ipAddr": "209.165.200.241"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 6
  }
}
```


Subscriber Session Details for Roaming-specific Information for hSMF

The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** CLI command displays the detailed information about subscriber sessions for roaming-specific use case as hSMF.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smfpsid
 5 summary
```


```
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310210789012346",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "560"
    },
    "allocatedIp": "209.165.200.240",
    "ratType": "NR",
    "sessTimeStamp": "2021-06-18 18:49:28.266245111 +0000 UTC",
    "authStatus": "Unauthenticated",
    "roamingStatus": "Roamer",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "210"
    }
  },
  "policySubData": {
    "TotalDynamicRules": 2,
    "TotalFlowCount": 2,
    "TotalNonGBRFlows": 1,
    "TotalGBRFlows": 1,
    "pcfInteraction": "Pcf Interaction: ON",
    "ruleBase": "starent"
  },
  "chargingData": {
    "chargParmMapInfo": [
      {
        "chargingId": "ChargingData-1",
        "offlineConverted": "false"
      },
      {
```

```
        "chargingId": "l10of",
        "offlineConverted": "false"
      },
      {
        "chargingId": "l10on",
        "offlineConverted": "false"
      },
      {
        "chargingId": "sesslevelurr",
        "offlineConverted": "false"
      }
    ],
    "chargingDisabled": "false",
    "dropTraffic": "false",
    "gtppGrp": "group1",
    "profileName": "chgprf1",
    "accountingEnabled": "false",
    "n40ChargingEnabled": "true",
    "QbcProfileName": "qbc_general",
    "qbcChargingEnabled": "True",
    "qbcChargParam": [
      {},
      {}
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "True"
  },
  "upfServData": {
    "smfSeid": 9007228892966842,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "QoS-1@def#TC",
        "qerId": 2,
        "refcnt": 1
      },
      {
        "qosId": "default@def#TC",
        "qerId": 3,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "ChargingData-1",
        "urrId": 16
      },
      {
        "chargingId": "l10of",
        "urrId": 33
      },
      {
        "chargingId": "l10on",
        "urrId": 55
      },
      {
        "chargingId": "sesslevelurr",
        "urrId": 76
      },
      {
```

```
        "chargingId": "qfi1",
        "urrId": 82
      },
      {
        "chargingId": "qfi2",
        "urrId": 98
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 1001,
            "ipAddr": "209.165.200.231"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 6
  }
}
```


Subscriber Details for Roaming-specific Information for vSMF

The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** CLI command displays the detailed subscriber information for roaming-specific use case as vSMF.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf psid
 5 full
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310480789012346",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "260"
    },
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "209.165.202.131",
    "nrLocation": {
      "ncgi": {
        "mcc": "310",
        "mnc": "260",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "310",
        "mnc": "260",
        "tac": "1820"
      }
```

```
    },
    "alwaysOn": "None",
    "dcnr": "None",
    "wps": "Non-Wps Session",
    "ratType": "NR",
    "ueType": "NR Capable UE",
    "sessTimeStamp": "2021-06-18 18:55:11.252750658 +0000 UTC",
    "callDuration": "42.336122162s",
    "commonId": 2097159,
    "snssai": {
      "sd": "Abf123",
      "sst": 2
    },
    "authStatus": "Unauthenticated",
    "roamingStatus": "Vistor HR",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "480"
    }
  },
  "accessSubData": {
    "amfID": "AFbe08",
    "amfPlmnId": {
      "mcc": "310",
      "mnc": "260"
    },
    "ueCmStatus": "UeCMConnected",
    "amfNrfID": "76517361-338e-4d77-bc76-713a79779574",
    "epsInterworkingIndication": "WITHOUT_N26"
  },
  "policySubData": {
    "TotalFlowCount": 2,
    "TotalNonGBRFlows": 1,
    "TotalGBRFlows": 1,
    "qosFlow": [
      {
        "qfi": 1,
        "GBRFlow": "False",
        "bindingParameters": {
          "x5Qi": 5,
          "arp": {
            "preemptCap": "NOT_PREEMPT",
            "preemptVuln": "NOT_PREEMPTABLE",
            "priorityLevel": 1
          },
          "priorityLevel": 10,
          "maximumDataBurstVolume": 1,
          "averagingWindow": "2003"
        }
      },
      {
        "qfi": 4,
        "GBRFlow": "True",
        "bindingParameters": {
          "x5Qi": 4,
          "arp": {
            "preemptCap": "NOT_PREEMPT",
            "preemptVuln": "NOT_PREEMPTABLE",
            "priorityLevel": 1
          },
          "priorityLevel": 1,
          "maximumDataBurstVolume": 1,
          "averagingWindow": "1"
        },
```

```
        "AggregatedULGFbr": 10000000,
        "AggregatedDLGFbr": 10000000,
        "AggregatedULMFbr": 1000000000,
        "AggregatedDLMFbr": 1000000000,
        "ebi": 8
      }
    ],
    "SessAmbrUl": 200000000,
    "SessAmbrDl": 125000000
  },
  "chargingData": {
    "invcSeqNo": 3,
    "pduChId": 2097159,
    "ccId": "0",
    "chargingIdRtgGrpMapInfo": {},
    "chTriggerInfo": {},
    "chThresholdInfo": {
      "sessthresholdInformation": {}
    },
    "startTime": "2021-06-18T18:55:11Z",
    "chargingDisabled": "false",
    "dropTraffic": "false",
    "profileName": "chgprf1",
    "accountingEnabled": "false",
    "n40ChargingEnabled": "true",
    "QbcProfileName": "qbc_maxlimit",
    "qbcChargingEnabled": "True",
    "roamingQbcInfo": {
      "qfiTh": {
        "volTh": 40000,
        "durTh": 90
      },
      "qfis": {
        "rgTriggerInfo": [
          {
            "triggerType": "QOS_CHANGE",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          },
          {
            "triggerType": "TIME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          },
          {
            "triggerType": "VOLUME_LIMIT",
            "triggerCategory": "IMMEDIATE_REPORT",
            "triglevel": 2
          }
        ]
      },
      "partialRecordMethod": "PartialRecordMethod_DEFAULT"
    },
    "qbcChargParam": [
      {
        "chargingId": "qfi1",
        "qfi": 1,
        "meteringMthd": "MeteringMethod_DURATION_VOLUME",
        "reportingParam": "True",
        "limitParam": "True",
        "parent": "True"
      },
      {
        "chargingId": "qfi4",
```

```
            "qfi": 4,
            "meteringMthd": "MeteringMethod_DURATION_VOLUME",
            "reportingParam": "True",
            "limitParam": "True",
            "parent": "True"
          }
        ],
        "chfGroupId": "CHF-dnn=intershat;",
        "fbcChargingEnabled": "False"
      },
      "upfServData": {
        "numberOfTunnels": 1,
        "smfSeid": 9007233406673128,
        "qerInfo": [
          {
            "qosId": "Sess#Level",
            "qerId": 1,
            "refcnt": 1
          },
          {
            "qosId": "BQF_1",
            "qerId": 2,
            "refcnt": 1
          },
          {
            "qosId": "BQF_4",
            "qerId": 4,
            "refcnt": 1
          }
        ],
        "urrInfo": [
          {
            "chargingId": "qfi1",
            "urrId": 18
          },
          {
            "chargingId": "qfi4",
            "urrId": 50
          }
        ],
        "mapping": {
          "tunnelMapping": [
            {
              "TunnelID": 1,
              "tunnelName": "gnbTunnel",
              "RemoteTeid": {
                "teID": 5555,
                "ipAddr": "209.165.200.242"
              }
            }
          ]
        },
        "upfSeid": "17293822569102704642",
        "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
        "TotalNumberOfFars": 4,
        "TotalNumberOfQers": 3,
        "TotalNumberOfUrrs": 2
      }
    }
```

Subscriber Session Details for Roaming-specific Information for vSMF

The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** CLI command displays the detailed information about subscriber sessions for roaming-specific use case as vSMF.

```
[unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf psid
 5 summary
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-310480789012346",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "3GPP_ACCESS",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "310",
      "mnc": "260"
    },
    "allocatedIp": "209.165.200.231",
    "ratType": "NR",
    "sessTimeStamp": "2021-06-18 18:55:11.252750658 +0000 UTC",
    "authStatus": "Unauthenticated",
    "roamingStatus": "Vistor HR",
    "uePlmnId": {
      "mcc": "310",
      "mnc": "480"
    }
  },
  "policySubData": {
    "TotalFlowCount": 2,
    "TotalNonGBRFlows": 1,
    "TotalGBRFlows": 1,
    "SessAmbrUl": 200000000,
    "SessAmbrDl": 125000000
  },
  "chargingData": {
    "chargingDisabled": "false",
    "dropTraffic": "false",
    "profileName": "chgprf1",
    "accountingEnabled": "false",
    "n40ChargingEnabled": "true",
    "QbcProfileName": "qbc_maxlimit",
    "qbcChargingEnabled": "True",
    "qbcChargParam": [
      {},
      {}
    ],
    "chfGroupId": "CHF-dnn=intershat;",
    "fbcChargingEnabled": "False"
  },
  "upfServData": {
    "smfSeid": 9007233406673128,
    "qerInfo": [
      {
        "qosId": "Sess#Level",
        "qerId": 1,
        "refcnt": 1
      },
      {
        "qosId": "BQF_1",
        "qerId": 2,
```

```
        "refcnt": 1
      },
      {
        "qosId": "BQF_4",
        "qerId": 4,
        "refcnt": 1
      }
    ],
    "urrInfo": [
      {
        "chargingId": "qfi1",
        "urrId": 18
      },
      {
        "chargingId": "qfi4",
        "urrId": 50
      }
    ],
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel",
          "RemoteTeid": {
            "teID": 5555,
            "ipAddr": "209.165.200.242"
          }
        }
      ]
    },
    "upfSeid": "17293822569102704642",
    "TotalNumberOfPdrs": "4 (Ul:2 Dl:2)",
    "TotalNumberOfFars": 4,
    "TotalNumberOfQers": 3,
    "TotalNumberOfUrrs": 2
  }
}
```


Roamer UE Alerts

This section describes the alerts supported for roamer UEs. These alerts can be enhanced per RAT based or as per the intent of the end user.

In-roamer UE Failure Threshold Alert

Use the following example to configure alerts related to In-roamer UE Failure Threshold.

```
alerts rules group RoamerUEs
 rule In-Roamer_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"visitor-lbo\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by (namespace)
 (increase(smf_service_stats{app_name=\"smf\", roaming_status=\"visitor-lbo\", rat_type!=\"\",
 status=\"attempted\"}[5m])) < 0.10"
  severity major
  type "Communications Alarm"
  annotation summary
   value "This alert is fired when the percentage of successful InRoamer is lesser than
threshold"
  exit
exit
```

Out-roamer UE Failure Threshold Alert

Use the following example to configure alerts related to Out-roamer UE Failure Threshold.

```
rule Radius_Acct_Release_SR
   rule Out-Roamer_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"roamer\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", roaming_status=\"roamer\", rat_type!=\"\",
status=\"attempted\"}[5m])) < 0.10"
  severity major
  type "Communications Alarm"
  annotation summary
   value "This alert is fired when the percentage of successful InRoamer is lesser than
threshold"
  exit
exit
```

Roamer UE Bulk Statistics

Use the following SMF service bulk statistics to monitor the failures or issues associated with Roamer UEs.

Table 424: Roamer UE

Bulk Statistics Name	Query	Descriptio
4G_In-Roamers_Attempted	bulk-stats query 4G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='EUTRA'}) by (namespace)" exit	
4G_In-Roamers_Success	bulk-stats query 4G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='EUTRA'}) by (namespace)" exit	
4G_Out-Roamers_Attempted	bulk-stats query 4G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='EUTRA'}) by (namespace)" exit	
4G_Out-Roamers_Success	bulk-stats query 4G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='EUTRA'}) by (namespace)" exit	
5G_In-Roamers_Attempted	bulk-stats query 5G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='NR'}) by (namespace)" exit	
5G_In-Roamers_Success	bulk-stats query 5G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='NR'}) by (namespace)" exit	
5G_Out-Roamers_Attempted	bulk-stats query 5G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='NR'}) by (namespace)" exit	

Bulk Statistics Name	Query	Description
5G_Out-Roamers_Success	bulk-stats query 5G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='NR'}) by (namespace)" exit	
WiFi_In-Roamers_Attempted	bulk-stats query WiFi_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='WLAN'}) by (namespace)" exit	
WiFi_In-Roamers_Success	bulk-stats query WiFi_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='WLAN'}) by (namespace)" exit	
WiFi_Out-Roamers_Attempted	bulk-stats query WiFi_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='WLAN'}) by (namespace)" exit	
WiFi_Out-Roamers_Success	bulk-stats query WiFi_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='WLAN'}) by (namespace)" exit	

Roaming Error Logs

This section provides the basic error conditions and logs that are captured to debug the failures for the roaming feature.

PLMN Validation Failure

The following example displays the error log for PLMN validation failure resulting into setting the roaming status as "none".

```
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 0
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=0)
2021/01/06 15:25:18.630 smf-service [ERROR] [genericinfo.go:1082]
[smf-service.smf-app.subscriber] PLMN validation failed
2021/01/06 15:25:18.630 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-223310101010101 imei-123456786666660  0 123 456 intershat}
```

Homer UE Status (Homer)

The following is an example of the generic logs for UE Roaming Status.

```
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 1
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=1)
2021/01/06 15:04:39.146 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345 msisdn-9999988888
 imei-352099001761480 Abf123 2 310 310 intershat}
```

Out-roamer UE Status (Roamer)

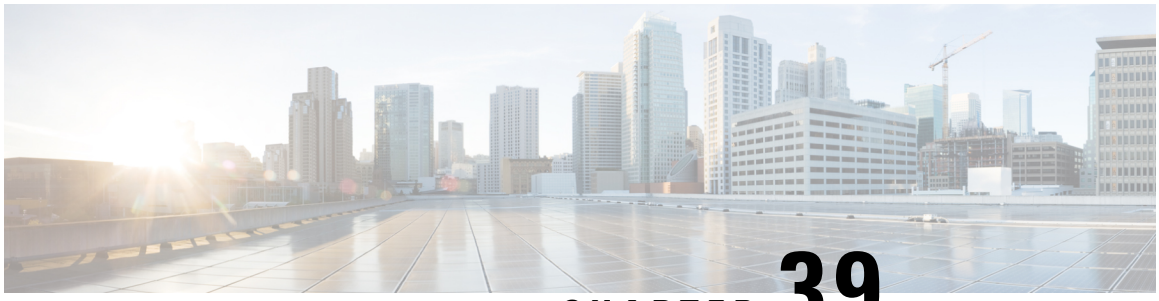
The following is an example of the generic logs for out-roamer UE status.

```
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 4
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=4)
2021/01/06 16:11:02.710 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
```

In-roamer UE Status (Visitor LBO)

The following is an example of the generic logs for in-roamer UE status.

```
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 2
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber]  Subscriber is %!s(uint32=2)
2021/01/06 15:54:32.323 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-223310101010101 imei-123456786666660  0 310 310 intershat}
```



CHAPTER 39

Session and Service Continuity Mode

- Feature Summary and Revision History, on page 1363
- Feature Description, on page 1363
- Configuring SSC Mode, on page 1365

Feature Summary and Revision History

Summary Data

Table 425: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 426: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The Session and Service Continuity (SSC) support in 5G system architecture addresses the various continuity requirements of different applications and services for the User Equipment (UE). The 5G system supports

different SSC modes. The SSC mode associated with a PDU session does not change during the lifespan of a PDU session. The SSC feature supports the following three modes:

- SSC mode 1—The network preserves the connectivity service provided to the UE. For the PDU session of IPv4 or IPv6 or IPv4v6 type, the IP address is preserved.
- SSC mode 2—The network may release the connectivity service delivered to the UE and also release the corresponding PDU sessions. For IPv4 or IPv6 or IPv4v6 type, the release of the PDU session induces the release of IP addresses allocated to the UE.
- SSC mode 3—Changes to the user plane can be visible to the UE while the network ensures that the UE suffers no loss of connectivity. A connection through new PDU session anchor point is established before the previous connection is terminated for better service continuity. For IPv4 or IPv6 or IPv4v6 type, the IP address is not preserved in this mode when the PDU session anchor changes.

SSC Mode Selection

The SSC mode selection policy determines the type of mode associated with an application or group of applications for the UE. As part of the subscription information from UDM, the SMF receives the list of supported SSC modes and the default SSC mode per DNN and per S-NSSAI.

To select the SSC mode, when UE sends SSC mode in PDU Session Establishment Request, the allowed SSC mode is determined by checking against the subscriber data and local SMF configuration.

Important SMF supports only SSC mode-1.

Priority for Choosing SSC Mode

The priority levels for choosing SSC mode are:

- Priority #1—Subscriber data from UDM has the highest priority. UDM sends DefaultSscMode and AllowedSscMode.
- Priority #2—Local SSC mode configuration data present in DNN profile contains ssc-mode and allowed-ssc-mode.

SSC Mode Selection Method

The SSC mode supports the following selection methods:

- The SMF verifies if UE sent SSC mode is part of either default SSC mode or allowed SSC mode in order of priority. If it is found, PDU Establishment procedure continues. Otherwise, PDU Session Establishment Reject message will be sent to the UE with allowed SSC modes in reject message.
- If the SMF does not receive SSC mode from the UE, then default SSC mode in order of priority is chosen and used to establish the PDU session.

When UE requests SSC mode-2 or mode-3, if the UE's subscription (in order of priority: UDM or Local configuration on SMF) allows SSC mode-1 along with mode-2 or mode-3, then SMF sends PDU Session Establishment Reject with 5GSM cause 68 (Not supported SSC mode) and Allowed SSC mode as 01. This

method allows the UE to retry with SSC mode-1. As per 3GPP TS 24.501, the 5GSM cause 68 is sent when the requested SSC mode is not supported by the subscription.

To honor PDU Session Establishment, the SMF expects SSC mode either through UDM subscription or local configuration. If SMF does not have SSC mode as part of UDM subscription or local configuration, the SMF rejects PDU Session Establishment with 5GSM cause 31 (Request rejected and unspecified).

Configuring SSC Mode

To configure the Session and Service Continuity Mode parameters in the DNN profile, use the following sample configuration:

```
config
   profile dnn dnn_name
      ssc-mode sscmode_value [ allowed allowed_sscmode_value ]
      exit
```

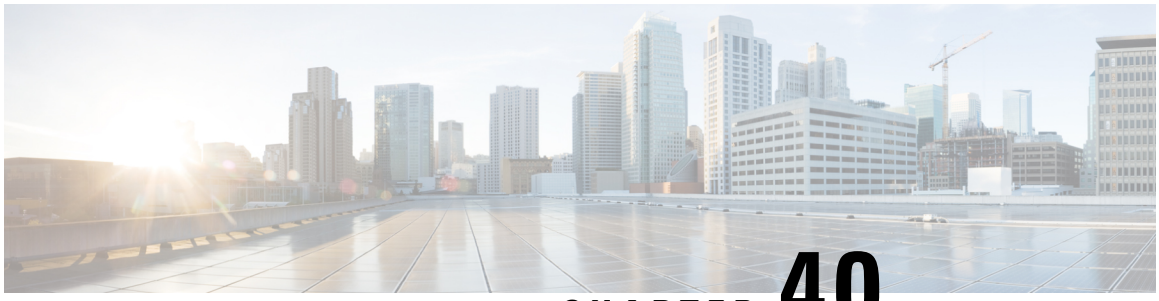
NOTES:

- **profile dnn** *dnn_name*: Enter the DNN profile configuration mode.
- **ssc-mode** *sscmode_value* **[allowed** *allowed_sscmode_value* **]**: Configure the SSC mode parameters.
  - **ssc-mode** *sscmode_value*: Specify the default SSC mode. *sscmode_value* must be an integer in the range of 1–3.

    The SMF supports only SSC mode-1.
  - **allowed** *allowed_sscmode_value*: Specify the allowed SSC modes. Up to two modes can be configured in addition to the default SSC mode. *allowed_sscmode_value* must be an integer in the range of 1–3.

    If the UEs are sent with SSC mode values defined under **allowed** command, then these values are supported along with the default SSC mode supported for the DNN profile.
- **no ssc-mode**: Specify this command to remove the SSC mode from the DNN profile.
- When UE requests SSC mode-2 or mode-3, if the UE's subscription (in order of priority: UDM or Local configuration on SMF) allows SSC mode-1 along with mode-2 or mode-3, then SMF sends PDU Session Establishment Reject with 5GSM cause 68 (Not supported SSC mode) and Allowed SSC mode as 01. This method allows the UE to retry with SSC mode-1. As per 3GPP TS 24.501, the 5GSM cause 68 is sent when the requested SSC mode is not supported by the subscription.

  To honor PDU Session Establishment, the SMF expects SSC mode either through UDM subscription or local configuration. If SMF does not have SSC mode as part of UDM subscription or local configuration, the SMF rejects PDU Session Establishment with 5GSM cause 31 (Request rejected and unspecified).



CHAPTER 40

Session Timers

- Feature Summary and Revision History, on page 1367
- Feature Description, on page 1368
- 3GPP-Compliant Timers, on page 1369
- Non-3GPP Compliant Timers, on page 1380

Feature Summary and Revision History

Summary Data

Table 427: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 428: Revision History

Revision Details	Release
Added support for session idle timers.	2023.03.0
Added support for session setup timer and back-off timer.	2021.02.0
First introduced.	2020.02.0

Feature Description

This chapter provides detailed information about the function, operation, and configuration of the timers.

The SMF supports configurable timers that are either session timers or non 3GPP session imers.

- Non 3GPP session timers
  - Absolute timer
  - Control Plane Inactive timer
  - User Plane Inactive timer
  - Session Setup timer
- 3GPP session timers
  - GTP timer
  - N11 timer
  - Back-off timer
  - Default Flow Only timer
  - EPS Fallback Guard timer
  - Indirect Data Forwarding Tunnel timer
  - Dedicated Bearer Delay and Retry timer
  - Dedicated Bearer Procedure Failure Handling timer
  - Procedure SLA timer
  - Dynamic Configuration Change Support timer
  - IPAM Quarantine timer
  - Provisioning of Policy Revalidation timer
  - Router Advertisement Parameters timer

For details on timers other than GTP and N11, see the following sections:

- EPS Fallback Guard Timer Support, on page 206
- Indirect Data Forwarding Tunnel (IDFT) Timer Support, on page 201
- Create Dedicated Bearer Delay and Retry Support, on page 254
- IPAM Quarantine Timer, on page 772
- Provisioning of Policy Revalidation Time, on page 1020
- Configuring Router Advertisement Parameters, on page 817

3GPP-Compliant Timers

GTP and N11 Timers

Feature Description

The SMF supports retransmission through the GTP and N11 timers. With this provision, when the peer does not respond with the timer value, the SMF retransmits the GTP and N11 requests. You can configure the maximum number of retransmissions through SMF.

How it Works

The SMF supports the following 3GPP timers:

GTP Retransmission Timer

The SMF or PGW-C starts the timer denoted in the T3-RESPONSE. The timer is invoked when a signalling message, for which a reply is expected, is sent. A signalling message or the triggered message may be lost if a response is not received before the T3-RESPONSE timer expires.

After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is then retransmitted if the total number of retry attempts is less than N3REQUESTS.

5G N1N2 Reattempt Timer

If AMF rejects the N1N2 MessageTransfer with cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing", then the SMF starts the timer for reattempting N1N2 MessageTransfer.

After the timer expires, the message corresponding to N1N2 MessageTransfer is reattempted based on the configured retry attempts.

Standards Compliance

The 3GPP timers support feature complies with the following standards:

- *3GPP TS 29.510 V15.2.0 (2018-12)—5G; 5G System; Network function repository services; Stage 3*

Configuring the N11 and GTP Timers

This section describes how to configure the 3GPP-compliant timers—N11 and GTP timers.

Configuring the N11 Timers

The N11 timer configuration is invoked when AMF rejects the N1N2 message transfer with the "Temporary reject registration ongoing" or "Temporary reject handover ongoing" cause code. Then, SMF considers the timer and reattempts the message transfer. When the timer expires, the transfer is reattempted based on the configured retry count.

To configure an N11 timer, use the following sample configuration:

```
config
  profile failure-handling failure_handling_name
```

```
interface [ gtpc | N11 ] message message_type
  cause-code [ temp-reject-register | temp-reject-handover ]
    action [ retry { timeout timeout_duration |
    max-retry retry_count } | clear | terminate ]
    end
```

NOTES:

- **profile failure-handling** *failure_handling_name*—Enter the name of the profile for failure handling.
- **interface [gtpc | N11]** —Configure the interface over which the message transfer must happen.
- **message** *message_type*—Configure the message type to be transferred over the interface. The N11 interface supports the message type as N1N2Transfer.
- **cause-code [temp-reject-register | temp-reject-handover]** —Configure the HTTP cause code. You can configure multiple cause code values for a message.
- **action [retry | clear | terminate]**—Configure the action to perform when the message transfer is not successful.
- **action [retry { max-retry** *retry_count* **| timeout** *timeout_duration* **}** —Specify the number of times the message transfer must be reattempted and the time interval between the consecutive attempts.

Example Configuration

Following is an example of N11 timer configuration.

```
show running-config
profile failure-handling n11-fht
  interface n11 message n1n2transfer
    cause-code temp-reject-register
     action retry
       timeout 1000
         max-retry 2
```

Configuring the GTP Timers

The GTP timer configuration is implemented when a signaling message or triggered message, for which a reply is expected, is lost as it did not get a response before the T3-RESPONSE timer expired. After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is retransmitted if the total number of retry attempts is less than the N3-REQUESTS times.

To configure a GTP timer, use the following sample configuration:

```
config
   instance instance-id gr_instance_id
      endpoint gtp
         retransmission { max-retry retry_count | timeout timeout_duration }
         end
```

NOTES:

- **endpoint gtp**—Enter the GTP retransmission configuration.
- **max-retry** *retry_count*—Specify the number of times the signalling message request to SMF must be reattempted. The accepted range is 0–5. Default range is 3. When the *retry_count* is set to "0", the retransmission feature is disabled.

- **timeout** *timeout_duration*—Configure the interval of time (in milliseconds) after which the GTP retransmission request is reattempted. The accepted range is 0–10. Default range is 2. When the *timeout_duration* is set to "0", the retransmission feature is disabled.

Example Configuration

Following is an example of GTP timer configuration.

```
show running-config
instance instance-id 1
  endpoint gtp
   retransmission max-retry 2 timeout 5
```

Back-off Timer Support

Feature Description

The SMF supports configurable back-off timer to inform the UE to wait with a re-registration and new connection attempt after a network-initiated release. This timer helps to recover the system from failure.

The SMF sends the configured back-off timer value to AMF in the following scenarios:

- N4 path failure during a UPF switchover
- IP address exhaustion

Important These scenarios are currently supported only in home-routed roaming and non-roaming sessions.

The SMF sends the back-off timer value to S-GW only during the exhaustion of IP address.

Note The back-off timer support is applicable only for the 4G non-roaming sessions and 5G roaming and non-roaming sessions.

If the SMF detects that the UPF is inactive, it includes a back-off timer and cause value in PDU Session Release Command message sent over N1. Then, SMF clears the PDU session.

When the IP addresses get exhausted while initiating the 4G attach, the PGW-C includes the back-off timer IE and cause value in Create Session Response message.

In case of IP address exhaustion during 5G attach, the SMF includes the back-off timer IE and cause value in PDU Session Establishment Reject message sent over N1.

How it Works

The SMF provides an option to configure back-off timer value with failure condition and Cause value. For configuration details, see the Configuring Back-off Timer, on page 1378 section in this guide.

The SMF detects if the UPF is down due to N4 path failure. If the UPF is down, SMF includes the configured back-off timer value and cause value in the N1 PDU Session Release Command while clearing PDU session.

In home-routed roaming scenario, vSMF includes the back-off timer and cause value in PDU Session Release Command message sent over N1 when any of the following conditions are met:

- hSMF detects that the hUPF is inactive due to path failure.
- vSMF detects that the vUPF is inactive due to path failure.

If the SMF or PGW-C detects that the IP addresses are exhausted, SMF includes the back-off timer and cause value in the N1 PDU Session Establishment Reject message or Create Session Response depending on the RAT type.

In the roaming scenario, if the hSMF detects that the IP addresses are exhausted, it sends PDU Session Create Error to vSMF with the back-off timer and cause values. Based on this value, vSMF includes the back-off timer and Cause value in N1 PDU Session Establishment Reject message.

Note Encoding of back-off timer in PDU Release Command and PDU Establishment Reject is as defined in *3GPP TS 24.008—Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*.

Encoding of back-off timer in Create Session Response is as defined in *3GPP TS 29.274—3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*.

Call Flows

This section provides the call flows for this feature.

N4 Path Failure Handling Call Flow

This section describes how the SMF handles the N4 path failures observed in non-roaming and roaming scenarios.

Handling of N4 Path Failures in Non-roaming Session

The following figure illustrates the N4 path failure handling call flow for a non-roaming session.

Figure 257: N4 Path Failure Handling Call Flow for Non-roaming Session

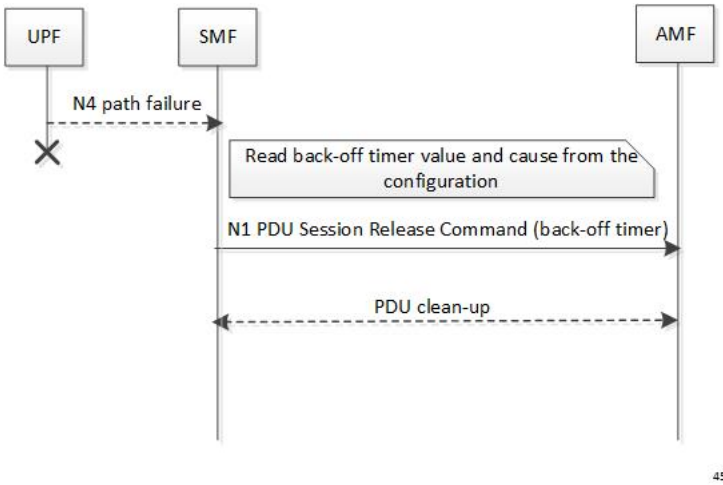


Table 429: N4 Path Failure Handling Call Flow Description for Non-roaming Session

Step	Description
1	The SMF checks if the UPF is inactive due to N4 path failure.
2	If the SMF detects that the UPF is inactive, it fetches the back-off timer and cause value from the DNN profile configuration. The SMF sends the timer and cause value in the N1 PDU Session Release Command to AMF. Then, the SMF performs the PDU clean up.

Handling of N4 Path Failures in vUPF During Roaming Session

The following figure illustrates the call flow of handling N4 path failures in vUPF during the roaming session.

Figure 258: vUPF Path Failure Handling Call Flow for Roaming Session

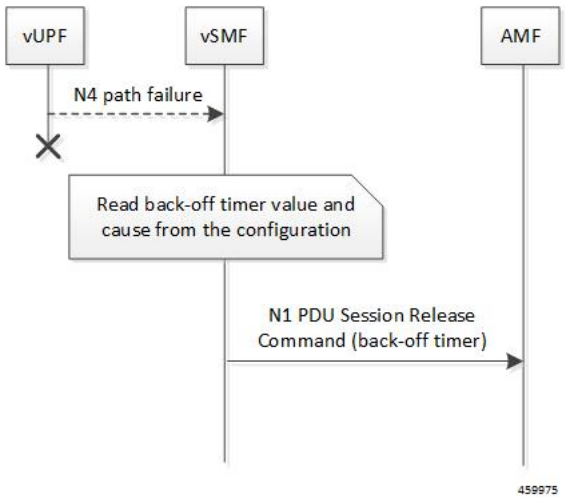


Table 430: vUPF Path Failure Handling Call Flow Description for Roaming Session

Step	Description
1	The vSMF checks if the vUPF is inactive due to N4 path failure.
2	If the vSMF detects that the vUPF is inactive, it fetches the back-off timer value and cause from the DNN profile configuration. The vSMF sends the timer and cause value in the N1 PDU Session Release Command to AMF. Then, the vSMF performs the PDU clean up.

Handling of N4 Path Failures in hUPF During Roaming Session

The following figure illustrates the call flow of handling N4 path failures in hUPF during the roaming session.

Figure 259: hUPF Path Failure Handling Call Flow for Roaming Session

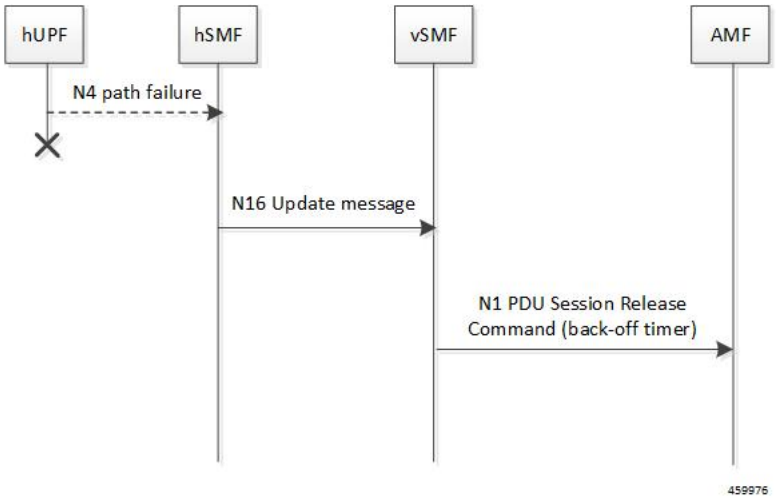


Table 431: hUPF Path Failure Handling Call Flow Description for Roaming Session

Step	Description
1	The hSMF checks if the hUPF is inactive due to N4 path failure.
2	If the hUPF is inactive, hSMF sends the back-off timer and cause to vSMF through the N16 update request.
3	The vSMF includes the back-off timer and cause value in N1 PDU Session Release Command message.

IP Address Exhaustion Handling Call Flow for 5G Sessions

This section describes how the SMF handles the IP address exhaustion condition in 5G sessions.

Handling of IP Address Exhaustion in 5G Non-roaming Sessions

The following figure illustrates the IP address exhaustion handling call flow for 5G non-roaming sessions.

Figure 260: IP Address Exhaustion Handling Call Flow for 5G Non-roaming Sessions

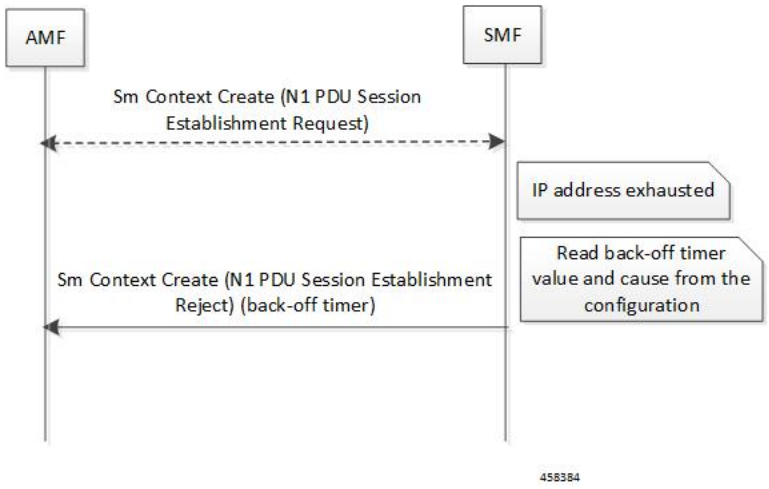


Table 432: IP Address Exhaustion Handling Call Flow Description for 5G Non-roaming Sessions

Step	Description
1	AMF sends the SM Context Create message for the N1 PDU Session Establishment Request to SMF.
2	Upon detecting the exhaustion of IP address in a 5G non-roaming call, the SMF reads the configured back-off timer and cause value. Then, SMF sends this timer and cause value in the N1 PDU Session Establishment Reject message to AMF.

Handling of IP Address Exhaustion in 5G Roaming Sessions

The following figure illustrates the IP address exhaustion handling call flow for 5G roaming sessions.

Figure 261: IP Address Exhaustion Handling Call Flow for 5G Roaming Sessions

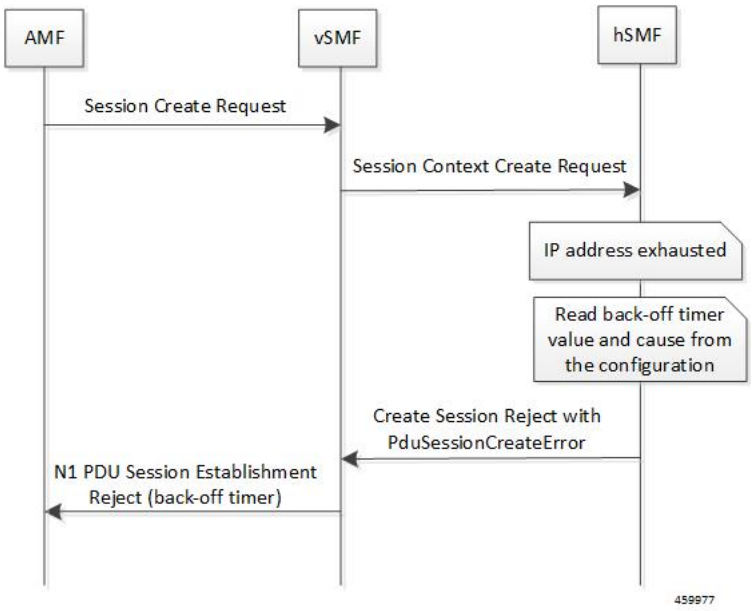


Table 433: IP Address Exhaustion Handling Call Flow Description for 5G Roaming Sessions

Step	Description
1	The AMF sends the SM Context Create message for the N1 PDU Session Establishment Request to vSMF.
2	The vSMF sends Session Context Create Request message to the hSMF.
3	If hSMF detects that the IP addresses are exhausted, it sends PduSessionCreateError to the vSMF with back-off timer and cause value based on configuration on hSMF. Based on this value, the vSMF includes the back-off timer and cause value in N1 PDU Session Establishment Reject message.

IP Address Exhaustion Handling Call Flow for 4G Sessions

This section describes how the SMF handles the IP address exhaustion condition in a 4G session.

The following figure illustrates the IP address exhaustion handling call flow for 4G sessions.

Figure 262: IP Address Exhaustion Handling Call Flow for 4G Sessions

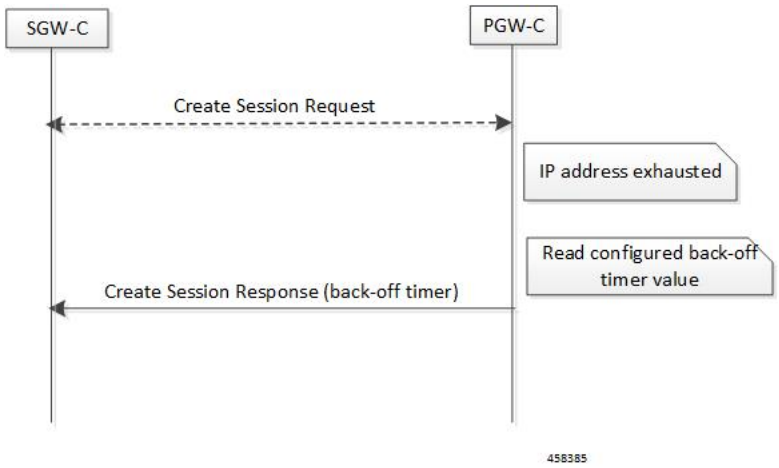


Table 434: IP Address Exhaustion Handling Call Flow Description for 4G Sessions

Step	Description
1	SGW-C sends the Create Session Request to PGW-C.
2	Upon detecting the exhaustion of IP address in a 4G call, the PGW-C reads the configured back-off timer value and cause. Then, PGW-C sends this timer value and cause in the Create Session Response message to SGW-C.

Limitations

This feature has the following limitation:

- Back-off timer triggering is not supported while clearing 4G PDN sessions as the 3GPP 29.274 specification does not support back-off timer IE in Delete Bearer Request message.

Note The preceding limitation is applicable only to the non-roaming scenarios.

Standards Compliance

The Back-off Timer Support feature complies with the following standards:

- *3GPP 29.274, version 15.9.0, Release 15—Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*
- *3GPP 24.008, version 15.9.0, Release 15—Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*
- *3GPP 24.501, version 15.6.0, Release 15—5G; Non-Access Stratum (NAS) protocol for 5G System (5GS); Stage 3*

- *3GPP TS 29.502, version 15.6.0, Release 15—5G; Session Management Services; Stage 3*

Configuring Back-off Timer

This section describes how to configure the back-off timer.

Configuring the back-off timer involves the following steps:

- Configuring Back-off and Jitter Timers in DNN Profile, on page 1378
- Enabling Message-level Back-off Timer, on page 1378

Note This feature works only when both the back-off timer and cause are configured. The back-off timer configuration remains the same for both the non-roaming and roaming calls.

Configuring Back-off and Jitter Timers in DNN Profile

To define values for the back-off and jitter timers in DNN profile, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      timeout backoff backoff_timer_value
      timeout jitter jitter_timer_value
      end
```

NOTES:

- **timeout backoff** *backoff_timer_value*: Specify the back-off timer value, in seconds. *backoff_timer_value* must be an integer in the range of 0-576000.

  The back-off timer is the maximum allowed duration used during IP exhaustion and N4 path failure cases.

- **timeout jitter** *jitter_timer_value*: Specify a jitter value to introduce randomness in the back-off timer value. *jitter_timer_value* must be an integer in the range of 0-1000.

  The jitter allows spreading the different backoff timers to the UE devices so that they all wait at different times before the next reconnection attempt.

  This configuration helps to prevent a session storm after the back-off timer expiry.

The following is an example configuration used during N4 path failure scenarios.

```
config
   profile dnn test
      timeout backoff 200 jitter 50
      end
```

Enabling Message-level Back-off Timer

Use the following sample configuration to enable the back-off timer at the GTP-C and N1 message levels.

```
config
   profile access access_profile_name
      gtpc message-handling create-session-response condition ip-exhaust
```

```
action backoff cause cause_code_value
    n1 message-handling pdu-session-release condition n4-pathfail action
backoff cause cause_code_value
     n1 message-handling pdu-session-establishment condition ip-exhaust
action backoff cause cause_code_value
     end
```

NOTES:

- **gtpc message-handling create-session-response condition ip-exhaust action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the GTP-C interface level for the Create Session Response (CSR) message. That is, the CSR message includes the Back-off Timer IE and its cause code during the exhaustion of IP address.
- **n1 message-handling pdu-session-release condition n4-pathfail action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the N1 interface level for the PDU Session Release message. That is, the PDU Session Release message includes the Back-off Timer IE and its cause code when the N4 path failure occurs.
- **n1 message-handling pdu-session-establishment condition ip-exhaust action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the N1 interface level for the PDU Session Establishment message. That is, the PDU Session Establishment message includes the Back-off Timer IE and its cause code during the exhaustion of IP address.

The following is an example configuration used during the 4G attach and the exhaustion of IP addresses.

```
config
   profile access access1
      gtpc message-handling create-session-response condition ip-exhaust
 action backoff cause 73
      end
```

In this scenario, the attach fails and the CSR is sent with Back-off Timer IE and cause 73.

The following is an example configuration used during the 5G attach and the exhaustion of IP addresses.

```
config
   profile access access1
      n1 message-handling pdu-establishment condition ip-exhaust action
backoff cause 26
      end
```

In this scenario, the attach fails and the PDU Session Establishment is sent with Back-off Timer and cause code value set to 26.

The following is an example configuration used during the 5G attach and the N4 path failure scenario.

```
config
   profile access access1
     n1 message-handling pdu-session-release condition n4-pathfail action
 backoff cause 26
      end
```

In this scenario, clear subscriber is triggered internally and PDU Session Release command is sent with Back-off Timer IE and cause 26.

Verifying the Back-off Timer Configuration

This section describes how to verify the back-off timer configuration.

Use the **show running-config** command to verify the feature configuration.

The following is an example output of the **show running-config profile access access1** command.

```
[unknown] smf# show running-config profile access access1
profile access access1
n1 message-handling pdu-establishment condition ip-exhaust action backoff cause 26
n1 message-handling pdu-release condition n4-pathfail action backoff cause 26
n26 idft enable timeout 15
n2 idft enable timeout 15
gtpc gtpc-failure-profile gtp1
gtpc message-handling create-session-response condition ip-exhaust action backoff cause 76
exit
```

The following is an example output of the **show running-config profile dnn intershat** command.

```
[unknown] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
timeout backoff 500 jitter 100
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr true
exit
```

Non-3GPP Compliant Timers

Feature Description

The SMF supports non-3GPP session timers for each PDU session. This section provides detailed information about the function, operation, and configuration of the following timers:

- Absolute Timer
- Control Plane and User Plane Idle Timer
- User Plane Inactivity timer
- Session Setup Timer

Note This section is also applicable to 4G calls with diameter interfaces.

Configuring Non-3GPP Session Timers

To configure non-3GPP session timers in the DNN profile, use the following sample configuration:

```
config
      profile dnn dnnprofile_name
            timeout absolute absolutetimer_value
            timeout { cp-idle timer_value | up-idle timer_value }
            timeout setup timeout_value
            userplane-inactivity-timer timer_value
            end
```

NOTES:

- **timeout absolute** *absolutetimer_value*—Specify the maximum duration of the session (in seconds), before the system automatically terminates the session.
  - The default value is 0, which indicates that it's a disabled function.
  - The *absolutetimer_value* must be an integer in the range of 0-2147483647.
  - The absolute session timer gets triggered during the session creation. You can't modify the timer value during the interim handling of any access and mobility procedures for that session.
  - Once the timer expires, the SMF performs the SMF-initiated release by informing all SBI interfaces and N4 Interfaces. It includes the following interfaces: UE, UDM, PCF, CHF, and UPF.
  - For 4G calls with legacy-interfaces, the SMF-initiated release will be performed by informing the following interfaces: Diameter (Gx and Gy), GTP, RADIUS, and N4 interfaces.
- **timeout cp-idle** *timer_value*—Specify the maximum duration of the 4G or the 5G session, after the migration to CP idle state and before the automatic termination.
  - The default value is 0, which indicates that it's a disabled function.
  - The *timer_value* must be an integer in the range of 0-2147483647.
- **timeout up-idle** *timer_value*—Specify the maximum duration of the 5G session, after the migration to the UP idle state and before the automatic termination.
  - The default value is 0, which indicates that it's a disabled function.
  - The *timer_value* must be an integer in the range of 0-2147483647.
- **cp-idle timer**—Starts when any 4G or 5G procedure ends. The timer stops when any new procedure starts. If the timer expires, the SMF clears the session.
- **up-idle timer**—Starts when an AN-initiated or Network-initiated 5G session enters the idle mode. The timer stops when the session exits the idle mode. On the expiry of the timer, the SMF clears the 5G sessions.
- **timeout setup** *timeout_value*—Specify the session setup timeout value in milliseconds.
  - The default value is 10000 milliseconds.
  - The *timeout_value* must be an integer in the range of 5000-60000.

- The SMF aborts the creating procedure when the call isn't complete within the configured time. It sends the PDU Session Establishment Reject or the Create Session Reject. This timer applies to 4G, 5G, and Wi-Fi sessions.
- In the 4G Create procedure, if the CSR receives Maximum Wait Time, then the procedure SLA timer sets the Maximum Wait Time. Either the guard timer or the SLA timer expires first, depending on the timeout values.

- **userplane-inactivity-timer** *timer_value*—Specify the timer value in seconds.
  - The default value of the timer is 0, which indicates that it's a disabled function.
  - The timer value must be an integer in the range of 0-86400.
  - The SMF sends the configured inactivity timer to the UPF through the N4 PDU Session Establishment request. After the session establishment, if the configured value changes, the SMF reports the changes to the UPF through the N4 modification request.
  - The UPF starts the inactivity timer when there's no uplink or downlink data transmission over the N3 /S5-U tunnel. It stops the timer when the data transmission over the N3 /S5-U tunnel is resumed.
  - On the expiry of the timer, the UPF sends the session report to the SMF with the user plane inactivity request (UPIR) flag set.
  - After receiving the report indication for a session, the SMF clears the session, when it's a 4G session, and initiates idle mode entry, when it's a 5G session.

Note Enable the **userplane-inactivity-timer** parameter for the 5G call only when the **always-on** parameter gets disabled in the respective DNN.

To disable this parameter, configure the value of **always-on** to *false*.

Configuration Example

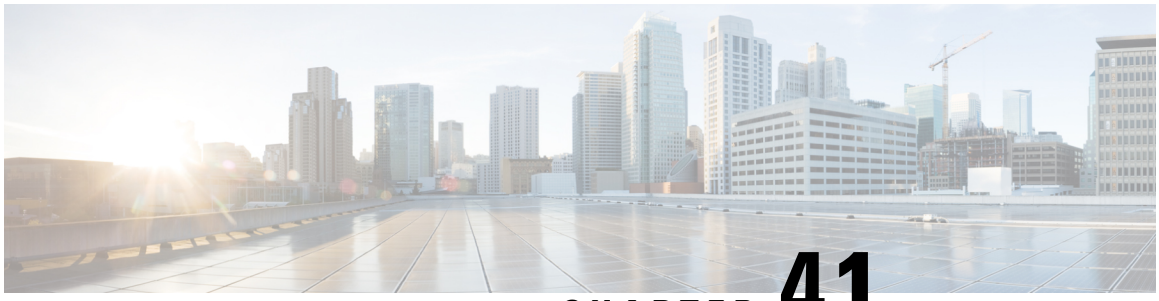
The following is an example configuration.

```
smf(config)# profile dnn intershat timeout absolute 900
```

Configuration Verification

To verify the configuration:

```
show running-config
 profile dnn intershat
 timeout absolute 900
 exit
```



CHAPTER 41

SMF Capabilities to Support 4G and 5G Devices

- Feature Summary and Revision History, on page 1383
- Feature Description, on page 1384
- How it Works, on page 1386
- Configuring Parameters to Support 4G and 5G Devices, on page 1387
- OAM Support, on page 1391
- Troubleshooting Information, on page 1393

Feature Summary and Revision History

Summary Data

Table 435: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 436: Revision History

Revision Details	Release
Periodic Secondary RAT Usage Data Report is supported from MME over S5/S8 interface in the Modify-Bearer-Request, Delete-Session-Request, Delete-Bearer-Response, and Change-Notification-Request	2023.04.0

Revision Details	Release
Added the extended QoS support for SMF with the legacy interfaces.	2023.02.0
The Phase-2 support for 4G-UE and Option-3x feature includes: • DCNR based UPF selection • Handling Secondary RAT Data Usage Report from S-GW/MME and relaying it to CHF • UE Presence Reporting • Handling GTPV1 messages for 4G to 3G handover • SUPI+IP session and affinity key for 4G and WiFi handover • Avoiding sending of 5G QoS for 4G-only UE • Handling 5GCNRS and 5GCNRI indication flags from S-GW/MME	2021.01.0
First introduced.	2020.03.0

Feature Description

Important The PGW-C term used in this chapter denotes the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The dual connectivity enabled UEs support 4G LTE and 5G NR. Such UEs send a signal to the 4G Core Network, indicating that it's a dual connectivity-enabled device.

When the Dual Connectivity New Radio (DCNR)-capable UE attempts to register in an MME, the MME sets the "UP Function Selection Indication Flags" IE with the DCNR flag set to 1 in the Create Session Request message. After the S-GW receives this IE over S11, it sends the IE over S5 to PGW-C. This IE transmission helps the SGW-C and PGW-C to select SGW-U and UPF, which supports dual connectivity with NR.

The SMF and PGW-C support Packet Data Unit (PDU) sessions from both the 4G-only capable device and the Option 3x capable device (NR and LTE radio connected to the EPC).

The SMF supports the following features and functionality:

• DCNR-based UPF Selection, on page 1385
• Secondary RAT Data Usage Report, on page 1385
• #unique_2068 unique_2068_Connect_42_section_adw_rlv_5pb
• 4G to 2G or 3G Handover, on page 1385

- Extended QoS Support with Legacy Interfaces
- SUPI+IP session and affinity key for 4G to Wi-Fi handover
- Avoiding sending of 5G QoS for 4G-only UE (QoS Rules and QoS Flow Description)
- Handling 5GCNRS and 5GCNRI indication flags from S-GW and MME

DCNR-based UPF Selection

The SMF selects DCNR supported UPF for DCNR enabled session if DCNR is configured under query parameters. DCNR isn't a mandatory query parameter for UPF selection. You can configure DCNR under the UPF Group profile.

For more information, refer to the *UPF Node Selection* section in the *Policy and User Plane Management* feature chapter.

Secondary RAT Data Usage Report

The SMF and UPF track the usage on eNB to differentiate the NR or LTE usage for NSA devices. SMF receives usage data ports on the S5 interface in various messages and reports the usage towards CHF.

The SMF handles the periodic Secondary RAT Usage Data Report from MME over the S5 or S8 interface in the Modify Bearer Request, Delete Session Request, Delete Bearer Response, and Delete Bearer Command based on the Intended Receiver PGW-C (IRPGW) flag. SMF retains the Usage-Report if IRPGW = 1.

The SMF supports multiple instances of Secondary RAT Usage Data Report IEs. It stores reports until they are sent out to CHF based on the triggers. SMF sends out the stored secondary RAT usage data report through gtpp-ep endpoint when any of the charging triggers are met. You can configure the maximum number of stored secondary RAT usage reports under Charging Profile. SMF sends the stored secondary RAT usage data report along with offline usage report when CDR is closed due to offline usage report.

Presence Reporting Area

Presence Reporting Area (PRA) is an area defined within the 3GPP packet domain for reporting UE presence within that area due to policy control and/or charging reasons. For E-UTRAN, a PRA consists of a set of neighbor or non-neighbors tracking areas, eNBs and/or cells. You can enable the PRA functionality under the DNN profile.

The two types of Presence Reporting Areas that apply to an MME pool are UE-dedicated Presence Reporting Areas and Core Network preconfigured Presence Reporting Areas. SMF supports Core Network preconfigured PRAs.

4G to 2G or 3G Handover

During 4G to 2G or 3G handover, the SMF rejects the GTPv1 message request and reattaches with 2G or 3G for nondisrupted service continuity. If SMF drops the request, it delays the handover failure and subsequent attach to 2G or 3G.

Extended QoS Support with Legacy Interfaces

When the DCNR-enabled 4G devices connect to the SMF with the legacy interfaces and the Extended-BW-NR feature is negotiated with PCRF, the SMF sends the APN-AMBR values that are greater than 4.2 Gbps towards PCRF in the extended Bit-rates AVP.

If the SMF receives APN-AMBR values greater than 4.2 Gbps in the GTP-v2 messages from S-GW and the DCNR feature isn't enabled, then the SMF limits the APN-AMBR value to 4.2 Gbps.

If the SMF receives extended QoS values from PCRF and the session isn't DCNR-enabled, then the SMF limits the APN-AMBR value to 4.2 Gbps.

How it Works

The SMF generates a PDU session ID (pdu-session-id) upon receiving a Create Session Request from the 4G-only UE. The SMF validates if the request has the EPS interworking indication without the PDU session ID in the Protocol Configuration Option. The UDM provides the interworking indication to the SMF per DNN. The SMF does not use this indication for deciding whether the UE is 5G capable.

The SMF generates a pdu-session-id based on Linked EPS Bearer Identity (LBI). For the 4G sessions, the pdu-sesion-id is LBI+64 and for the Wi-Fi sessions, the pdu-session-id is LBI+80.

The SMF allows you to configure the default NSSAI under the profile DNN. The NSSAI is part of sliceInfo IE sent in the Policy Create Request to the PCF during session creation from 4G-only UEs. If the default slice is not configured, then SMF selects one of the configured slices.

When the UE is DCNR capable, and the DCNR is enabled for the session, the SMF considers that the UE is capable of supporting dual connectivity. You can configure DCNR per DNN and other NFs, such as UPF. The S-GW notifies the DCNR support to PGW-C through the UPF Selection Indication Flags IE.

Standards Compliance

The Option 3x and 4G-Only Device feature complies with the following standards:

- *3GPP TS 23.003 [2]*
- *3GPP TS 24.301 [23]*
- *3GPP TS 29.272 [70]*
- *3GPP TS 29.274*
- *3GPP TS 29.212*

Limitations

This feature has the following limitations:

- Ultra low latency QCIs are not supported.
- PRA:
  - PRA is supported only towards PCF and not CHF.
  - PRA is applied only based on RAT type of the connecting device and not based on the device type. It is applied to both 4G and 5G devices when connected from LTE.
  - A maximum of four PRA-IDs are processed in a single PCF update message. If a PCF update has more than four PRA-IDs, then the other PRA-IDs are ignored.

- Only the PRA-ID will be sent in the "Presence Reporting Area Action" IE on S5 interface. User location information will not be sent.
- Only the PRA-ID will be sent in the "repPraInfos" IE on N7 interface. User location information will not be sent.
- PRA Set is not supported due to which "Additional PRA Information" is not supported on S5 and N7 interfaces.

- Secondary RAT Data Usage Report:
  - Supports only Option 3 and Option 3x (NR Secondary RAT) UEs on S5 interface.
  - Does not support E-UTRAN Secondary RAT on N2 interface.

Configuring Parameters to Support 4G and 5G Devices

This section describes how to configure the SMF with the capabilities to support 4G and 5G devices.

Configuring this feature involves the following steps:

- Configuring the NSSAI, on page 1387
- Enabling DCNR in DNN Profile, on page 1388
- Configuring UPF Selection, on page 1388
- Configuring Secondary RAT Usage Report, on page 1389
- Configuring Presence Reporting, on page 1390

Configuring the NSSAI

This section describes how to configure the default NSSAI in SMF, which it includes in sliceInfo IE in the Policy Create Request message. The SMF sends this message towards the PCF during the session creation from 4G-only UEs.

Use the following sample configuration to configure the default NSSAI in the SMF:

```
config
  profile dnn profile_name
    nssai { sd sd_value | sst sst_value }
    exit
```

NOTES:

- **profile dnn** *profile_name*: Specify the DNN profile name. *profile_name* must be an alphanumeric string.
- **nssai { sd** *sd_value* **| sst** *sst_value* **}**: Configure the default NSSAI.
  - **sd** *sd_value*: Specify the slice descriptor (sd). *sd_value* must be a 6-digit hex string ([0-9a-fA-F]{6} - 000000 – ffffff). For example, 1A2B3c.
  - **sst** *sst_value*: Specify the slice type (sst) value. *sd_value* must be an integer in the range of 0–255.

Enabling DCNR in DNN Profile

To enable SMF to support the DCNR capability for the sessions handled using the DNN profile, use the following sample configuration:

```
config
   profile dnn profile_name
      dcnr { false | true }
      exit
```

NOTES:

- **profile dnn** *profile_name*: Specify the DNN profile name. *profile_name* must be an alphanumeric string.
- **dcnr { false | true }**:
  - **false**: Configure the DNN profile to have DCNR flag set to false. The DCNR configuration is disabled by default.
  - **true**: Configure the DNN profile to have DCNR flag set to true.

    This configuration enables the SMF to support DCNR capability. When the DCNR capability is enabled, the UE sends the DCNR flag to indicate that it supports dual connectivity.

Configuring UPF Selection

This section describes how to enable the DCNR flag and configure the appropriate precedence for DCNR.

Defining the UPF Group

Use the following sample configuration to configure the UPF group and define DCNR in the UPF Group profile.

```
config
  profile upf-group profile_name
    dcnr { false | true }
    exit
```

NOTES:

- **profile upf-group** *profile_name*: Specify the UPF group name that must be associated to the specified UPF network configuration. *profile_name* must be an alphanumeric string.
- **dcnr { false | true }**: Configure the DCNR capability.
  - **false**: Disable support for DCNR. This is the default setting.
  - **true**: Enable support for DCNR.

Associating UPF Selection Query Parameters

Use the following sample configuration to associate the defined UPF group with the UPF network element in the DNN profile.

```
config
  profile dnn profile_name
    upf-selection-policy  upfpolicy_name
    exit
```

NOTES:

- **policy dnn** *profile_name*: Enter the DNN Profile configuration mode. *profile_name* must be an alphanumeric string.
- **upf-selection-policy** *upfpolicy_name*: Specify the name of the UPF selection policy that must be associated to the DNN profile. *upfpolicy_name* must be an alphanumeric string.

Configuring Precedence for DCNR

Use the following sample configuration to configure the appropriate precedence for DCNR in the UPF Selection Policy profile.

```
config
  policy upf-selection upf_name
    precedence precedence_num
      dcnr
      exit
    exit
```

NOTES:

- **policy upf-selection** *upf_name*: Specify the UPF policy name that must be associated with the DNN profile. *profile_name* must be an alphanumeric string.
- **precedence** *precedence_num*: Assign the precedence value to the UPF policy. *precedence_num* must be an integer in the range of 1–4.
- **dcnr**: Configure the DCNR capability.

Configuring Secondary RAT Usage Report

Use the following sample configuration to configure secondary RAT usage reports before being sent to CHF.

```
config
  profile charging profile_name
    max-secondary-rat-reports report_range
    exit
```

NOTES:

- **profile charging** *profile_name*: Enter the Charging Profile configuration mode.
- **max-secondary-rat-reports** *report_range*: Configure the maximum number of secondary RAT usage reports to trigger GTPP (Gz) or CHF update. *report_range* must be an integer in the range of 0–50. Default value: 0.

Configuring Presence Reporting

Use the following sample configuration to configure presence reporting.

```
config
  profile dnn dnnprofile_name
    presence-reporting { false | true }
    exit
```

NOTES:

- **profile dnn** *dnnprofile_name*: Enter the DNN Profile Configuration mode.
- **presence-reporting { false | true }**: Configure presence reporting for the DNN.
  - **false**: Disable presence reporting. This is the default setting.
  - **true**: Enable presence reporting.

Configuration Verification

To verify the configuration, use the following command:

show subscriber supi *supi_id* **nf-service smf**

In the output of the preceding show command, check the value associated with the field "dncr". This field displays one of the following values:

- Enabled
- None
- UE Requested and Enabled

If the feature is configured, then the "dcnr" field displays "Enabled".

The following configuration is an example output of the **show subscriber supi nf-service smf** command:

```
unknown] smf# show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
"subResponses": [
{
"status": true,
"genericInfo": {
……
},
"sScMode": 1,
"chargEnabled": true,
"uetimeZone": "+00:15+1",
"allocatedIp": "209.165.201.12",
"eUtranLocation": {
"ecgi": {
"mcc": "123",
"mnc": "456",
"eutraCellId": "1234567"
},
"tai": {
"mcc": "123",
"mnc": "456",
```

```
"tac": "1820"
}
},
"alwaysOn": "None",
"dcnr": "Enabled",
……
"policySubData": {
 "TotalDynamicRules": 3,
……
Presence Information: "Enabled",
 "praIdList": [  -> list of all enabled PRA IDs
          "8388608",  Status = IN
          "8388618" Status = OUT
        ]
 },
```

OAM Support

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF uses the "dcnr" label in the session gauge "smf_session_counter" and "smf_service_stats" for collecting the DCNR session count. When the SMF session is DCNR supported, the "dcnr" label value is enabled. The label does not support non-DCNR sessions.

The following is a sample query to count the active DCNR SMF sessions:

```
nts{action_type="rejected",app_name="smf",cluster="smf",data_center="unknown",
failure_type="hdr_decode_failure",hdr_decode_fail_reason="",instance_id="0",interface_type="
",message_type="",reject_cause="",service_name="gtpc-ep"} 2
```

```
smf_session_counter: sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)
```

```
smf_service_stats: sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)
```

```
smf_session_counters{ presence-reporting ="enable"}) by (presence-reporting)
```

DCNR Session Count

For DCNR, Session Count supports the "dcnr" label in the existing session gauge "smf_session_counter". If the SMF session is a DCNR session, then the "dcnr" label value is "enable", otherwise it is "disable" for DCNR session.

The following is a sample query to count the DCNR active SMF sessions:

```
sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)
```

For DCNR statistics, the existing "smf_service_stats" counter supports the "dcnr" label. For DCNR sessions, this counter pegs the following labels and values:

- Attempt Statistics – dcnr= "enable" and status= "attempted"
- Success Statistics – dcnr= "enable" and status= "success"
- Failure Statistics – dcnr= "enable" and status= "failures"

The following is a sample query for DCNR statistics:

```
sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)
```

Secondary RAT Data Usage Reports

The Secondary-Rat-Data-Usage-Reports support the "smf_secondary_rat_usage_report_stats" counter. Labels for these statistics include ebi, qfi, rat_type, reason, service_name, and status. This counter pegs with the following labels and values:

- ebi=ebi-val
- qfi=qfi-val
- rat_type=NR
- reason=success/failure
- service_name=smf-service
- status=ReceivedFromSgw/SentToChf

The following is a sample query for DCNR statistics:

```
sum (smf_secondary_rat_usage_report_stats”) by (qfi, status, reason)
```

Presence Reporting

For Presence Reporting, Session Count supports the "pra" label in the existing session gauge "smf_session_counter". If the SMF session has presence reporting enabled, then the "presence-reporting" label value is "enable" else it is "none" if presence reporting is not enabled.

The following is a sample query to count the DCNR active SMF sessions:

```
sum (smf_session_counters{ pra ="enable"}) by (pra)
```

For Presence Reporting, statistics support the "presence-reporting" label in the existing counter "smf_service_stats". For presence-reporting session, this counter pegs the following labels and values:

- Attempt Statistics – pra = "enable" and status= "attempted"
- Success Statistics – pra = "enable" and status= "success"
- Failure Statistics – pra = "enable" and status= "failures"

The following is a sample query for DCNR statistics:

```
sum (smf_session_stats{ pra ="enable"}) by (pra, status, reason)
```

Bulk Statistics

The Option 3x and 4G-Only Device feature supports the following bulk statistics in SMF schema:

Bulk Statistics Name	Statistics Type	Trigger	Description
smf_session_counters	Gauge	Increments or decrements for session attach or detach.	Indicates the total number of currently active SMF sessions. You can filter the active session using labels, such as "dcnr=enable" for the DCNR session count.

Bulk Statistics Name	Statistics Type	Trigger	Description
smf_session_stats	Counter	Increments for success or failures of the call flow.	Indicates the statistics for call flow states such as attempted, success, and failures. You can filter the statistics using labels, such as “dcnr=enable” for only DCNR statistics.
The Secondary RAT Data Usage Report functionality supports the following bulk statistics:			
smf_secondary_rat_usage_ report_stats	Counter	Increments for the status of the secondaryRatDataUsage Report processing.	Displays the statistics for secondaryRatUsageReports processing for call flow status such as "ReceivedFromSgw" and "SentToCHF". You can filter the statistics using labels, such as reason and QFI.
OFCS_CDR_MESSAGE_STATS	Counter		A new label "Trigger Type" captures the event when a configured Secondary RAT usage limit is reached. The trigger type label contains 'SECONDARY_RAT_USAGE_LIMIT_REACHED' value.
The PRA functionality supports the following bulk statistics:			
smf_session_counters	Gauge	Increments or decrements for session attach or detach.	Indicates the total number of current active SMF sessions. You can filter the session using labels, such as "pra=enable" for the presence reporting enabled session count.
smf_session_stats	Counter	Increments for success or failures of the call flow.	Indicates the statistics for call flow states such as attempted, success, and failures. You can filter the statistics using labels, such as “pra=enable” for only presence-reporting statistics.

Troubleshooting Information

This section provides information on using the command line interface (CLI) commands, alerts, logs, and metrics for troubleshooting issues that may arise during system operation.

Subscriber Details with DCNR and Presence Reporting Enabled

The **show subscriber nf-service smf supi** *supi_id* **full** CLI command displays the DCNR active session with presence reporting enabled for the Option-3x feature.

Note In 2021.02 and later releases, the **namespace** keyword is deprecated and replaced with the **nf-service** keyword.

```
[unknown] smf# show subscriber nf-service smf supi imsi-310260789012345 full

subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-310260789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "fast.t-mobile.com",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
…
        "alwaysOn": "None",
        "dcnr": "Enabled",
        "wps": "Non-Wps Session",
        "ratType": "EUTRA",
        "ueType": "NR Capable UE",
        "iwkEpsInd": true,
        "sessTimeStamp": "2021-01-12 12:40:39.931012285 +0000 UTC",
        "callDuration": "4m25.36784895s",
        "ipPool": "poolv4",
        "commonId": 16777223,
        "linkedEbi": 5,
        "smfIwkEpsInd": true,
        "snssai": {
          "sd": "Abf123",
          "sst": 1
        },
        "authStatus": "Unauthenticated",
        "roamingStatus": "Roamer",
        "uePlmnId": {
          "mcc": "310",
          "mnc": "260"
        }
      },
      "policySubData": {
        "TotalDynamicRules": 2,
        "TotalFlowCount": 2,
        "TotalNonGBRFlows": 1,
        "TotalGBRFlows": 1,
        …
        "presenceReporting": "Enabled",
        "praList": [
          {
            "praId": "0x80000b",
            "presenceState": "Inactive"
```

```
            },
            {
              "praId": "0x800000",
              "presenceState": "InArea"
            },
            {
              "praId": "0x80000a",
              "presenceState": "OutOfArea"
            }
          ]
        },
        …
        }
      }
    ]
}
```

Option-3x: DCNR Enabled UE Alerts

This section describes the alerts supported for DCNR enabled UEs with presence-reporting enabled. You can enhance these alerts as per 4G procedure or as per the intent of the end user.

Examples of DCNR statistics or gauges are pdn_sess_create, pdn_inter_sgw_handover, pdn_mbr, pcf_req_ded_brr_mod, pcf_req_ded_brr_create, pcf_req_ded_brr_delete, delete_session_request, smf_initiated_pdn_detach, ue_req_pdn_sess_rel, and so on.

DCNR UE Attach Failure Threshold Alert

Use the following example to configure alerts related to DCNR UE Attach Failure Threshold.

```
alerts rules group DCNRUEs
 rule DCNR_UE_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\",
procedure_type=\"pdn_sess_create\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", dcnr =\"enable\", rat_type!=\"EUTRA\",
status=\"attempted\", procedure_type=\"pdn_sess_create\"}[5m])) < 0.10"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when attach success rate of DCNR enabled UE lesser than
threshold"
  exit
 exit
```

DCNR UE Attach Failure Threshold Alert with Presence Reporting

Use the following example to configure alerts related to DCNR UE Attach Failure Threshold with presence reporting enabled.

```
rule DCNR_UE_PRA_ENABLE_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\", procedure_type=\"pdn_sess_create\",
 pra=\"enable\"}[5m])) / sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr =\"enable\", rat_type!=\"EUTRA\", status=\"attempted\",
procedure_type=\"pdn_sess_create\", pra=\"enable\"}[5m])) < 0.10"
  severity   major
  type       "Communications Alarm"
  annotation summary
   value "This alert is fired when attach success rate of DCNR enabled UE and presence
```

```
reporting enabled lesser than threshold "
  exit
 exit
```

DCNR UE Bulk Statistics

Use the following SMF service bulk statistics to monitor the failures or issues associated with DCNR UEs.

Table 437: DCNR UE

Bulk Statistics Name	Query	Description
4G_DCNRUE_Attempted	bulk-stats query 4G_DCNRUE_Attempted expression "sum(smf_service_stats {dcnr='enable',status='attempted', rat_type='EUTRA'}) by (namespace)" exit	
4G_DCNRUE_Success	bulk-stats query 4G_DCNRUE_Success expression "sum(smf_service_stats {dcnr='enable',status='success', rat_type='EUTRA'}) by (namespace)" exit	
4G_PRA_ENABLE_Attempted	bulk-stats query 4G_PRA_ENABLE_Attempted expression "sum(smf_service_stats {pra='enable',status='attempted', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit	
4G_PRA_ENABLE_Success	bulk-stats query 4G_PRA_ENABLE_Success expression "sum(smf_service_stats {pra='enable',status='success', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit	

Option-3x Device Specific Error Logs

This section provides the basic error conditions and logs that are captured to debug the failures for the Option-3x feature.

DCNR Disabled UE or 4G capable UE only

The following example displays the error log for DCNR disabled UE or 4G capable UE only.

```
2021/01/24 10:11:22.648 smf-service [ERROR] [GenericGtpMsg.go:1811] [smf-service.smf-app.sgw]
 secRatUsageRpt recvd wrongly for DNCR disbled UE, ignoring report

2020/12/19 13:17:17.834 smf-service [ERROR] [GenericGtpMsg.go:1834] [smf-service.smf-app.sgw]
 secRatUsageRpt recvd wrongly for 4gOnly UE, ignoring report
```

Secondary RAT Usage with invalid EBI

The following example displays the error log for secondary RAT usage with invalid EBI.

```
2021/01/24 11:38:18.917 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
 Secondary Rat Data Usage Report Recvd
2021/01/24 11:38:18.917 smf-service [WARN] [IntMethods.go:137] [smf-service.Policy.gen] Qos
 Flow not found with EBI [8]
2021/01/24 11:38:18.917 smf-service [ERROR] [GenericGtpMsg.go:1853] [smf-service.smf-app.sgw]
  Qfi invalid in secRatUsageRpt
```

Secondary RAT Usage invalid RAT Type

The following example displays the error log for secondary RAT usage with invalid RAT type.

```
2021/01/24 11:42:21.474 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
 Secondary Rat Data Usage Report Recvd
2021/01/24 11:42:21.474 smf-service [ERROR] [GenericGtpMsg.go:1861] [smf-service.smf-app.sgw]
  Rat type invalid in secRatUsageRpt
```

Secondary RAT Usage with intended PGW set to zero

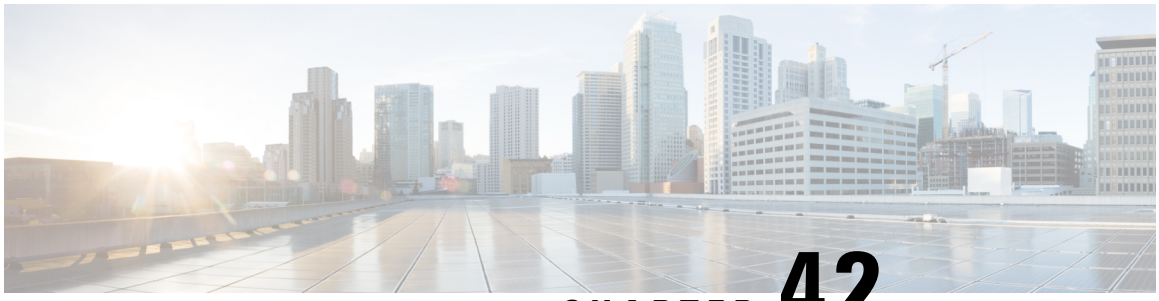
The following example displays the error log for secondary RAT usage with intended P-GW set to zero (IRPGW:0).

```
2021/01/24 11:33:10.390 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
 Secondary Rat Data Usage Report Recvd
2021/01/24 11:33:10.390 smf-service [ERROR] [GenericGtpMsg.go:1865] [smf-service.smf-app.sgw]
  secRatUsageRpt.IRPGW is false
```

PRA ID received greater than four

The following example displays the error log when PRA ID received is greater than four.

```
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_types.go:659] [smf-service.Policy.gen]
 praConfig:true for dnn:fast.t-mobile.com
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388608
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 8388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388619
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
Max 4 PRAs allowed, ignoring the PRA-ID (8388608) from PCF
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
Max 4 PRAs allowed, ignoring the PRA-ID (8388619) from PCF
```



CHAPTER 42

SMF Serviceability

- Feature Summary and Revision History, on page 1399
- Feature Description, on page 1400
- How it Works, on page 1401
- Call Failure Logs, on page 1405
- Procedure Failure Logs, on page 1406
- Generic Procedure Failure Logs, on page 1409
- Additional Call Flow Failure Logs, on page 1410
- Event Trace Logs, on page 1413
- Call Flow Statistics Logs, on page 1417
- Core Dump Utility Logs, on page 1418
- Monitor Subscriber (MonSub) Logs, on page 1420
- N40 Additional Logs and Statistics, on page 1424
- N7 Additional Logs and Statistics, on page 1425

Feature Summary and Revision History

Summary Data

Table 438: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 439: Revision History

Revision Details	Release
First introduced.	2023.01.0

Feature Description

The SMF logs and serviceability feature perform in the following modes:

- It helps and captures capabilities to enable limited debug logs in the production with a chain of troubleshooting tools.
- These further help in improving the time taken in finding a root cause of any issue found during the production.

This feature allows the operator to enable specific LogTag to debug call failures and procedure failures, to facilitate a better RCA in the production. It has the following characteristics:

- The SMF must provide a tool or utility to generate core dumps that help in downloading and investigating the problem further.
- The SMF must print the SUPI of the failed subscriber along with the error details in the logs.
- The required subscriber information MonSub helps in debugging a particular subscriber.

Relationships

The following modules are associated with this feature:

- Call Failure Logs, on page 1405
- Procedure Failure Logs, on page 1406
- Generic Procedure Failure Logs, on page 1409
- Additional Call Flow Failure Logs, on page 1410
- Event Trace Logs, on page 1413
- Call Flow Statistics Logs, on page 1417
- Core Dump Utility Logs, on page 1418
- Monitor Subscriber (MonSub) Logs, on page 1420
- N40 Additional Logs and Statistics, on page 1424
- N7 Additional Logs and Statistics, on page 1425

How it Works

This section describes how this feature works.

Log Instances

The log instance generates messages, used for identifying issues, deployment status, and performance tuning. The application infrastructure provides a common way to enable log messages across applications. Each log instance has the following:

- Timestamp
- Log message
- Log level
- LogTag

LogTag

The LogTag is used as a filter to enable or disable the specific type of log messages. Before or during the logging session, they are precreated, evaluated, and exempted. It consists of the following:

- Module name
- Component name
- Interface name

Creating a LogTag

The following is a sample example of creating a LogTag:

```
common.LogTagN7RestEp = appCtx.RegisterLogTag("rest_ep", "app", "n7")
```

Logging a Message

The following is a sample example of a LogTag message logging:

```
appCtx.Info(common.LogTagN7RestEp, "Starting rest-ep app")
```

Log Levels

The application infrastructure provides upto six variants of log levels, which can be used as filter along with LogTag to enable or disable specific logs. Each level represents the level of importance of a log message, which can be used while troubleshooting. The following table lists log levels and their usage:

Table 440: Log Levels

Log Levels	Usage
Error	Used when there's incorrectness leading to serious issues.
Warning	Used to notify and warn, when there's an occurrence of any of the following scenarios: • Something serious is about to happen. • If there's an activity which is erroneously running • Continuously giving error notes • Not attended scenarios
Info	Used for normal expected behavior such as starting an application or stopping the same, and so on.
Debug	Used to provide more information required to debug problems.
Trace	Used to provide extensive information. Also, used in monitoring routines, where the same debug log keeps coming periodically.
Off	Used when there isn't any meaning in the logging information. Configured in the CLI to turn off or turn on the logging activity.

Log Level Order

Every time, the application infrastructure logs any log message, it matches the log level, and the LogTag with the configured log setting, before logging.

Table 441: Log Levels

Log Levels (Order)	Usage
Error (0)	Matches error logs.
Warn (1)	Matches warn and error logs.
Info (2)	Matches info, warn, and error logs.
Debug (3)	Matches debug, info, warn, and error logs.
Trace (4)	Matches trace, debug, info, warn, and error logs.
Off (5)	Matches no log to disable errors.

SMF Logs

The SMF supports operators to enable specific LogTag. The following is a list of modules which support the implementation of this feature.

1. **Call Failure LogTag:**
    - Enabled in the CLI mode
    - The SMF must enable the following logs based on the disconnect reason:
        - Error
        - Warning
        - Debug
    - It prints the following log parameters:
        - Transaction ID
        - Disconnect reason
        - Event Trace
        - Session Keys
        - Error Category (For major disconnect reason)

2. **Procedure Failure LogTag**:
    - Enabled in the CLI mode
    - The SMF must enable the following logs based on the disconnect reason:
        - Warning
    - It prints the following log parameters:
        - Transaction ID
        - Procedure Name
        - Event Trace
        - Detailed Error: It includes the following:
            - Failure reason or cause
            - Disconnect reason (if applicable)
            - Failure metrics

3. **Additional Call Flow Failure LogTag**:
    - Enabled for specific reasons or conditions
    - It prints the following log parameters:
        - Transaction ID

- Event Trace
- Call flow-specific error messages

- The supported log levels:
  - Error
  - Warning
  - Info
  - Debug

4. **Additional Generic Procedure Failure LogTag**:
   - Enabled in the CLI mode
   - The SMF must not enable the Event Trace based on the disconnect reason.
   - If the operator needs failure logs for all procedures, then the operator can enable this LogTag.

Note The operator needs to activate this LogTag carefully, as it prints logs of all failed procedures. This action can cause an overflow of service logs.

   - It prints the following log parameters:
     - Transaction ID
     - Procedure Name
     - Detailed Error: It includes the following:
       - Failure reason or cause
       - Disconnect reason (if applicable)
       - Failure metrics

5. **Call Flow Statistics LogTag**:
   - This process gets tabulated at the end of all procedures.

6. **Core Dump LogTag**:
   - This process initiates the debugging activities for a core dump utility.

7. **Subscriber Monitoring LogTag**:
   - This process initiates the debugging activities for any kind of failures. It also processes the subscriber monitoring based on the subscriber SUPI.

Timesaver For more information, see *Troubleshooting Information* > Logs, on page 1621.

Call Failure Logs

The following are the synopsis of the Call Failure logs to trigger session management policies towards the SMF:

- For call failures and call releases, the disconnect-reason-based statistics are defined and attached.
- Disconnect Reasons—They are classified into three categories as the following:
  - Major
  - Minor
  - Normal
- On call failure or call release scenarios, messages are logged as the following:
  - Major (Catastrophic) Category Disconnect Reasons—The transaction log at Error level is to display the Error category, Disconnect reason, along with Event Trace, and Session keys.
  - Minor (Critical) Category Disconnect Reasons—The transaction log at Warning level to dump the Disconnect reason, along with Event Trace, and Session keys.
  - Normal Category Disconnect Reasons—The transaction log at Debug level to dump the Disconnect reason along with the Event Trace and Session keys.
  - Graceful Core Dump—This transaction log also gets performed with the same LogTag and levels.
- A new LogTag to log the Call Failures also gets defined.
- The Transaction ID gets printed in a Call Failure logs to align with the logs and call flow.
- Based on the disconnect reason statistics, the callfailure tag with the corresponding log level can be enabled to collect further information of the session. The following is a list of examples:
  - Event Trace
  - Session keys
  - Core Dump

Sample Dump for Call Failure Logs

The following is a sample dump for Call Failure logs:

Example: For a procedure lapsed time of over two seconds, a Warning message gets logged with the event trace.

```
2022/08/23 11:10:31.222 [WARN] [smf-service.smf-app.callfailure-debug] 2sec Time Elapsed:
EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
```

```
CurIndex:[2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                           |PROC INST |TXN ID    |TIMESTAMP                          |
|1    |N11SmContextCreateReq               |INCOMING_EVENT       |PDU Session Establishment
                           |1         |1         |2022-08-23 11:10:31.215 +0530 IST  |
|2    |N11SmContextCreateReq               |ENDPROC_EVENT        |PDU Session Establishment
                           |1         |1         |2022-08-23 11:10:31.221 +0530 IST  |
```

Configuring the Call Failure Logs

To configure this feature, use the following configuration:

logging name smf-service.smf-app.callfailure-debug level application/transaction <debug level>

NOTES:

- **Warning**—The logging level supported for call failure LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
config
   logging name smf-service.smf-app.callfailure-debug level transaction warn
   logging name smf-service.smf-app.callfailure-debug level application error
exit
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.callfailure-debug
 logging name smf-service.smf-app.callfailure-debug level application error
 logging name smf-service.smf-app.callfailure-debug level transaction warn
```

Procedure Failure Logs

The following are the synopsis of the Procedure Failure logs to trigger session management policies towards the SMF:

- During the termination scenario, each Procedure Failure log turns on the EndProcedure.
- During the failure scenario, the Error Code returns to the SMF Infra indicating whether the procedure was a success or a failure.
- On failure, a Transaction log (common to all procedures) with level warning is used to dump the session details as the following:
  - Event Trace
  - Procedure Name

  - Error Details—It contains failure reason or cause, disconnect reason (if applicable) and failure metrics.

- The Procedure Failure LogTag is common to all procedures.
- Procedure-specific LogTags will be configured for each procedure and used to enable logging for specific procedure failures.
- The Transaction ID gets printed in a procedure failure logs to align with the logs and call flow.
- The detailed errors note gets printed in the procedure failure logs. It helps in understanding the problem, the actual error cause, disconnect reason (if applicable), and failure metrics.

Logging a Message for Procedure Failure Logs

The following is a sample example of a LogTag for Procedure Failure logs:

```
2023/01/15 11:34:30.002 [WARN] [smf-service.smf-app.pdnsetup-procfailure]
[Txn :7]Procedure=[PDN Connect [LTE]], PduState=[IDLE], Rat-Type=[rat_type_unknown],
FailureReason=[udm_subscribe_notify_failure],
DisconnectReason=[disc_pdnsetup_udm_sub_notify_resp_failed]
2023/01/15 11:34:30.002 [WARN] [smf-service.smf-app.pdnsetup-procfailure] [Txn :7]EVENT
TRACE
CurIndex:[8], CurProcInst:[0], CreateTimeStamp:[2022-09-13 11:34:27.942 +0000 UTC],
BaseTimeStamp:[2022-09-13 11:34:27.942 +0000 UTC]

|INDEX|EVENT NAME |EVENT TYPE |PROC NAME |PROC INST |TXN ID |TIMESTAMP |

|1 |S5S8CreateSessReq |INCOMING_EVENT |PDN Connect [LTE] |1 |7 |2022-09-13 11:34:27.942
+0000 UTC |
|2 |N10RegistrationSuccess |INCOMING_EVENT |PDN Connect [LTE] |1 |7 |2022-09-13 11:34:27.943
 +0000 UTC |
```

Configuring the Procedure Failure Logs

To configure this feature, use the following configuration:

```
logging  name  smf-service.smf-app.pdusetup-procfailure          level
transaction <debug level>
logging  name  smf-service.smf-app.pdnsetup-procfailure   level
transaction <debug level>
logging  name  smf-service.smf-app.pdurelease-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.pdndisconnect-procfailure       level
  transaction <debug level>
logging  name  smf-service.smf-app.5gim-procfailure
 level          transaction <debug level>
logging  name  smf-service.smf-app.xnho-procfailure
 level          transaction <debug level>
logging  name  smf-service.smf-app.n2ho-procfailure
level   transaction <debug level>
logging  name  smf-service.smf-app.nrtowifiho-procfailure
level   transaction <debug level>
```

```
logging  name  smf-service.smf-app.enbtowifiho-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.wifitonrho-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.wifitoenbho-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.4gdedbrr-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.pdnmodmbr-procfailure            level
  transaction <debug level>
logging  name  smf-service.smf-app.5gmodify-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.5g4gho-procfailure
level  transaction <debug level>
logging  name  smf-service.smf-app.n26ho-procfailure
 level          transaction <debug level>
```

NOTES:

- **Warning**—The logging level supported for procedure failure LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
config
  logging name smf-service.smf-app.4gdedbrr-procfailure level transaction warn
  logging name smf-service.smf-app.5g4gho-procfailure level transaction warn
  logging name smf-service.smf-app.5gim-procfailure level transaction warn
  logging name smf-service.smf-app.5gmodify-procfailure level transaction warn
  logging name smf-service.smf-app.enbtowifiho-procfailure level transaction warn
  logging name smf-service.smf-app.n26ho-procfailure level transaction warn
  logging name smf-service.smf-app.n2ho-procfailure level transaction warn
  logging name smf-service.smf-app.nrtowifiho-procfailure level transaction warn
  logging name smf-service.smf-app.pdndisconnect-procfailure level transaction warn
  logging name smf-service.smf-app.pdnmodmbr-procfailure level transaction warn
  logging name smf-service.smf-app.pdnsetup-procfailure level transaction warn
  logging name smf-service.smf-app.pdurelease-procfailure level transaction warn
  logging name smf-service.smf-app.pdusetup-procfailure level transaction warn
  logging name smf-service.smf-app.wifitoenbho-procfailure level transaction warn
  logging name smf-service.smf-app.wifitonrho-procfailure level transaction warn
  logging name smf-service.smf-app.xnho-procfailure level transaction warn
exit
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name
 logging name smf-service.smf-app.4gdedbrr-procfailure level transaction warn
 logging name smf-service.smf-app.5g4gho-procfailure level transaction warn
 logging name smf-service.smf-app.5gim-procfailure level transaction warn
 logging name smf-service.smf-app.5gmodify-procfailure level transaction warn
 logging name smf-service.smf-app.enbtowifiho-procfailure level transaction warn
 logging name smf-service.smf-app.n26ho-procfailure level transaction warn
 logging name smf-service.smf-app.n2ho-procfailure level transaction warn
 logging name smf-service.smf-app.nrtowifiho-procfailure level transaction warn
```

```
logging name smf-service.smf-app.pdndisconnect-procfailure level transaction warn
logging name smf-service.smf-app.pdnmodmbr-procfailure level transaction warn
logging name smf-service.smf-app.pdnsetup-procfailure level transaction warn
logging name smf-service.smf-app.pdurelease-procfailure level transaction warn
logging name smf-service.smf-app.pdusetup-procfailure level transaction warn
logging name smf-service.smf-app.wifitoenbho-procfailure level transaction warn
logging name smf-service.smf-app.wifitonrho-procfailure level transaction warn
logging name smf-service.smf-app.xnho-procfailure level transaction warn
```

Generic Procedure Failure Logs

The following are the synopsis of the Generic Procedure Failure logs to trigger session management policies towards the SMF:

- During the termination scenario, each Procedure Failure log turns on the EndProcedure.
- During the failure scenario, the Error Code returns to the SMF Infra indicating whether the procedure was a success or a failure.
- On failure, a Generic Transaction log (common to all procedures) with level warning is used to dump the session details as the following:
  - Transaction ID
  - Procedure Name
  - Detailed Error—It contains failure reason or cause, disconnect reason (if applicable) and failure metrics.
- The Generic Procedure Failure LogTag is common to all procedures.
- When a specific procedure failure LogTag is disabled and a Generic Procedure Failure LogTag is enabled, then the SMF doesn't print the Event Trace.
- The Event Trace is printed, only when a specific procedure failure LogTag gets enabled.
- The Transaction ID gets printed in a procedure failure logs to align with the logs and call flow.
- The Detailed errors note gets printed in the generic procedure failure logs. It helps in understanding the problem, the actual error cause, disconnect reason (if applicable), and failure metrics.

Logging a Message for Generic Procedure Failure Logs

The following is a sample example of a LogTag for Generic Procedure Failure logs:

```
2023/01/15 10:58:01.171 [WARN] [smf-service.smf-app.procfailure] [Txn :1]Procedure=[PDN
Connect [LTE]],
PduState=[IDLE], Rat-Type=[rat_type_unknown], FailureReason=[udm_subscribe_notify_failure],

DisconnectReason=[disc_pdnsetup_udm_sub_notify_resp_failed]
```

Configuring the Generic Procedure Failure Logs

To configure this feature, use the following configuration:

logging name smf-service.smf-app.procfailure level transaction <debug level>

NOTES:

- **Warning**—The logging level supported for generic procedure failure LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
config
 logging name smf-service.smf-app.procfailure level transaction warn
exit
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.procfailure
logging name smf-service.smf-app.procfailure level transaction warn
```

Additional Call Flow Failure Logs

The following are the synopsis of the Additional Call Flow Failure logs to trigger session management policies towards the SMF:

- Extra LogTags are added for specific procedures.
- These LogTags can be enabled for specific conditions between the procedure flow.
- The Additional Call Flow Failure logs help in identifying a procedure lapsed event and reciprocate with a logged warning message in the event trace.

Sample Dump for Additional Call Flow Failure Logs

The following is a sample dump for Additional Call Flow Failure logs:

Example: For a procedure lapsed time of over two seconds, a warning message gets logged with the event trace.

```
2022/08/23 11:10:31.222 [WARN] [smf-service.smf-app.5gmodify-failure] 2sec Time Elapsed:
EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                           |PROC INST |TXN ID    |TIMESTAMP                          |
```

Logging a Message for Additional Call Flow Failure Logs

The following is a sample example of a LogTag for Additional Call Flow Failure logs:

```
2022/08/23 11:10:31.222 [WARN] [smf-service.smf-app.5gmodify-failure] 2sec Time Elapsed:
EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[2], CurProcInst:[0], CreateTimeStamp:[2022-08-23 11:10:31.204 +0530 IST],
BaseTimeStamp:[2022-08-23 11:10:31.204 +0530 IST]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                          |PROC INST |TXN ID    |TIMESTAMP                          |
```

Configuring the Additional Call Flow Failure Logs

To configure this feature, use the following configuration:

```
Logging name smf-service.smf-app.4gdedbrr-failure level transaction <debug
 level>
logging      name     smf-service.smf-app.pdnmodmbr-failure     level
  transaction     <debug level>
logging      name     smf-service.smf-app.5gmodify-failure          level
     transaction     <debug level>
logging      name     smf-service.smf-app.5g4gho-failure            level
     transaction     <debug level>
logging      name     smf-service.smf-app.n26ho-failure             level
     transaction     <debug level>
logging      name     smf-service.smf-app.wifi-nr-ho
level     transaction     <debug level>
logging      name     smf-service.smf-app.datacheck       level
transaction     <debug level>
logging      name     smf-service.smf-app.N16             level
transaction     <debug level>
logging      name     smf-service.smf-app.erir             level
transaction     <debug level>
logging      name     smf-service.smf-app.flagdb            level
transaction     <debug level>
logging     name     smf-service.smf-app.dcr        level     transaction
     <debug level>
logging      name     smf-service.smf-app.dcr-ue        level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-dup       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-mme       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-pcf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-ubr       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-absent      level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-amf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-chf      level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-gnb       level
transaction     <debug level>
```

```
logging      name     smf-service.smf-app.dcr-brr-smf       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-udm       level
transaction     <debug level>
logging      name     smf-service.smf-app.dcr-brr-ue       level
transaction     <debug level>
logging      name     smf-service.smf-app.epsfb        level
transaction     <debug level>
```

NOTES:

- **Warning**—The logging level supported for additional call flow failure LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
config
  logging name smf-service.smf-app.4gdedbrr-failure level transaction warn
  logging name smf-service.smf-app.5g4gho-failure level transaction warn
  logging name smf-service.smf-app.5gmodify-failure level transaction warn
  logging name smf-service.smf-app.N16 level transaction warn
  logging name smf-service.smf-app.datacheck level transaction warn
  logging name smf-service.smf-app.dcr level transaction warn
  logging name smf-service.smf-app.dcr-brr-absent level transaction warn
  logging name smf-service.smf-app.dcr-brr-amf level transaction warn
  logging name smf-service.smf-app.dcr-brr-chf level transaction warn
  logging name smf-service.smf-app.dcr-brr-dup level transaction warn
  logging name smf-service.smf-app.dcr-brr-gnb level transaction warn
  logging name smf-service.smf-app.dcr-brr-mme level transaction warn
  logging name smf-service.smf-app.dcr-brr-pcf level transaction warn
  logging name smf-service.smf-app.dcr-brr-smf level transaction warn
  logging name smf-service.smf-app.dcr-brr-ubr level transaction warn
  logging name smf-service.smf-app.dcr-brr-udm level transaction warn
  logging name smf-service.smf-app.dcr-brr-ue level transaction warn
  logging name smf-service.smf-app.dcr-ue level transaction warn
  logging name smf-service.smf-app.epsfb level transaction warn
  logging name smf-service.smf-app.erir level transaction warn
  logging name smf-service.smf-app.flagdb level transaction warn
  logging name smf-service.smf-app.n26ho-failure level transaction warn
  logging name smf-service.smf-app.pdnmodmbr-failure level transaction warn
  logging name smf-service.smf-app.wifi-nr-ho level transaction warn
end
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name
 logging name smf-service.smf-app.4gdedbrr-failure level transaction warn
 logging name smf-service.smf-app.5g4gho-failure level transaction warn
 logging name smf-service.smf-app.5gmodify-failure level transaction warn
 logging name smf-service.smf-app.N16 level transaction warn
 logging name smf-service.smf-app.datacheck level transaction warn
 logging name smf-service.smf-app.dcr level transaction warn
 logging name smf-service.smf-app.dcr-brr-absent level transaction warn
 logging name smf-service.smf-app.dcr-brr-amf level transaction warn
 logging name smf-service.smf-app.dcr-brr-chf level transaction warn
 logging name smf-service.smf-app.dcr-brr-dup level transaction warn
```

```
logging name smf-service.smf-app.dcr-brr-gnb level transaction warn
logging name smf-service.smf-app.dcr-brr-mme level transaction warn
logging name smf-service.smf-app.dcr-brr-pcf level transaction warn
logging name smf-service.smf-app.dcr-brr-smf level transaction warn
logging name smf-service.smf-app.dcr-brr-ubr level transaction warn
logging name smf-service.smf-app.dcr-brr-udm level transaction warn
logging name smf-service.smf-app.dcr-brr-ue level transaction warn
logging name smf-service.smf-app.dcr-ue level transaction warn
logging name smf-service.smf-app.epsfb level transaction warn
logging name smf-service.smf-app.erir level transaction warn
logging name smf-service.smf-app.flagdb level transaction warn
logging name smf-service.smf-app.n26ho-failure level transaction warn
logging name smf-service.smf-app.pdnmodmbr-failure level transaction warn
logging name smf-service.smf-app.wifi-nr-ho level transaction warn
```

Event Trace Logs

The following are the synopsis of the Event Trace logs to trigger session management policies towards the SMF:

- Event Trace logs provide an execution sequence for a session. It represents the following:
  - Message Type
  - Event Type—Incoming or Outgoing or Internal submitted event type.
  - Procedure Type and Procedure Instance—Where the message is associated with.
  - Txn ID—Where the message is associated with.
  - Timestamp—For the same message associated with
- Event Trace logs also describe other events as the following:
  - Local2DB—When the session details are derived into a primitive structure.
  - DB2Local—When the session details aren't derived from DB to Session DS.
  - Procedure Events—When it conveys the END or SUSPEND or ABORT or CLEANUP events also.

Sample Dump for Event Trace Logs

The following is a sample dump for Event Trace logs:

```
2020/09/10 13:16:16.177 smf-service [DEBUG] [Genericutil.go:5739]
[smf-service0.smf-app.event-trace] EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[31], CurProcInst:[1], CreateTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC],
BaseTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC]
|INDEX|EVENT NAME                          |EVENT TYPE           |PROC NAME
                          |PROC INST |TXN ID    |TIMESTAMP                          |

|1    |N11SmContextCreateReq               |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.503 +0000 UTC  |
|2    |N10RegistrationRequest              |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.525 +0000 UTC  |
|3    |N10RegistrationSuccess              |INCOMING_EVENT       |PDU Session Establishment
```

```
                            |1          |1776      |2020-09-10 13:16:15.605 +0000 UTC  |
|4    |N10SubscriptionFetchReq            |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1776      |2020-09-10 13:16:15.606 +0000 UTC  |
|5    |N10SubscriptionFetchSuccess        |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1776      |2020-09-10 13:16:15.644 +0000 UTC  |
|6    |N10SubscribeForNotificationReq     |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1776      |2020-09-10 13:16:15.65 +0000 UTC   |
|7    |N10SubscribeForNotificationSuccess |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1776      |2020-09-10 13:16:15.67 +0000 UTC   |
|8    |NIntSelfTxnPduSetup                |INTERNAL_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.67 +0000 UTC   |
|9    |Message Type None                  |LOCAL_2_DB           |Unknown
                            |0          |0         |2020-09-10 13:16:15.671 +0000 UTC  |
|10   |N11SmContextCreateSuccess          |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1776      |2020-09-10 13:16:15.711 +0000 UTC  |
|11   |NIntSelfTxnPduSetup                |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|12   |N7SmPolicyCreateReq                |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|13   |N7SmPolicyCreateSuccess            |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.797 +0000 UTC  |
|14   |NmgrRersourceMgmtRequest           |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.805 +0000 UTC  |
|15   |NmgrRersourceMgmtResponse          |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.814 +0000 UTC  |
|16   |N7SmPolicyUpdateReq                |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.823 +0000 UTC  |
|17   |N7SmPolicyUpdateSuccess            |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.853 +0000 UTC  |
|18   |N40ChargingDataReq                 |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.854 +0000 UTC  |
|19   |N40ChargingDataSuccess             |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.912 +0000 UTC  |
|20   |N4SessionEstablishmentReq          |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.921 +0000 UTC  |
|21   |N4SessionEstablishmentSuccess      |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.986 +0000 UTC  |
|22   |N11EbiAssignmentReq                |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.99 +0000 UTC   |
|23   |N11EbiAssignmentRsp                |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.017 +0000 UTC  |
|24   |N11N1N2MessageTransferReq          |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.021 +0000 UTC  |
|25   |N11N1N2MessageTransferSuccess      |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.096 +0000 UTC  |
|26   |Message Type None                  |LOCAL_2_DB           |Unknown
                            |0          |0         |2020-09-10 13:16:16.096 +0000 UTC  |
|27   |N11SmContextUpdateReq              |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.111 +0000 UTC  |
|28   |N4SessionModificationReq           |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.114 +0000 UTC  |
|29   |N4SessionModificationSuccess       |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.155 +0000 UTC  |
|30   |N4GtpuRouterAdvertisementReq       |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.156 +0000 UTC  |
```

```
|31   |N4SessionModificationSuccess       |ENDPROC_EVENT        |PDU Session Establishment
                          |1         |1778      |2020-09-10 13:16:16.175 +0000 UTC  |
```

Logging a Message for Event Trace Logs

The following is a sample example of a LogTag for Event Trace logs:

```
2020/09/10 13:16:16.177 smf-service [DEBUG] [Genericutil.go:5739]
[smf-service0.smf-app.event-trace] EVENT TRACE SessionKeys[[imsi-123456789012345:5 (pk)]]
CurIndex:[31], CurProcInst:[1], CreateTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC],
BaseTimeStamp:[2020-09-10 13:16:15.503 +0000 UTC]
|INDEX|EVENT NAME                         |EVENT TYPE           |PROC NAME
                          |PROC INST |TXN ID    |TIMESTAMP                           |

|1    |N11SmContextCreateReq              |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.503 +0000 UTC  |
|2    |N10RegistrationRequest             |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.525 +0000 UTC  |
|3    |N10RegistrationSuccess             |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.605 +0000 UTC  |
|4    |N10SubscriptionFetchReq            |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.606 +0000 UTC  |
|5    |N10SubscriptionFetchSuccess        |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.644 +0000 UTC  |
|6    |N10SubscribeForNotificationReq     |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.65 +0000 UTC   |
|7    |N10SubscribeForNotificationSuccess |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.67 +0000 UTC   |
|8    |NIntSelfTxnPduSetup                |INTERNAL_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.67 +0000 UTC   |
|9    |Message Type None                  |LOCAL_2_DB           |Unknown
                          |0         |0         |2020-09-10 13:16:15.671 +0000 UTC  |
|10   |N11SmContextCreateSuccess          |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1776      |2020-09-10 13:16:15.711 +0000 UTC  |
|11   |NIntSelfTxnPduSetup                |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|12   |N7SmPolicyCreateReq                |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.712 +0000 UTC  |
|13   |N7SmPolicyCreateSuccess            |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.797 +0000 UTC  |
|14   |NmgrRersourceMgmtRequest           |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.805 +0000 UTC  |
|15   |NmgrRersourceMgmtResponse          |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.814 +0000 UTC  |
|16   |N7SmPolicyUpdateReq                |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.823 +0000 UTC  |
|17   |N7SmPolicyUpdateSuccess            |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.853 +0000 UTC  |
|18   |N40ChargingDataReq                 |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.854 +0000 UTC  |
|19   |N40ChargingDataSuccess             |INCOMING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.912 +0000 UTC  |
|20   |N4SessionEstablishmentReq          |OUTGOING_EVENT       |PDU Session Establishment
                          |1         |1777      |2020-09-10 13:16:15.921 +0000 UTC  |
|21   |N4SessionEstablishmentSuccess      |INCOMING_EVENT       |PDU Session Establishment
```

```
                            |1          |1777      |2020-09-10 13:16:15.986 +0000 UTC  |
|22   |N11EbiAssignmentReq                |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:15.99 +0000 UTC   |
|23   |N11EbiAssignmentRsp                |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.017 +0000 UTC  |
|24   |N11N1N2MessageTransferReq          |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.021 +0000 UTC  |
|25   |N11N1N2MessageTransferSuccess      |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1777      |2020-09-10 13:16:16.096 +0000 UTC  |
|26   |Message Type None                  |LOCAL_2_DB           |Unknown
                            |0          |0         |2020-09-10 13:16:16.096 +0000 UTC  |
|27   |N11SmContextUpdateReq              |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.111 +0000 UTC  |
|28   |N4SessionModificationReq           |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.114 +0000 UTC  |
|29   |N4SessionModificationSuccess       |INCOMING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.155 +0000 UTC  |
|30   |N4GtpuRouterAdvertisementReq       |OUTGOING_EVENT       |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.156 +0000 UTC  |
|31   |N4SessionModificationSuccess       |ENDPROC_EVENT        |PDU Session Establishment
                            |1          |1778      |2020-09-10 13:16:16.175 +0000 UTC  |
```

Configuring the Event Trace Logs

To configure this feature, use the following configuration:

logging name smf-service.smf-app.event-trace level transaction debug-level

NOTES:

- **Warning | Error**—The logging level supported for Event Trace LogTags.
- **Session Keys | Procedure Name | Event Trace**—The logging level parameters supported for Event Trace LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
logging name smf-service.smf-app.event-trace level transaction warn
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.event-trace
logging name smf-service.smf-app.event-trace level transaction warn
```

Call Flow Statistics Logs

The following are the synopsis of the Call Flow Statistics Logs to trigger session management policies towards the SMF:

- Currently, each call flow has the following general labels and other specific labels:
  - Attempted
  - Success
  - Failure + Reason
- All the call flow statistics gets integrated with EndProcedure.
- Each DispositionEnd used to end the call flow in the procedure, concludes either as a success or a failure scenario. Each failure scenario has a reason for integration as well.
- Failure causes can be classified into different levels. They are further mapped and classified as the following:
  - Major or Error
    - Internal Error—All internal errors due to which the call flow is failing, are categorized as error.
    - Transaction Timeout Error—On interfaces, outbound response timeouts (transaction timeouts) are categorized as errors.
  - Minor or Warning
    - Server Error—On interfaces, outbound responses with the http status code 5xx (server errors) are categorized as a warning.
    - Client Error—On interfaces, inbound responses with the http status code 4xx (client errors) or timeouts are categorized as a warning.
  - Normal
    - Server Error—On interfaces, inbound responses with the http status code 5xx (server errors) are categorized as normal.
    - Client Error—On interfaces, outbound responses with http status code 4xx (client errors) are categorized as normal.
- Unknown—Those scenarios, where the call flow gets failed, but the reason doesn't get populated, fall under the unknown cause.
- Further, these scenarios can be enhanced to cases, other statistics labels of statistics, which get integrated to empty statuses.

  Example: RAT type integrated as empty, DNN type not integrated, and so on.

Configuring the Call Flow Statistics Logs

To configure this feature, use the following configuration:

logging name smf-service.smf-app.stats-debug level transaction debug-level

NOTES:

- **Warning | Error**—The logging level supported for call flow statistics LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
logging name smf-service.smf-app.stats-debug level transaction warn
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.stats-debug
logging name smf-service.smf-app.stats-debug level transaction warn
```

Core Dump Utility Logs

The following are the synopsis of the Core Dump Utility Logs to trigger session management policies towards the SMF:

- The Core Dump Utility logs provide functionality to conditionally generate a core dump for debugging purposes.
- The core file generation doesn't kill the process and it continues to execute as usual.
- The core dump functionality is disabled by default and it needs to be enabled by specifying the appropriate configurable parameters.

Important The core dump generation is a performance impacting activity. Hence, it's recommended to restrict the core dump to a minimum number, such as one or two core dumps for every 15 minutes. As a result, you need to fine-tune the core dump, if you see any performance impact.

Logging a Message for Core Dump Utility Logs

The following is a sample example of a LogTag for Core Dump Utility Logs:

```
2022/10/14 09:14:38.809 [WARN] [smf-service.smf-app.pdusetup-procfailure] [Txn Id: 3] {PDU
 Session Establishment} -> COREDUMP ->
Generating Core: current core count 1,
File:/opt/workspace/smf-service/src/smf-service/procedures/pdusetup/procedure.go:612
2022/10/14 09:15:38.817 [WARN] [smf-service.smf-app.pdusetup-procfailure] {PDU Session
```

```
Establishment} -> COREDUMP ->
Generating Core: current core count 2,
File:/opt/workspace/smf-service/src/smf-service/procedures/generic/CallFailureDebug.go:70
```

Configuring the Core Dump Utility Logs

To configure this feature, use the following configuration:

```
config
   dump core [ count count_number | interval interval_details | expires
expires_details | pod-name pod_name | file-detail file_detail ]
   end
```

NOTES:

- **count** *count_number*—Specify the maximum number of times the core dump can be taken. Example: Two core dumps can be taken in a span of 15 minutes, where two is the count. Range: 0-50
- **interval** *interval_details*—Specify the total duration of the interval (in minutes) to take the core dumps. Example: Two cores can be taken in a span of 15 minutes, where 15 minutes is the total interval time to take two core dumps. Range: 1-3600
- **expires** *expires_details*—Specify the time after which a core agent stops generating a core dump. Format: CCYY-MM-DDTHH:MM:SS, with an example: 2020-03-24T23:15:00+05:30 or 2022-10-17T19:00:00+00:00
- **pod-name** *pod_name*—List the name of the pod to enable core dump activities.
- **file-detail** *file_detail*—List the file name, line number to a specific core dump. Example: Procedures or PDUIM or procedure.go:1902, the maximum size is 10.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
dump core count 2 interval 15 expires pod-name [ smf-service-n0-0 smf-service-n0-1 ]
file-detail [ procedures/generic/CallFailureDebug.go:70 procedures/pdusetup/procedure.go:612
 ]
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config dump core
dump core
count 2 interval 15 expires 2023-01-18T18:00:00-00:00 pod-name [ smf-service-n0-0
smf-service-n0-1 ] file-detail [ procedures/generic/CallFailureDebug.go:70
procedures/pdusetup/procedure.go:612 ]
exit
```

Monitor Subscriber (MonSub) Logs

The following are the synopsis of the Monitor Subscriber (MonSub) Logs to trigger session management policies towards the SMF:

- The logs help to control the logging level of transaction logs, when the monitor subscriber CLI gets enabled.
- The Monitor Subscriber CLI captures the transaction logs for a given SUPI or IMSI.
- The Monitor Subscriber Logger uses a specific logging level, used for the subscriber, for which the monitor subscriber CLI gets triggered.
- The SMF must support per-subscriber monitoring activities. If required, it must be used to monitor a particular subscriber based on the appropriate configurable parameters, such as SUPI or IMSI.
- As a default value, the monitor subscriber functionality is disabled. It gets enabled manually by specifying the appropriate configurable parameters.

Logging a Message for MonSub Logs

The following is a sample example of a LogTag for MonSub Logs:

```
smf# monitor subscriber imsi 123456789012345 capture-duration 3600 transaction-logs yes
internal-messages yes
Fri Oct 14 09:05:53.902 UTC+00:00
supi: imsi-123456789012345
captureDuration: 3600
enableInternalMsg: true
enableTxnLog: true
namespace(deprecated. Use nf-service instead.): none
nf-service: none
gr-instance: 0
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 318 100 116 100 202 12888 22444 --:--:-- --:--:-- --:--:-- 35333
Command: --header Content-type:application/json --request POST --data

{"commandname":"mon_sub",
"parameters":{"supi":"imsi-123456789012345",
"duration":3600,"enableTxnLog":true,"enableInternalMsg":true,
"action":"start","namespace":"none","nf-service":"none",
"grInstance":0}} http://oam-pod:8879/commands
Result start mon_sub,
fileName
->logs/monsublogs/none.imsi-123456789012345_WithTxnLogs_TS_2022-10-14T09:05:53.926268924.txt
Starting to tail the monsub messages from
file:
logs/monsublogs/none.imsi-123456789012345_WithTxnLogs_TS_2022-10-14T09:05:53.926268924.txt
Defaulted container "oam-pod" out of: oam-pod, apache
Transaction Log received from Instance: SMF.nodemgr.DC.SMF.1
************* TRANSACTION: 00166 *************
```

```
TRANSACTION SUCCESS:
Start Time : 2022/10/14 09:07:24.449
GR Instance ID : 1
Txn Type : GtpcAssocEstReq(2114)
Priority : 1
Session Namespace : none(0)
CDL Slice Name : 1
LOG MESSAGES:
2022/10/14 09:07:24.449 [TRACE] [infra.message_log.core] >>>>>>>>
IPC message
Name: GtpcAssocEstReq
MessageType: GtpcAssocEstReq
Key:
--body--


{"IPv4address":167844075,"restart_counter":65535,
"nodemgr_instance_id":1,"timestamp":1665738444,
"gtpcPathStatus":2,"gtpcInterfaceType":4,"ddnInfo":{},
"gr_instance_id":1,"isNodeStarted":true}
2022/10/14 09:07:24.449 [DEBUG] [nodemgr1.app.Int] GetSessionNamespace for txn id: 166,
Type: 2114
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] Received New GTP Peer info
[&GtpcAssocEstReq{IPv4Address:167844075,IPv6Address:[],SupportedFeatures:0,RestartCounter:65535,
NodemgrInstanceId:1,Timestamp:1665738444,OverloadControl:nil,GtpcPathStatus:GTPC_PATH_UP,
GtpcInterfaceType:4,DdnInfo:&DdnInfo{DelayValid:false,ThrottleValRcvd:false,ThrottleActive:false,
DelayValue:0,ThrottleDelayValue:0,ThrottleDelayUnit:0,ThrottleFactor:0,},GrInstanceId:1,
IsNodeStarted:true,SelfRCVal:0,PeerType:0,DeletedAt:0,}]
2022/10/14 09:07:24.449 [INFO] [nodemgr.gtpmgr.gtp] GTPC Path Mgmt Disabled for interface
[4]
2022/10/14 09:07:24.449 [INFO] [nodemgr.gtpmgr.gtp] Rcvd timestamp 1665738444, stored
timestamp 1665738177
peer 10.1.24.235
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] Assoc req for already present peer
[10.1.24.235]
2022/10/14 09:07:24.449 [DEBUG] [nodemgr.gtpmgr.gtp] stop timer for existing gtp-peer
[10.1.24.235]
2022/10/14 09:07:24.451 [TRACE] [infra.message_log.core] <<<<<<<<


**********************************************
Transaction Log received from Instance: SMF.nodemgr.DC.SMF.1
************* TRANSACTION: 00167 *************
TRANSACTION SUCCESS:
Start Time : 2022/10/14 09:07:34.061
GR Instance ID : 1
Txn Type : GtpcAssocEstReq(2114)
Priority : 1
Session Namespace : none(0)
CDL Slice Name : 1
LOG MESSAGES:
2022/10/14 09:07:34.062 [TRACE] [infra.message_log.core] >>>>>>>>
IPC message
Name: GtpcAssocEstReq
MessageType: GtpcAssocEstReq
Key:
--body--
```

```
{"IPv4address":167844075,"restart_counter":100,"timestamp":1665738454,"gtpcInterfaceType":4,
"ddnInfo":{},"isNodeStarted":true}
2022/10/14 09:07:34.062 [DEBUG] [nodemgr1.app.Int] GetSessionNamespace for txn id: 167,
Type: 2114
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] Received New GTP Peer info
[&GtpcAssocEstReq{IPv4Address:167844075,IPv6Address:[],SupportedFeatures:0,RestartCounter:100,
NodemgrInstanceId:0,Timestamp:1665738454,OverloadControl:nil,GtpcPathStatus:GTP_PATH_INVALID,
GtpcInterfaceType:4,DdnInfo:&DdnInfo{DelayValid:false,ThrottleValRcvd:false,ThrottleActive:false,
DelayValue:0,ThrottleDelayValue:0,ThrottleDelayUnit:0,ThrottleFactor:0,},GrInstanceId:0,
IsNodeStarted:true,SelfRCVal:0,PeerType:0,DeletedAt:0,}]
2022/10/14 09:07:34.062 [INFO] [nodemgr.gtpmgr.gtp] GTPC Path Mgmt Disabled for interface
[4]
2022/10/14 09:07:34.062 [INFO] [nodemgr.gtpmgr.gtp] Rcvd timestamp 1665738454,
stored timestamp 1665738444 peer 10.1.24.235
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] Assoc req for already present peer
[10.1.24.235]
2022/10/14 09:07:34.062 [DEBUG] [nodemgr.gtpmgr.gtp] stop timer for existing gtp-peer
[10.1.24.235]
2022/10/14 09:07:34.065 [TRACE] [infra.message_log.core] <<<<<<<<

*********************************************
```

Configuring the Monitor Subscriber Logs

To configure this feature, use the following configuration:

```
config
   monitor subscriber [ supi supi_id | imsi imsi_value | imei imei_id |
capture-duration capture_duration | dump dump_name | gr-instance gr_instance_id |
 internal-messages internal_messages | list list_details | namespace namespace_details
 | nf-service nf_service_details | transaction-logs transaction_logs ]
   end
```

NOTES:

- **supi** *supi_id*—Specify the subscriber identifier. For example, imsi-123456789, imsi-123*
- **imsi** *imsi_value*—Specify the subscriber IMSI. For example: 123456789, *
- **imei** *imei_id*—Specify the subscriber IMEI. For example: 123456789012345, *
- **capture-duration** *capture_duration*—Specify the duration in seconds during which the monitor subscriber activity gets captured. The default is 300 seconds (five minutes). It's an optional parameter.
- **dump** *dump_filename*—Specify the name of the dump filename. Example: monitor subscriber-dump [filename]
- **gr-instance** *gr_instance_id*—Specify the GR instance ID. It's an optional parameter. It's a monitor subscriber for the given gr-instance only. The instance ID 1 denotes the local instance ID.
- **internal-messages** *internal_messages*—When set to yes, it enables internal messaging. By default, a disabled value It's an optional parameter.
- **list** *list_details*—Specify the details of the list. It includes the monitor subscriber list files.

- **namespace** *namespace_details*—Enable the specified namespace. By default, the namespace is set to none. It's an optional parameter.

Note A deprecated keyword in the release 2021.02.0 and replaced with nf-service as the keyword

- **nf-service** *nf_service_details*—Enable the specified NF service. By default, nf-service is set to none. It's a mandatory parameter. The possible values: sgw, smf, pgw

Note The nf-service keyword replaces the namespace keyword in the release 2021.02 and onwards.

- **transaction-logs** *transaction_logs*—Enable transaction logs when set to yes. By default, a disabled value. It's an optional parameter.

Note To view the transaction history logs, use the dump transaction history command. The latest transaction logs get stored in a circular queue of size 1024 transaction logs.

- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Important The MonSub needs subscriber SUPI or IMSI in monitor subscriber command. The following are important actions:

- As a prerequisite, the SMF must print the subscriber SUPI or IMSI in the logs.
- Currently, SMF transaction logs are printing subscriber session keys which include subscriber SUPI or IMSI in the transcation logs.
- The operator can pick the subscriber SUPI or IMSI from these logs.

Configuration Example

The following is an example configuration.

```
logging level monitor-subscriber info
logging name infra.message_log.core level monitor-subscriber debug
```

Configuration Verification

To verify the configuration:

```
smf# show running-config logging
logging level monitor-subscriber info
logging name infra.message_log.core level monitor-subscriber debug
```

N40 Additional Logs and Statistics

The following are the synopsis of the additional logs and statistics for N40 to trigger session management policies towards the SMF:

- Enhances the current message-level statistics for rest-ep consisting of extra LogTag or labels, as the following:
  - DNN type
  - RAT type
  - PDN type
  - Procedure type
  - Types of error cause, when there are errors.
  - Interface failure
- When the current message-level statistics get enhanced, the redundant statistics from the SMF-Service such as Message-level statistics can be removed, as the rest-ep already consists of the same message.
- The problems and their details can be updated for all the CHF-initiated messages as the following:
  - Notify
  - For Abort
  - Re-Auth
- The transaction logging levels and the LogTag for the additional logs and statistics for N40 must be in sync. In the event of a failure scenario, the applicable LogTag for N40 must be added. They are as the following:
  - Major (Error)
  - Minor (Warning)
  - Normal (Info)
- When the logging level gets enabled with the corresponding category, the following options are available:
  - Event Trace
  - Core Dump

Configuring the N40 Additional Logs and Statistics

To configure this feature use the following configuration:

```
logging name smf-service.smf-app.chf level transaction debug-level
```

NOTES:

- **Warning | Error**—The logging level supported for the N40 additional logs and statistics LogTags.

- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

The following is an example configuration.

```
logging name smf-service.smf-app.chf level transaction warn
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.chf
logging name smf-service.smf-app.chf level transaction warn
```

N7 Additional Logs and Statistics

The following are the synopsis of the additional logs and statistics for N7 to trigger session management policies towards the SMF:

- It detects HTTP error codes for the PCF initiated update notification and terminate messages containing problem details.
- Enhances the current message-level statistics for rest-ep consisting of extra LogTag or labels, as the following:
  - DNN type
  - RAT type
  - PDN type
  - Procedure type
  - Types of error cause, when there are errors.
  - Interface failure
- The transaction logging levels and LogTag for the additional logs and statistics for N7 must be in sync. They are as the following:
  - Error
  - Warning
  - Info
- When the logging level gets enabled with the corresponding category, the following options are available:
  - Event Trace
  - Core Dump

Configuring the N7 Additional Logs and Statistics

To configure this feature, use the following configuration:

`logging name smf-service.smf-app.pcf level transaction debug-level`

NOTES:

- **Warning | Error**—The logging level supported for N7 additional logs and statistics LogTags.
- For more information, see *Troubleshooting Information* > Logs, on page 1621.

Configuration Example

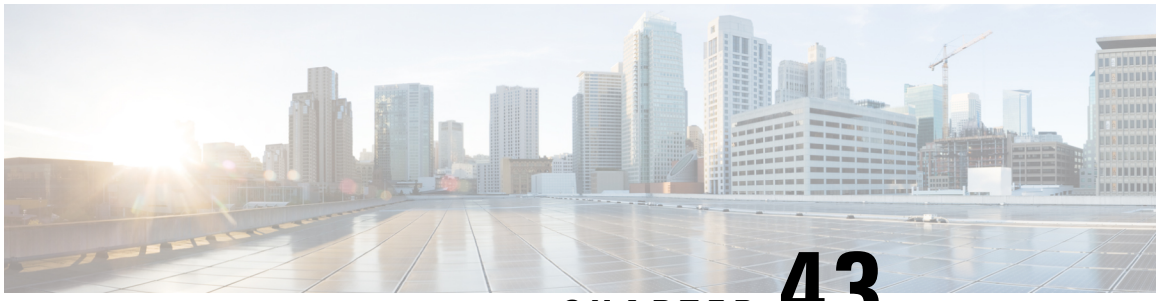
The following is an example configuration.

```
logging name smf-service.smf-app.pcf level transaction warn
```

Configuration Verification

To verify the configuration:

```
[smf] smf# show running-config logging name smf-service.smf-app.pcf
logging name smf-service.smf-app.pcf level transaction warn
```



CHAPTER 43

Subscriber Charging

- Feature Summary and Revision History, on page 1427
- Feature Description, on page 1428
- Mapping of Charging Scenario on Various Interfaces, on page 1455
- Failure Handling Scenarios, on page 1461
- Dynamic Update of Charging Configurations, on page 1468

Feature Summary and Revision History

Summary Data

Table 442: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platforms	SMI
Feature Default Setting	• Subscriber Charging: Disabled – Configuration Required. • Final Unit Indication for Gy Interface: Disabled – Configuration Required to Enable.
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 443: Revision History

Revision Details	Release
Added Gz interface details for subscriber charging.	2023.04.0

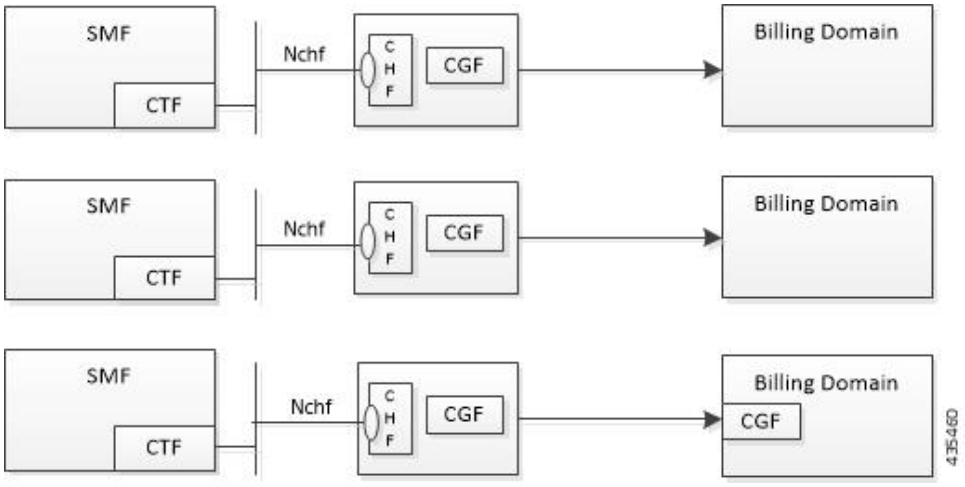
Revision Details	Release
Added support for the following features: • Added the dynamic change in configuration of APN, ECS, and Charging profile. • Gz Usage Report Handling with GTPP. • Added Support for Final Unit Indication for Gy Interface.	2023.03.0
Added support for the following features: • Charging Disable functionality • Processing QoS Descriptor for Static and Predefined Rules	2023.01.0
Added support for extension in Charging Characteristics ID range values.	2021.02.3.t3
Added support for Query Interface IE.	2021.02.0
Introduced support for reconciliation of billing records when CHF is unreachable.	2021.02.0
Added session-level limitations on the N4 interface.	2021.01.1
Introduced support for the following: • Zero Usage Report Suppression • Dynamic ACS Configuration Change	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF acts as a Charging Transfer Function (CTF). The CTF generates charging events toward the Charging Function (CHF), which is responsible for generating Charging Data Records (CDRs).

This SMF interacts with various interfaces, such as N40, Gy, N4, N7, and N10, facilitating charging in entirety. SMF uses the Nchf/N40 , Online Chargig System (OCS)/Gy , and Offline Charging System (OFCS)/Gz interfaces to generate charging events.

Figure 263: SMF as a Charging Transfer Function



The SMF Charging feature supports the following functionality.

- Converged Online and Offline charging.
- PDU session charging using the service-based interface.
- Network slice instance charging.
- Charging information collection per PDU session for UEs served under 3GPP and non-3GPP access (untrusted non-3GPP access, trusted non-3GPP access and wireline).

Note OCS/OFCS charging behaviour is applicable to the SMF 4G session when the SMF configuration has DNN profile with network element profiles for OCS/OFCS.

- Unique identity number assignment per PDU session for billing purposes.
- Separate count of data volumes on both the uplink and downlink directions. The data volumes reflect the data as delivered to and forwarded from the user.
- Charging mechanism that provides the date and time information when the PDU session starts.
- Handling of Charging Characteristics specific to a subscription or a subscribed DNN.
- Identification of data volumes, elapsed time, or events for individual service data flows (flow-based charging). One PCC rule identifies one service data flow.
- Usage reporting of a service, a detected application per rating group, or per combination of the rating group and service ID. You can activate this reporting level per PCC rule.
- Quota management only per Rating Group (RG) in case of N40, RG/RG+SID in the case of Gy/Gz per PDU session.
- Charging for IP-based PDU session types.

Converged Charging

The 5G system supports converged charging for offline and online charging scenarios.

The SMF performs converged charging for each of the following:

- Charging data that is related to a PDU session.
- Charging data that is related to service-data flows within a PDU session.

The scope of convergent charging in this implementation includes quota management and usage reporting. For convergent charging, the SMF interacts with the CHF or OCS /OFCS for charging data related to PDU sessions. The Charging Data Request and the Charging Data Response messages are exchanged between the SMF and the CHF based on session-based charging (SCUR scenarios). The Charging Data Request is issued by the SMF only when conditions that are related to chargeable events are met.

Chargeable Events

You can activate, deactivate, and modify PCC charging rules at any time during the PDU session lifetime.

PCF can modify the following attributes in a dynamic PCC rule active in the SMF:

- Charging Key
- Service Identifier
- Measurement Method

Note No modification is supported for Gy/Gz.

Activities on PCC rules and QoS flows aren't chargeable events. However, a change of charging rule in PCC rules leads to chargeable events. Some of the examples are the following:

- Start of service data flow.
- Termination of service data flow, for the last service data flow for the original PCC rule.

The charging key (that is, rating group) is used to request an online charging quota.

Note Depending on the reporting level received from the PCRF:

- For Gy, the quota is requested based on Rating Group (RG) or Rating Group and Service ID (RG+SID).
- For Gz, the quota is reported based on RG or RG+SID.

If no reporting level is received, then the quota is derived from rating group or service ID values received from the PCRF.

Charging Identifier

The charging identifier correlates charging information between the SMF and CHF or OCS /OFCS during the duration of a PDU session. The SMF generates and assigns a charging identifier when a PDU session is

established. The charging identifier is unique for that PDU session and is used in all messages that are exchanged in that PDU session.

Charging Information

The SMF collects the following charging information for converged online and offline charging:

- Usage of access and core network resources: Describes the amount of data that is delivered to and forwarded from the UE.
- Usage duration: Time interval from PDU Session Establishment to PDU Session Release.
- User: UE information used by the user for a PDU session.
- Data network: Data network address as determined by the DNN.
- Start time: PDU session start time.
- User location: HPLMN and VPLMN reporting area.

For service-data flows (flow-based charging), the SMF collects the following information:

- PDU session description.
- Data that are transmitted in uplink and downlink directions based on the rating-group information, or a combination of rating-group and service ID during volume-based charging.
- Duration of service data flow based on the rating group, or a combination of rating-group and service ID during event-based charging.
- The number of events and corresponding time stamps categorized by rating group or combination of the rating group and service id when event based charging applies.

The SMF collects charging information for service data flows per UPF, within a PDU session, based on the rating-group or based on a combination of rating-group and service ID.

How it Works

Charging Session

The SMF supports converged session-based charging (SCUR) as specified in *3GPP TS 32.290, section 5.3.2.3*. If Gy is enabled, SMF supports session-based charging as specified in *3GPP TS32.299, 12.9.0 section 6.4*.If Gz is enabled, SMF supports session-based charging as specified in *3GPP TS32.298, 12.9.0 section 5.1.2.2*.

The SMF establishes a charging session with the CHF with the Charging Data Request and Response (Initial) exchange. During the life of the PDU session, usage is reported with a Charging Data Request or Response (Update) exchange. After the session is released, Charging Data Request or Response (Termination) messages are exchanged.

In the case of a 4G session when Gy is enabled, then SMF establishes charging session with OCS by sending credit control request and credit control response (initial) message exchange. During the PDU session, the usage is reported with credit control request and credit control response (update) messages. After the session release, credit control request and credit control response (terminate) messages are exchanged.

In the case of a 4G session when Gz enabled, then SMF creates the offline URRs, if dynamic PCC rule is received. Then, the SMF maps the PCC rule to the corresponding charging buckets (Service Data Flow (SDFs))

and sends the N4 Establishment Request towards CnPGW-U. During the life of PDU session, the usage is reported for offline SDF or Bearer-level URRs through N4 Session Report or in the N4 Delete Session Response from UPF, it may send the GTPP Data Record Transfer request towards GTPP.

Offline Charging and Online Charging

Table 444: Feature History

Feature Name	Release Information	Description
Gz support for subscriber charging	2023.04	You can enable Gz for 4G session so that SMF can send N4 Establishment Request with default Bearer Level URR and SDF Level URR in the case of dynamic rule.

Charging is enabled for a session based on the input that is received from the PCF or PCRF.

For offline charging, the SMF sends Charging Data Request Initial toward the Charging Function (CHF) based on the presence of charging descriptors and refChgData field set in the smPolicyDecision message from the PCF in the SM Policy Control Create response.

On determining if charging is required during initial session establishment or post-session establishment, charging is enabled for the PDU session. Once charging is enabled, SMF sends the Charging Data Request (Initial) Message toward the CHF.

The SMF determines the Volume/Time threshold value either locally or from the Charging Data Response. These values are used to update the Volume/Time threshold IE in URR and to set the reporting trigger accordingly. The measurement method that is used in URR is derived from charging data.

For online charging, the SMF receives the Volume/Time Threshold and Quota values from the CHF. These values are received in the Charging Data Response (Initial) or using a Charging Data Request (Update) during a PDU Session Establishment. The SMF relays these Volume/Time Threshold and quota values to the UPF in the corresponding URR.

If Gy is enabled for an SMF 4G session, the session SMF sends the Credit Control Request (Initial) towards OCS to get the Volume/Time threshold and quota values. SMF relays these values towards to the UPF in the corresponding URR. If the SMF doesn't receive the volume threshold from OCS, the SMF determines the volume threshold from the local configuration.

If Gz is enabled for an SMF 4G session, SMF sends N4 Establishment Request with default Bearer Level URR and SDF Level URR in the case of dynamic rule. In the case of static and predefined rule, URRs are created after the PFCP session Report received with Start of Traffic (SoT). Bearer Level URR TIME_THRESHOLD and VOLUME_THRESHOLD values are received from egcdr threshold values that are configured in the Rulebase profile. SDF Level URR TIME_THRESHOLD and VOLUME_THRESHOLD values are received from egcdr threshold values that are configured in Charging profile. All the SDF Level URRs are linked to Bearer Level URR.

Note The threshold values from CHF always override the locally configured values.

The following table maps the IEs that are shared with the UPF during Create or Update URR during online or offline charging scenarios:

Table 445: IE Mapping for Online and Offline Charging Scenarios

IE	Online	Offline	Derived From (N40)	Derived From Gy	Derived From Gz
Volume Limit	Yes	Yes	CHF Response or Local Configuration	OCS Response or Local Configuration	-
Time Limit	Yes	Yes	CHF Response or Local Configuration	OCS Response	-
Volume Quota	Yes	No	CHF Response	OCS Response	-
Time Quota	Yes	No	CHF Response	OCS Response	-
Quota Holding Time	Yes	—	CHF Response	OCS Response	-
Monitoring Time	Yes	Yes	• Local configuration for offline charging • CHF response for online charging	OCS Response or Local Configuration	-
Reporting Trigger	Yes	Yes	The respective triggers that are set as shown in the following table.	OCS Response or Local Configuration	Local Configuration
Validity Time	Yes	-	-	OCS Response or Local Configuration	-

The following table lists the reporting triggers and their derived source:

Table 446: Reporting Triggers and the Derived Source

Reporting Trigger	Derived From N40	Derived From Gy	Derived From Gz
Volume Threshold Trigger	If Volume threshold is set	OCS Response or Local Configuration	If Volume Threshold is set
Time Threshold Trigger	If Time threshold is set	OCS Response or Local Configuration	If Time Threshold is set
Volume Quota Trigger	If Quota Exhausted trigger is set from CHF	OCS Response or Local Configuration	-
Time Quota Trigger	If Quota Exhausted trigger is set from CHF	OCS Response or Local Configuration	-
Linked Usage Reporting (LIUSA) Trigger	If URR contains Linked URR	-	If URR contains Linked URR

Quota Management

The SMF requests quota from the CHF upon meeting any of the following conditions:

- The Rating Group (RG) is installed for the first time and the charging method is Online for the dynamic rule.
- The start of traffic trigger is initiated from the UPF for the RG in the case of static or predefined rules.
- A specific trigger type, as defined in the 3GPP specification 32.255, is received in the usage report for the online charging service from the UPF.

The SMF uses the **quota request always** CLI command to request the quota always. This CLI command is available in the Charging Profile configuration mode. Upon configuring this CLI command, the SMF always requests for quota when reporting the usage to the CHF for the online services. The quota requesting ends when the charging service stops.

Irrespective of the **quota request [always | standard]** CLI configuration, the quota request is disabled for the trigger type "qht" configured through the **quota suppress triggers** CLI command.

If Gy is enabled for a 4G session, SMF sends the Credit Control Request-Initial (CCR-I) message with the Requested Service Unit (RSU) attribute to OCS when the **send charging-initial** CLI command is configured as **on-receving-rule** and the **reqQuotaForDynRules** CLI command is configured as **session-start**. Only if the **send charging-initial** is available, the CCR-I message is sent without RSU. SMF sends the CCR-I message with RSU when session report received with start of traffic, if **charging-initial** and **reqQuotaForDynRules** CLI commands are configured as **traffic-start**. SMF requests for Quota based on the reporting level received from PCRF or based on the local configuration available in the Charging profile, which is either RG or RG+SID.

If Gy is enabled for a 4G session, SMF uses the following CLI commands in the Charging profile:

- **send charging-initial [session-start | traffic-Start]**

Note The default value is **session-start**.

- **dynamic-rules [request-quota on-receiving-rule | start-of-traffic]**

Note The default value is **on-receving-rule**.

Service Units for Quota Management

The SMF sends Charging Data Record (CDR) to the Charging Function (CHF) for the service to be granted authorization to start, and to reserve the number of units. While triggering the CDR, the SMF requests volume (uplink, downlink, total) and time quota from CHF to support VoLTE and other use cases. The values of the requested units for static rules are obtained from the Diameter configuration under Active Charging Service. For the dynamic audio or video rules, the values for the requested service units are configured through the **requested-service-unit** CLI command in the Charging Profile Configuration mode.

Note If the Gz-enabled SMF interacts with OFCS to report usage, then Bearer Level and SDF Level values are received from the local egcdr configurations from rulebase and charging profiles respectively.

Support for Validity Time

The SMF uses time quota value and its corresponding trigger on N4 interface to arm the UPF about the time when the SMF needs the reporting of validity time.

The CHF arms the SMF to report the usage for the rating group when the timer associated with the validity_time expires.

Based on the presence of Validity Quota and Time Quota, the SMF behaves as specified in the following ways:

- When the CHF sends only the Time Quota and not the Validity Quota, the SMF relays the CDR-U to the CHF and reports as Quota_EXHAUSTED upon receiving the usage report from the UPF.
- When the CHF sends only the Validity Quota and not the Time Quota, the SMF relays the CDR-U to the CHF and reports as VALIDITY_TIME upon receiving the usage report from the UPF.
- When the CHF sends both the Validity Quota and the Time Quota, the SMF determines the lower value of time_quota and validity_time, and then relays the CDR-U to the CHF accordingly. The SMF sends the "VALIDITY_TIME" trigger when the validity_time is lesser than the time_quota value. Similarly, when the validity_time is greater than the time_quota value, the SMF sends the "Quota_EXHAUSTED" trigger.

In addition to preceding behavior, the SMF sends Gy CCAU with one USU for volume and duration. For Gy, if the usage report is received with the volume and duration for the validity time, the SMF forwards the report to UPF.

CHF Selection

The CHF selection can be performed through one of the following options:

1. PCF-provided one or more CHF addresses as part of the PCC rule
2. UDM-provided charging characteristics
3. NRF-based discovery
4. SMF locally provisioned charging characteristics

Important The SMF uses one of the last two options to fetch the CHF IP address and port details. The SMF initially performs NRF-based discovery to select the CHF server. If the SMF fails to identify the server, then it uses the locally provisioned charging characteristics. If Gy is enabled, SMF uses the locally configured Diameter client profile to connect with the OCS server.Similarly, if Gz is enabled, SMF uses the locally configured GTPP profile to connect with the Offline Charging System (OFCS) server.

Charging Activities at SMF

URR Generation Toward N4

The SMF receives charging-data and usage-monitoring-data from the PCF. Based on this information, the SMF derives URR toward N4. In case the SMF is configured with volume/time limit at the session level, the SMF creates session-level URR.

Handling of Initial Event in Charging Component

The session context of SMF is configured with trigger/threshold as per the default described in *3GPP TS 32.255*. It overrides the same based on configuration present in the charging profile. The same values can be further overridden by CHF Charging Data Response Initial. Currently, trigger/threshold cannot be overridden when in PDU Establishment state.

The charging profile is referenced from the charging-characteristic profile. The CC profile is taken from UDM subscription for PDU session. If the CC profile is not mentioned in the UDM response, it is taken from the DNN profile.

After trigger/threshold/quota are determined, the SMF N4 Setup Request with set of Create URRs are derived from charging-data with one session-level URR.

If the session-level reporting is determined, the session-level URR is associated to each SDF URR.

The following triggers are supported:

- Volume/Time trigger at session/RG level (N40) /RG or RG+SID level (Gy/Gz)
- AMBR change
- QoS change
- Quota threshold and quota exhausted
- Quota handling time
- Tariff time change

Note Gz supports Qos, ULI, and MsTimezone triggers only.

Obtaining Threshold Values at SMF

Threshold values, during online charging, are always obtained from the CHF/OCS. In the case of Gy, if volume threshold is unavailable in the OCS response, the volume threshold is obtained from the local configuration. Whereas the threshold values, during offline charging, are obtained either from the CHF or from the charging profile configuration.

If charging profile is not determined during PDU establishment, the SMF refers to the charging profile from the DNN profile. Once the Charging Profile is determined, the SMF uses the determined Charging Profile to obtain the threshold values for Session/SDF URR.

In case of Gz, the Threshold values are received from rulebase for the Bearer Level URR and Charging profile from the SDF Level URR.

The configuration has threshold values at a session level or rating-group level. The rating-group level threshold values are generic and not about a rating-group. These threshold values are overwritten by CHF response.

The Gz interface supports the SDF-level configuration that is applied from the charging profile. This interface doesn't support the Rating Group level configuration.

Note The CHF response has various triggers. If some trigger is available at the session level or rating-group level, and if the volume or time threshold value is unavailable, then these values are assumed to be disabled at the corresponding level.

Trigger Determination at SMF

The SMF has triggers enabled by default, as specified in 3GPP TS 32.255, section 5.2.1.4.

These triggers can be overwritten at a session level by trigger configurations present in the charging profile. Further, these triggers can also be overwritten by CHF/OCS responses.

Trigger configuration in charging profile is only applicable at a session level. It is not applicable for rating-groups. The trigger configuration is applicable at the SDF level.

In the case of Gz, the trigger configuration applicable to the SDF level URRs.

Reporting Category

The charging trigger can be of two reporting categories—Immediate and Deferred. The usage report of the immediate category must be reported to the CHF immediately. For reporting events that must be deferred, the SMF stores the usage report locally, and publishes either when the next trigger of the immediate category is invoked, or when the storage limit is exhausted.

When reporting stored usage reports to the CHF, the usage report is triggered because of the trigger type in UsedUnitCategory and the message is triggered because of the trigger type in ChargingDataRequest.

Sometimes, a scenario can have two triggers hit at the same time. AMBR_Change and QoS Change can happen at the same time. In which case, all the triggers as applicable at the RG level or session level will have multiple trigger values. For OCS, all the triggers are applicable at MSCC level. For Gz, all the triggers are applicable at SDF level.

A trigger can be enabled at the RG level, and for some RG it can be immediate reporting and for others it can be deferred reporting. When a trigger event is hit, various usage reports will have a corresponding category filled respectively in usedUnitContainer.

Deferred CDR will be relayed in the following scenarios:

- An immediate category event happens.
- Maximum number of charging conditions are crossed.
- Configured number of maximum deferred reporting is crossed.

Maximum Charging Characteristics (CC) is reset whenever there are push CDRs. This could be because of maximum CC limits being crossed or because of immediate category reporting.

In case of Gz, CDRs are relayed based on the maxlosdb configuration in the charging profile.

Note Currently, SMF does not support two charging descriptors with the same rating group.

Only immediate reporting category is applicable in the case of Gy.

Handling Reporting Level

The reporting category is classified into the following:

- Rating Group (RG) level: The RG is mandatory at this level.
- Service ID level: The RG and service ID is mandatory at this level.
- Sponsor ID level: The RG and Sponsor ID is mandatory at this level.

PCF communicates the reporting level to the SMF through the Charging Data Request. If the reporting level is RG, then RG is the primary key. If the reporting level is Service level or Sponsor Level, then RG and Service ID or RG and Sponsor ID respectively become the primary key. The SMF drops the charging descriptors from the PCF if the preceding requirement is not satisfied.

Note In the case of Gy or Gz, PCRF communicates the reporting level to SMF. If SMF receives no reporting level from PCRF, the reporting level is derived from the Rating Group or Service ID values received from the PCRF.

Re-Authorization

The CHF triggers Reauthorization of charging descriptors using Charging Notify request. Reauthorization is implemented at the session-level or at a RG-level for both online and offline charging.

The SMF processes the reauthorization details (which contain an array of RG, ServiceId, QuotaMgmtIndicator) received in CHF Notify and retrieves the charging descriptors associated with the current PDU session. SMF ignores any unmatched reauthorization item.

For the charging descriptors identified for reauthorization, the SMF queries for usage reports from UPF and sends it to the CHF.

As part of the CHF response, the SMF detects any change in quota or threshold information and performs N4 Session Modification to update URRs.

Final Unit Indication Support for N40 Interface

The SMF supports N40 Final Unit Indication (FUI) in the Charging Data Initial or Update Response from CHF as per 3GPP TS 32.291, section 6.1.6.2.1.12.

On receiving FUA, the SMF installs a new FAR and associates its FAR-ID in the URR, in the FAR ID Quota Action IE. If a FAR with the same parameters exists, the SMF uses its FAR-ID in the Create or Update URR. The UPF initiates appropriate actions set in FAR after quota exhaustion.

SMF supports FUI in CCA-I or CCA-U message from OCS. On receiving FUA, SMF installs a new FAR and associates its FAR-ID in the URR. If an FAR with the same parameters exists, SMF uses its FAR-ID in create or update URR. UPF initiates appropriate action as set in FAR after the quota exhaustion.

By default, the terminate configuration isn't activated to terminate the session and SMF only reports the final Used Service Unit to OCS without requesting further quota. UPF drops the further traffic after the quota exhaustion until OCS allocates the new quota through reauthorization.

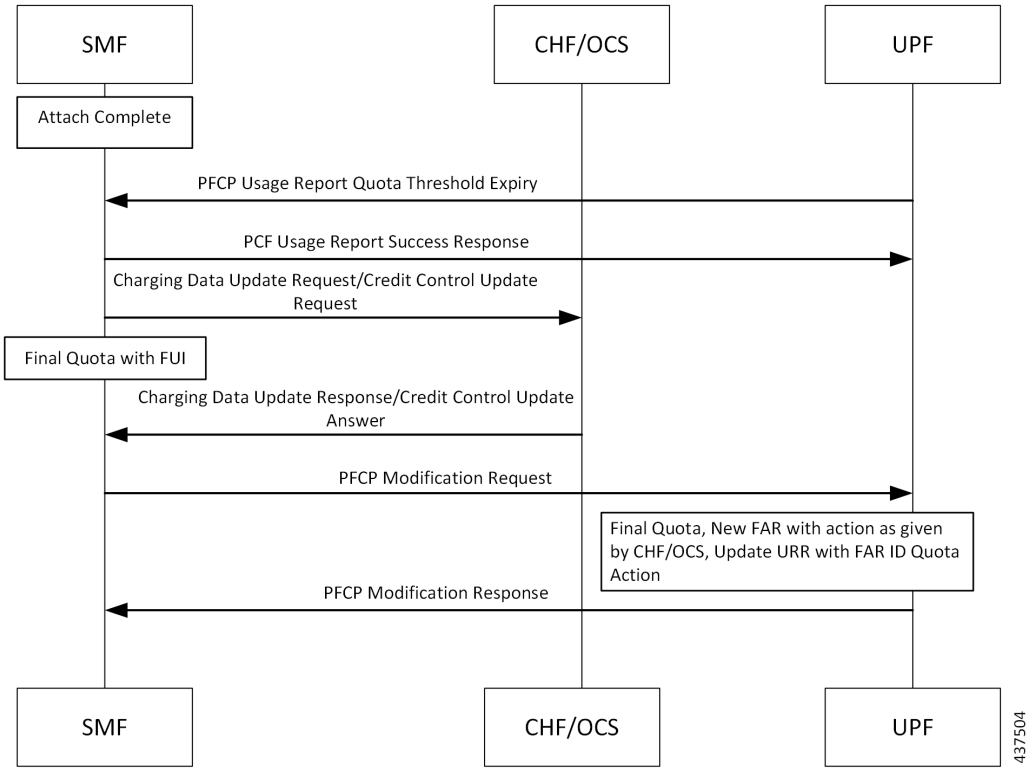
Note Reauthorization is supported for Gy.

FUI at MSCC Level—If FUI is received at the MSCC level and FUI CLI is configured to terminate the session, then SMF terminates the session if either the quota is exhausted or no quota is available.

FUI at Command Level—If FUI is received at the command level, then SMF terminates the session after quota is exhausted irrespective of FUI CLI configuration or no quota is available and FUI is received.

Currently, the SMF only supports Terminate and Redirect FU actions in the case of N40.

Figure 264: FUI in the Charging Data Initial or Update Response from CHF



- At any instance, CHF/OCS provides granted unit (Quota) to the SMF along with FUI.
- When the SMF receives the granted unit with FUI, the SMF creates FAR toward N4 and associates it to the corresponding URR which carries the quota information.
- After UPF receives the FAR associated with the URR, the corresponding FAR action is implemented when the quota exhausts.

Final Unit Indication Support for Gy Interface

Table 447: Feature History

Feature Name	Release Information	Description
Final Unit Indication (FUI) support in CCR-U	2023.04	As part of Gy Usage Reporting, SMF supports FUI in CCA-U from OCS.FUI is enabled or activated during the session creation or update. After FUI activation, when there is any update triggers due to an event trigger or Usage report, SMF sends subsequent CCR-U toward OCS without requesting further Quota and receives CCA-U.

Feature Description

SMF supports Final Unit Indication (FUI) in Credit Control Answer-Initial (CCA-I)/Credit Control Answer-Update (CCA-U) from the Online Charging System (OCS) to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP must be taken.

Upon receiving the Final Unit Action (FUA), the SMF installs a new Forwarding Action Rules (FAR) and associates its FAR-ID in Usage Reporting Rule (URR). If a FAR with the same parameters already exists, the SMF uses its FAR-ID in create/update URR. SMF takes an appropriate action as set in the FAR after the quota exhaustion.

In case of Final Unit Action terminate, the SMF installs a new FAR with the application action “drop” and associates its FAR-ID in URR. SMF terminates the Protocol Data Unit (PDU) session immediately after reporting the final Used-Service-Unit to OCS without requesting further quota, if configured to terminate the session and, the quota is exhausted for that service/MSCC regardless of the state of the other MSCCs.

If the usage report is received due to volume/time threshold or validity time, SMF reports the usage report only through Gy-CCR-U and continues to request for further quota.

By default, the terminate configuration is not activated to terminate the session and the SMF will only report the final Used Service Unit to OCS requesting further quota. SMF drops the further traffic after the quota exhaustion until OCS allocates the new quota through reauthorization.

Upon receiving a further quota from the OCS after FUI activation, the previous FUI gets overwritten.

Note Currently, the SMF with Gy interface supports only Terminate FU actions.

For FHT with Continue action, SMF terminates the PDU session immediately after receiving quota exhaustion for any FUI URR and reports the final usage to OCS through Gy-CCRT if CLI is configured to terminate the session or had received command level FUI. SMF sends Gy-CCRT to OCS with Termination Cause "DIAMETER-ADMINISTRATIVE" and MSCC Reporting reason as "FINAL".

When both time quota and validity time are received and the time quota exceeds validity time or when validity time alone is received without time quota, then SMF sends Gy-CCRU with MSCC reporting reason as "VALIDITY-TIME" and requests further quota.

Levels of FUI

FUI exists at two levels:

- **Final Unit Indication at MSCC Level**: If FUI is received at the MSCC level then the SMF terminates the session after the quota exhausts, only if the FUI CLI is configured to terminate the session. Also, if there is no quota and FUI is received, the SMF terminates the session immediately, only if the FUI CLI is configured to terminate the session.
- **Final Unit Indication at Command Level**: If FUI is received at the Command level, the SMF terminates the session after quota exhaust irrespective of FUI CLI configuration. Also, if there is no quota and FUI is received, then the SMF terminates the session immediately.

How it Works

FUI gets enabled or activated during the session creation or update. After FUI activation, when there is any update trigger due to an event trigger or Usage report, SMF sends subsequent CCR-U toward OCS without requesting further quota and receives CCA-U. Following scenarios can occur:

- **CCA-U receives with Quota and no FUI**: SMF resets the FUI, de-associates the FAR, and sends new quota in the update URR.
- **CCA-U receives with Quota and FUI**: SMF sends new quota in update URR, associates the previously dropped FARs, and continues with FUI without any update.
- **CCA-U receives without Quota and no FUI**: SMF does not send any updated URR and continues with the FUI without any update.
- **CCA-U receives without Quota and with FUI**:

  SMF terminates the session immediately

  - if the FUI is received at the command level and there is no quota
  - if the FUI is received at the MSCC level, the FUI CLI is configured to terminate the session, and there is no quota.

- **CCA-U receives with FHT action as Terminate**: SMF terminates the session immediately due to FHT.
- **CCA-U receives with FHT action as Continue and sub action as None/Unknown**:

  SMF allocates the maximum quota to both FUI and non-FUI online URRs regardless of whether the FUI is received at Command Level or at MSCC Level and **mscc-final-unit-action terminate session** CLI is configured or not.

- **CCA-U receives with MSCC Level Error**: SMF skips the failed MSCC and continues with the FUI without any update.

Limitations

Following are the known limitations of the Final Unit Indication feature:

- Re-authorization is currently not supported in the FUI support for SMF with Gy interface.
- Redirection is currently not supported as part of FUI support for SMF with Gy interface.

Configuring Final Unit Indication

To activate the Final Unit Indication, use the following sample configuration:

```
config
  profile charging profile_name
    mscc-final-unit-action terminate session
    end
```

NOTES:

- **mscc-final-unit-action terminate session**—By default, this configuration is not activated. If the Final-Unit-Indication AVP comes with an action TERMINATE for a given MSCC, the session will not be terminated by the SMF, and the UPF should take appropriate action for further traffic as set in FAR after the quota exhaustion. When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session will be terminated immediately regardless of the state of the other MSCCs.

Configuration Verification

To verify the activation of FUI at MSCC level, use the following show command:

```
product smf(config)# show running-config profile charging chp
product smf(config-charging-chp)#
mscc-final-unit-action terminate session
```

OAM Support

Bulk Statistics Support

The SMF supports the following disconnect reason as part of **smf_disconnect_stats**:

- **disc_fua_terminate**—Session terminates due to Termination action of Final Unit Indication.

Following statistics is added as part of the **SMF Charging Final Unit Indication Stats Category**:

- **ocs_recieved_fui_stats counter**—Total number of Final Unit Indication received from OCS.

Reconciliation of Billing Records

Important The Reconciliation of Billing Records is a customer-specific feature that requires IE level compliance across both the SMF and the CHF.

The communication of SMF and CHF involves both the converged CHF and offline CHF. When all the converged CHF servers are unreachable, the SMF falls back to the offline CHF for uninterrupted usage reporting. Then, the SMF sends the usage to the offline CHF.

The reporting to offline CHF does not include any differentiator in Used Unit Container (UUC) for the offline service and the converted offline service.

SMF supports a new enumerated value “CONVERTED_OFFLINE” in the Quota Management Indicator (QMI) added to the UUC. The SMF uses this enumerated value to mark the converted offline usage records sent to the offline CHF.

With this feature, the offline CHF server can differentiate between normal offline usage and converted usage records.

Static and Predefined Rules for Charging

Configuration of static or predefined rules is similar to the procedures on SMF and UPF. The layout of configuration is as follows:

1. Rulebase: A one-to-many rulebase is configurable. For a single PDU session, you can activate a single rulebase any time. PCF can activate the rulebase at SMF by sending the rulebase name in the PCC rule.
2. Ruledef: Each rulebase can have one-to-many ruledef configurations. A ruledef can either be of static or predefined type. Each ruledef is assigned to a charging action.
3. Charging Action: Contains QoS and charging information.

The SMF derives charging data for each charging action in the rulebase. Charging action associated to static rules in the rulebase is immediately derived and updated in the PDU context. Charging action that is associated to predefined rules is derived and updated when PCF activates the specific predefined rule at SMF.

The charging action derived URR has the following behavior:

- Online charging is identified by the "**cca charging credit**" configuration under charging action.
- Offline charging is identified by the "**billing action egcdr**" configuration under charging action.
- Armed triggers for volume-limit and time-limit are under the gtpp group configuration, under APN. The UPF automatically detects these values and sends the respective usage reports. Gz uses triggers from the charging profile.
- The SMF, unlike the dynamic case, does not send the Create URR immediately for charging data that is derived from the configured rules.
- Using the online charging method, the UPF sends usage report with the "Start" trigger. The SMF uses CHF to derive the quota for the RG and relays the same information to the UPF in the Update URR message. In case of Gz, SMF reads the threshold values for Bearer Level URR from the rulebase and SDF Level URR threshold values from the Charging profile.
- You can configure the UPF threshold at a rulebase level. It creates a rulebase-level URR that is linked to all ruledef-level URR within the rulebase.

For a static rule, the SMF uses the active charging service configuration during run time to derive the QoS Descriptor information to be relayed towards CHF.

For predefined rules, the associated charging action results in creation of QoS Descriptor in session data with a combination of Rating Group (RG), service ID, and bandwidth ID values. When SMF relays the usage report to CHF, it checks for a match against the RG and service ID and uses the QoS that is applicable for the matched charging action.

Important If two predefined rules are simultaneously activated and the associated charging actions have the same RG and service ID but different bandwidth IDs, then the SMF checks if a match is found against the RG and service ID and uses the QoS that is applicable for the matched charging action. The SMF randomly selects the QoS Descriptor that is derived from one of the charging actions associated to the different predefined rules.

Note The preceding behavior is applicable to Gy as well.

Modification Scenarios in Charging

PCF/PRCF Update

The PCF performs the following actions during a modification scenario:

- Addition of PCC rules
- Modification of reference data
- Deletion of PCC rules
- Content update in charging data - using Measurement method

CHF/OCS Response

The CHF response, during an exchange, sends updated volume and time thresholds and quota. The SMF relays the updated URR toward N4.

A change in threshold, trigger, or quota triggers an Update URR, which leads to the N4 relay.

SMF sends the Update URR based on the following triggers:

- Volume or time threshold
- Volume or time quota
- Tariff time change
- Quota holding time, and so on

CDR Update for Immediate CC Events

The QUERY_INTERFACE IE supports sending the CDR message to the CHF for immediate CC events. If the CC trigger occurs at SMF and the trigger is armed at session level, the SMF queries the online and offline URRs at UPF, and the RADIUS URR if accounting is enabled. The QUERY_INTERFACE IE enables SMF to discover the URR that is available at UPF. This IE is configured along with the QUARR flag while sending the N4 Modification Request.

If the QUARR flag is not configured, the UPF does not report all URRs even if the QUERY_INTERFACE IE is configured. If QUARR flag is configured with the QUERY_INTERFACE IE, the Query URR will not be relayed to the UPF. This functionality is enabled or disabled using the **query-all-urr** CLI command in the Charging Profile configuration. By default, the configuration is enabled.

The QUERY_INTERFACE IE is a composite IE with bits for various interfaces.

The following flags are mapped to the specific URRs:

- GZ_Offline—Maps to interface 1 and UPF reports all offline SDF URRs.
- GY_Online—Maps to interface 7 and UPF reports all online SDF URRs.
- Radius_URR—Maps to interface 9 and UPF reports RADIUS URR.

- Bearer_URR—Maps to interface 2 and UPF reports all QBC URRs.
- Sess_URR—Maps to interface 12 and UPF reports Session level URR.

Note The **query-all-urr** CLI is not used for Gy or Gz.

Query interface is performed based on **query-all-urr** CLI for N40. However, the query interface is performed irrespective of CLI configuration for Gz and the query interface is not used for Gy.

URR Linking

If you have configured session-level volume or time value locally or have received them from the CHF, the SMF creates session-level URR and links it to all URR corresponding to offline charging descriptors.

If PCF receives multiple charging descriptors that are of the same rating group, the SMF creates extra URR and links it to all URR derived from charging descriptors of the same rating group.

URR Format

Following is the URR ID format:

- URR ID is 32-bit.
- MSB (32nd) bit for static or predefined URRs is configured to 1, and for dynamic URRs is configured to 0.
- First four LSB bits are configured for interface type.
  - 1 for offline
  - 7 for online
- Bit 4-31 is for URR ID number.

  For example: Dynamic first URR if ID is 1:

  0x00 00 01 01 Offline

  0x00 00 01 07 Online

  Static or Predefined first URR if ID is 1:

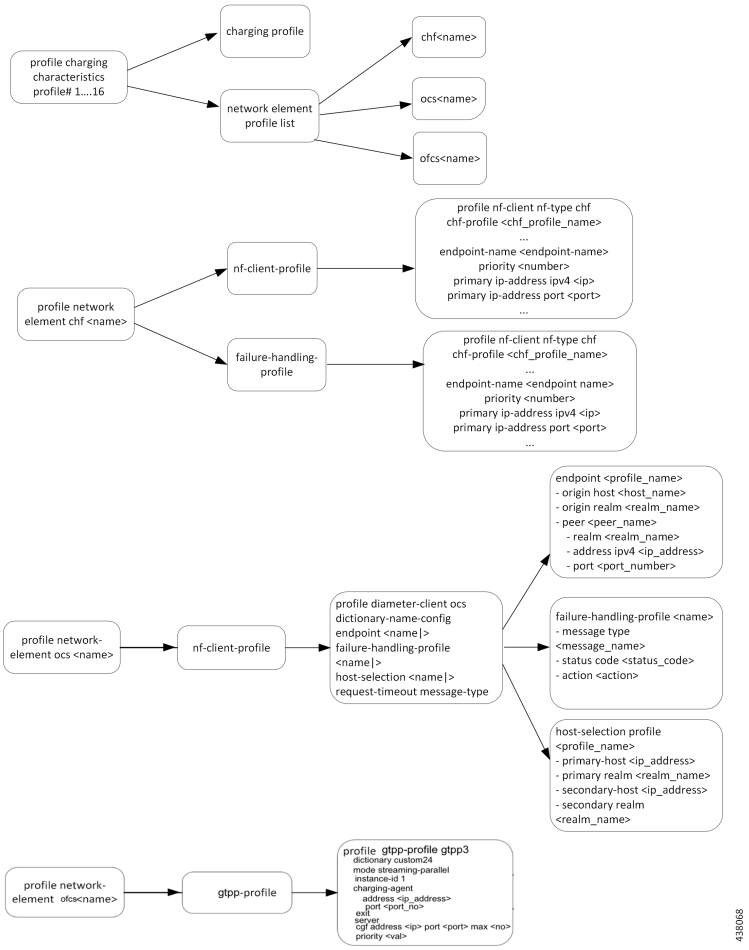
  0x80 00 01 01 Offline

  0x80 00 01 07 Online

Local Configuration

The following figure illustrates how local configuration works.

Figure 265: Local Configuration



- The SMF supports up to 16 charging characteristic profiles.
- Each CC profile comprises charging group and charging profile.
- The charging server group and charging profile are linked to the DNN profile. Currently, the charging profile supports configuration for trigger and thresholds.

Zero Usage Report Suppression

The SMF relays the offline resource usage report from the UPF to the CHF if any of the following conditions is met:

- Reporting type is immediate.
- Reporting type is deferred and the maximum number of deferred reportings is crossed.

The usage report includes the charging records with zero value as well. These zero value records (UUC and CDR-U) occupy unnecessary disk space on the CHF. To avoid this issue, the SMF leverages new configuration to control the offline charging records with zero byte data count.

When you configure the **offline zero-usage** CLI command in the Charging Profile configuration mode, the SMF relays the usage to the CHF without any overload of UUC or CDR-U.

The users can select the UUC or CDRs they want to suppress based on the CLI configuration.

Important The CDR release is never suppressed even if the **offline zero-usage drop cdr** command is configured in the Charging Profile configuration mode.

To support the zero suppress CDR, enable the **suppress-cdrs** CLI for Gz.

For details on the configuration, see the Charging Profile Configuration, on page 1451 section.

Call Flows

This section shows the following call flows:

PDU Session Establishment

The following figure illustrates the call flow of PDU session establishment.

Figure 266: PDU Session Establishment Call Flow

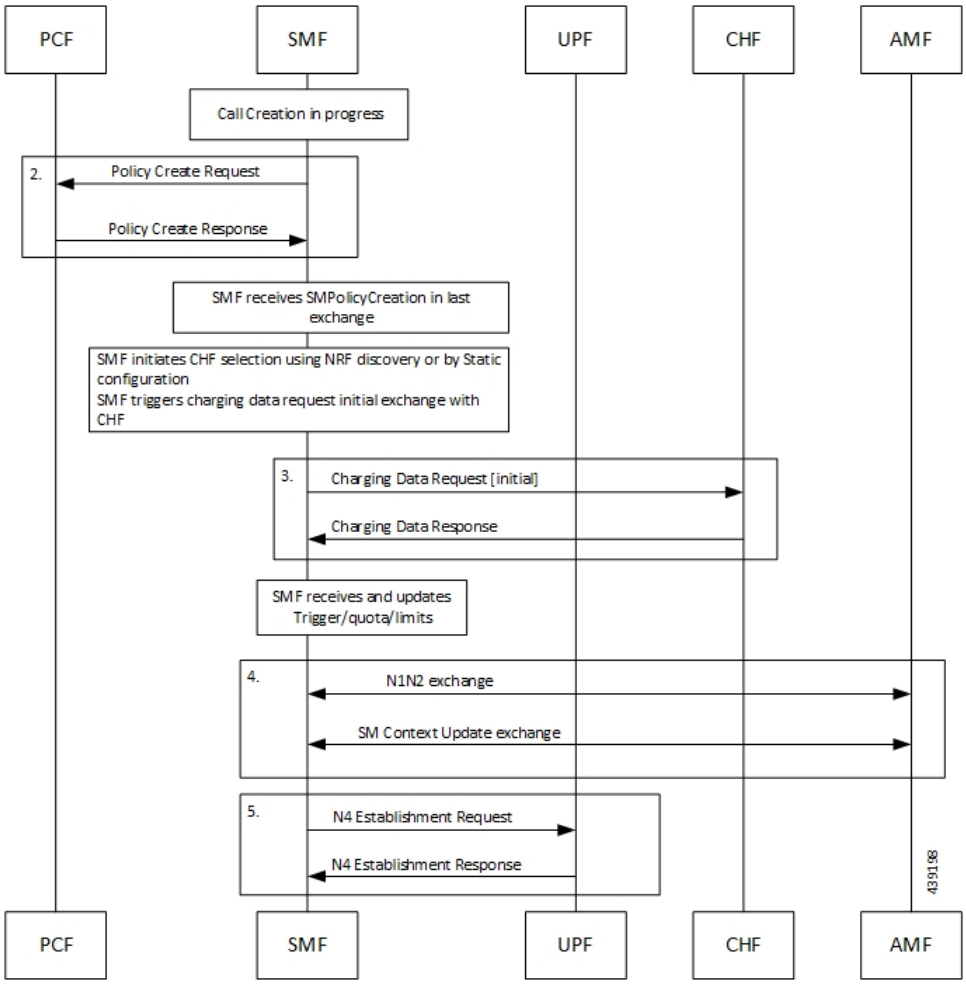


Table 448: PDU Session Establishment Call Flow Description

Step	Description
1.	Call creation starts at SMF.
2.	SMF performs a Policy Create exchange with PCF. In this exchange, the SMF can receive Charging Data that is associated to a PCC Rule. This Charging data indicates that charging is enabled for the session in progress. PCF may enable Static or Predefined rules. These rules can be also enabled with charging, based on the configuration.

Step	Description
3.	After the charging is detected at SMF, SMF initiates a Charging Data Request Initial exchange with CHF. In this exchange SMF may receive the following information from CHF: • CC triggers at session or RG level • Session level Time or Volume limits • Time or Volume limits at RG level • Quota at RG level
4.	SMF sends the N1N2 Exchange and SM Context Update Exchange to AMF.
5.	SMF initiates N4 session establishment request exchange with UPF. In the same request, SMF relays the information related to charging in the Create URRs.

Limitations

The SMF Charging feature has the following limitations on the N4 interface:

- If the session-level URR (CDR-I) is created once, it remains active throughout the session. This URR is not deleted in the subsequent session (CDR-U).
- If the session-level URR is not created, then it is not created in the subsequent CDR-U even if the session limits are available.

Standards Compliance

The SMF Charging feature complies with the following standards:

- *3GPP TS 32.255, version 15.3.0*
- *3GPP TS 32.290*
- *3GPP TS 32.299, version 12.9.0*
- *3GPP TS 32.298, version 12.9.0*

3GPP June 2019 Compliance for Charging Interface

The SMF is compliant with the 3GPP June 2019 specification TS 32.290 version 15.3.0.

For the June release, the messages goes over the version "v2" as indicated in the following URI format:

```
nchf-convergedcharging/v2/chargingdata
```

The CLI command for compliance configuration is: **service nchf-convergedcharging**. If this CLI command or version is not configured, the default version from 3GPP December 2018 is applied.

With the 3GPP June 2019 compliance, the following information elements (IE) are added:

- Authorized QoS
- Subscribed QoS
- IEs in QoSData

- Serving Network Function ID

Configuring SMF Charging

The SMF Charging involves the following configurations:

- DNN Profile Configuration, on page 1450
- Charging Characteristics Profile Configuration, on page 1450
- Charging Profile Configuration

DNN Profile Configuration

Use the following configuration to configure a DNN profile for SMF Charging.

```
config
  profile dnn profile_name
    charging-profile profile_name
    network-element-profiles [ chf profile_name | ocs profile_name ]
    end
```

NOTES:

- **charging-profile**: Specifies the Charging Profile configuration.
- **network-element-profiles**: Specifies the network element profile. Network element profile can be one of the following:

  chf: Specifies the CHF network element profile.

  ocs: Specifies the OCS network element profile.
- *profile_name*: Specifies the name of selected network element profile. After you select the network profile, enter a string.

Charging Characteristics Profile Configuration

Use the following configuration to configure charging characteristics profile for SMF Charging.

```
config
  profile charging-characteristics cc_value
    charging-profile profile_name network-element-profile-list chf chf_name
    end
```

NOTES:

- *cc_value*: Specifies the charging characteristics value, which must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 11AB.

Charging Characteristics ID Configuration

Use the following configuration to configure the charging characteristics ID, which is used to select the charging profile, if you have enabled the offline charging.

```
config
  profile dnn intershat charging-characteristics-id cc_id_value
    end
```

NOTES:

- **profile dnn intershat charging-characteristics-id** *cc_id_value*: Specify the charging characteristics ID value, which must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 11AB.

Charging Profile Configuration

Use the following configuration to configure the charging profile parameters for SMF charging.

```
config
  profile charging profile_name
    limit [ rating-group ] { duration duration_value | volume volume_value }
    max-charging-condition max_cc_value
    max-deferred-urr max_urr_value
    method { none | offline | online }
    offline zero-usage [ drop { cdr | uuc } | measurement { duration |
volume } | trigger { external | final | internal } ]
    query-all-urr { false | true }
    quota request [ always | standard ]
    quota suppress triggers [ qht ]
    reporting-level { offline | online { [rating-group]
    | rating-group | service-id }
    requested-service-unit time seconds volume downlink downlink_value
    uplink uplink_value total total_value
    tight-interworking-mode { false | true }
    triggers session session_level_triggers
    session-failover { false | true }
    send charging-initial  { session-start | traffic-start }
    dynamic-rules request-quota { on-receiving-rule | on-traffic-match
}
    quota validity-time  validity_time
    quota volume-threshold percent  volume_threshold_percent
    usage-reporting quota-to-report based-on-grant {
report-only-granted-volume }
    mscc-final-unit-action terminate session
    max-secondary-rat-reports report_range
    egcdr losdv-max-containers container_num
    egcdr service-data-flow threshold { {volume | interval } { downlink
 | total | uplink }  bytes | {interval  <duration>}
    egcdr closure-reason { admin-disconnect | normal-release | }
    egcdr triggers {qos-change | uli-change | ms-timezone-change}
    egcdr suppress-cdrs zero-volume triggers { external-trigger-cdr
final-cdr  internal-trigger-cdr }
    egcdr-final-record closing-cause [ same-in-all-partials | unique ]
    end
```

NOTES:

- **limit**: Specifies the threshold limit.
- **duration**: Specifies the duration threshold for charging. The threshold value ranges from 0 through 2147483647.
- **volume**: Specifies the volume threshold for charging. The threshold value ranges from 0 through 9223372036854775807.
- **rating-group**: Specifies the volume and duration threshold for a Rating Group.
- **max-charging-condition** *max_cc_value*: Specifies the maximum number of changes to the charging condition. *max_cc_value* must be an integer ranging from 0 through 500. The default value is 20.
- **max-deferred-urr** *max_urr_value*: Specifies the maximum number of deferred USU containers. *max_urr_value* must be an integer ranging from 0 through 200. The default value is 50.
- **method**: Specifies the charging method. The default charging method is offline.
- **offline zero-usage { drop | measurement | trigger }** : The SMF suppresses the offline URR with zero volume and duration. By default, the zero usage drop configuration is disabled on SMF.
  - **drop { cdr | uuc }**: The SMF suppresses the CDR or UUC with zero usage. If there are mutiple reports, then the SMF drops only the reports with zero usage. Note that there is no impact on the online reporting.

    If the **drop** command is not configured, the SMF stops sending UUC for the offline usage report.
  - **measurement { duration | volume }**: The SMF specifies the measurement method of the network usage for suppression. The measurement method is based on volume and duration.

    If the **measurement** command is not configured, the SMF suppresses the records with both zero volume and zero duration, or the records with zero volume or zero duration depending on the configuration.
  - **trigger { external | final | internal }**: Specifies the list of triggers to be suppressed.
    - **external**: The SMF suppresses the usage reports that are generated due to external triggers, such as QoS Change, RAT change, User Location change, and PLMN Change.
    - **final**: The SMF suppresses the usage reports that are generated at the end of a context.
    - **internal**: The SMF suppresses the usage reports that are generated due to internal triggers such as, volume limit, time limit, and tariff change.
- **query-all-urr { false | true }**: Specify to query all URRs. By default, this configuration is enabled (set to true).

  If this CLI command is disabled (configured to false) or the CC trigger is not armed at session level, the SMF will send QUERY_URR and report CC events along with usage report.
- **quota request [always | standard]**: Controls the requesting of quota from the CHF for online charging services based on the configuration. If the **quota request always** is configured, the SMF always requests for quota. If the **no quota request** or **quota request standard** CLI command is configured, then the SMF requests the quota for specific trigger types as defined in standard, which is the default behaviour.
- **quota suppress triggers [qht]**: Suppresses the quota from the CHF upon configuring the usage report trigger type "qht".

- **reporting-level**: Specifies the reporting level configuration to be used for offline and online charging.

  The default value is [rating-group] level.

- **requested-service-unit**: Configures the value for the requested service units.
  - **time** *seconds*: Configures the time quota value in seconds from 1 through 4000000000.
  - **downlink** *downlink_value*: Configures the downlink volume in bytes from 1 through 4000000000.
  - **uplink** *uplink_value*: Configures the uplink volume in bytes from 1 through 4000000000.
  - **total** *total_value*: Configures the total volume in bytes from 1 through 4000000000.
- **tight-interworking-mode**: Configuration to enable tight interworking mode for online or offline charging methods.
- **triggers**: Specifies the list of triggers to be configured.
- **session** *session_level_triggers*: Specifies the list for Session Level Triggers. The list of Session Level Triggers is as follows:
  - **repor3gpp-ps-change**
  - **ambr-change**
  - **max-number-of-changes-in-charging-conditions**
  - **plmn-change**
  - **qos-change**
  - **rat-change**
  - **serv-node-change**
  - **tarrif-time-change**
  - **ue-pra-change**
  - **ue-time-change**
  - **upf-add**
  - **upf-rem**
  - **user-loc-change**
- **session-failover { false | true }**: Enable Diameter session failover for Gy. The default value of this configuration is **false**.
- **send charging-initial { session-start | traffic-start }**: Specify whether to send CCR-I message towards OCS when dynamic and predefined rules are received, otherwise CCR-I message sends the usage report received with the start of traffic. The default value is **session-start**.
- **dynamic-rules request-quota { on-receiving-rule | on-traffic-match }**: Specify whether to send CCR-I message with RSU when dynamic rules received, otherwise CCR-I message sends the usage report received with start of traffic along with RSU. The default value is **on-receiving-rule**.

- **quota validity-time** *validity_time*: Specify the validity lifetime of the quota in seconds 1 through 4000000.
- **quota volume-threshold percent** *volume_threshold_percent*: Specify the volume threshold value as a percentage of the volume quota 1 through 100.
- **usage-reporting quota-to-report based-on-grant { report-only-granted-volume }**: The **based-on-grant** option specifies the report volume or duration in Used Service Unit to OCS if only it is granted in Granted Service Unit by OCS server. The **report-only-granted-volume** option specifies the filter for sending Used Volume quota to OCS base on Input, Output, or Total Octets granted in Granted Service Unit by OCS server.
- **mscc-final-unit-action terminate session**: Terminate the session when MSCC final unit action is terminate.
- **max-secondary-rat-reports** *report_range*: Configure the maximum number of secondary RAT usage reports to trigger the GTPP (Gz) update. *report_range* must be an integer in the range of 0 to 50. The recommended value for secondary RAT usage limit for max-secondary-rat-reports is 25.
- **egcdr losdv-max-containers** *container_num*: Specify the maximum List of Service Data containers (LOSDV) for creating a GTPP data record. The default value is 1.
- **egcdr service-data-flow threshold { {volume | interval } { downlink | total | uplink }** *bytes* **| {interval** <*duration*>**}**: Specify the SDF level offline URR threshold values. The limit for the number of downlink, total, or uplink octets must be an integer in the range of 100000-4000000000.
  - **egcdr service-data-flow threshold interval***duration*: Configure the threshold for offline charging. The threshold interval value must be an integer in the range of 60–40000000.
- **egcdr closure-reason { admin-disconnect | normal-release | }**: Configure the closure reason.
- **egcdr triggers {qos-change | uli-change | ms-timezone-change}**: Enable the triggers for CDR.
- **egcdr suppress-cdrs zero-volume triggers { external-trigger-cdr final-cdr internal-trigger-cdr }**:
  - **egcdr suppress-cdrs zero-volume**: Suppress the CDRs.
  - **triggers**: Configure one of the list of triggers that can be used to suppress CDR with zero volume.
  - **egcdr suppress-cdrs zero-volume triggers internal-trigger-cdr**: Specify that an Async volume usage reporting is from UPF through PFCP session usage report.
  - **egcdr suppress-cdrs zero-volume triggers final-cdr internal-trigger-cdr**: Specify that a call is getting terminated.
  - **egcdr suppress-cdrs zero-volume triggers external-trigger-cdr**: Specify that a Sync volume usage reporting is from UPF through Query URR.
- **egcdr-final-record closing-cause [same-in-all-partials | unique]**
  - **egcdr-final-record**: Configure the final CDR.
  - **closing-cause [same-in-all-partials | unique]**: Configure the closing cause in case of the final CDR. The **same-in-all-partials** value specifies that the same closing cause is to be included for multiple final CDRs. The **unique** value specifies that the closing cause for final CDR is to be unique.

The following is a sample configuration for SMF Charging:

```
config
   profile dnn intershat1
   charging-profile chgprf1
   exit
   profile charging chgprf2
   limit volume 15000
   limit duration 90
   limit rating-group volume 12000
   limit rating-group duration 80
   triggers session [ ambr-change qos-change max-number-of-changes-in-charging-conditions
]
   max-charging-condition 1
   max-deferred-urr 3
   reporting-level online service-id
   reporting-level offline service-id
   session-failover   true
   quota validity-time 200
   quota volume-threshold percent 80
   dynamic-rules request-quota on-traffic-match
   send charging-initial traffic-start
   usage-reporting quotas-to-report based-on-grant
   mscc-final-unit-action terminate session
   max-secondary-rat-reports 25
   egcdr losdv-max-containers 2
   egcdr service-data-flow threshold volume downlink 100000
   cdr service-data-flow threshold interval 100
   egcdr closure-reason normal-release
   egcdr triggers ms-timezone-change
   egcdr suppress-cdrs zero-volume triggers
   egcdr-final-record closing-cause [ same-in-all-partials | unique ]

exit
```

Mapping of Charging Scenario on Various Interfaces

Feature Description

The charging functionality and behavior of the SMF is influenced by the parameters and messages received from the CHF, PCF, and UPF on the N40, N7 and N4 interfaces. Based on the charging data that SMF receives, it provides reporting level support for online and offline charging.

How it Works

The SMF provides the different reporting levels for online and offline charging with the following rules:

- Configured rules are derived from the static or predefined charging actions.
- Session-level Usage Reporting Rule (URR) is derived from CHF trigger or local configuration.
- The SMF does not associate session-level URR for online and offline method charging description.
- The SMF does not associate session-level URR to the configured charging-action URRs.
- Rulebase URR is applicable only for the offline configured URR.
- For the configured online or online-offline charging method, if Ignore Service ID configuration exists, the URR list must contain "rg x urr-id y". Else, the SMF drops the charging actions as malformed.

Important The SMF supports multiple charging methods within the same rating group.

Charging Mapping

The N7 interface uses Charging Data from PCC rules or local configuration, N4 interface uses URR or Packet Detection Rule (PDR), and N40 interface uses Used Unit Container (UUC).

The SMF charging mapping on N7, N4, and N40 interfaces with various charging methods is described as follows.

Offline Method When Charging Data is Derived from One PCC Rule

Reporting level: Rating Group level or Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data limits from rating group trigger or local configuration.
- Second URR is derived from Session Limit, which is CHF or local configuration.
- Second URR is linked to the first URR.
- First PDR is derived from the first PCC rule.
- First and second URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- First UUC may or may not have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR replaces session-level URR.
- If configured and rulebase URR exists, it is linked to the first URR.

Online Method When Charging Data is Derived from One PCC Rule

Reporting level: Service ID level or Rating Group level

N4 interface:

- First URR is derived from the first Charging Data, which is threshold or quota from rating group granted-unit.
- Second URR is derived from Session Limit, which is CHF or local configuration.
- Second URR is linked to the first URR.
- First PDR is derived from the first PCC rule.

- First and second URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- First UUC may or may not have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.

Offline Method When Charging Data is Derived from Two PCC Rules

Reporting level: Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Third URR is derived from rating group level, which limits from Rating-Group trigger or local configuration.
- Fourth URR is derived from Session Limit, which is CHF or local configuration.
- The third and fourth URRs are linked to the first and second URRs.
- First PDR is derived from first PCC rule.
- Second PDR is derived from second PCC rule.
- First, third, and fourth URRs are linked to the first PDR.
- Second, third, and fourth URRs are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- Second UUC is derived from the usage report of the second URR.
- Both the first and the second UUCs have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR is linked to the first and second URRs.

Online Method When Charging Data is Derived from Two PCC Rules

Reporting level: Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be Linked Usage Reporting (LIUSA).
- Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Third URR is derived from rating group level, which is threshold or quota from the rating group granted unit.
- Fourth URR is derived from Session Limit, which is CHF or local configuration.
- Third and fourth URRs are linked to the second and fourth URRs.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First, third, and fourth URRs are linked to the first PDR.
- Second, third, and fourth URRs are linked to the second PDR.

N40 interface:

- First UUC is derived from usage report of the first URR.
- Second UUC is derived from the usage report of the second URR.
- Both the first and the second UUCs have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.
- If Ignore Service ID is configured, this method is not valid.

Offline-Online Method When Charging Data is Derived from One PCC Rule

Reporting level: Service ID level or Rating Group level

N4 interface:

- Offline URR is derived from the first Charging Data, which limits rating group trigger or local configuration.
- Online URR is derived from the first Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Offline and online URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the offline URR.
- Second UUC is derived from the usage report of the online URR.

Offline-Online Method When Charging Data is Derived from Two PCC Rules

Reporting level: Service ID level

N4 interface:

- First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Off3.
  - Second offline URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Off3.
  - Third offline URR is the rating group level, which limits the rating group trigger or local configuration.
  - First online URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online3.
  - Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online3.
  - Third online URR is the rating group level, which limits from the granted unit.
  - First PDR is derived from the first PCC rule.
  - Second PDR is derived from the second PCC rule.
  - First offline URR, first online URR, third offline URR, and third online URR are linked to the first PDR.
  - Second offline URR, third online URR, third offline URR, and third online URR are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first offline URR and has a service identifier.
- Second UUC is derived from the usage report of the second offline URR and has a service identifier.
- Third UUC is derived from the usage report of the first online URR and has a service identifier.
- Fourth UUC is derived from the usage report of the second online URR and has a service identifier.

Offline-Online Method When Charging Data is Derived from One PCC Rule with No Service Identifier

The offline and online reporting levels are at Service ID and Rating Group levels respectively.

Prerequisite: No Reporting Level from PCF

- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group

Note

- The SMF ignores the volume or time limit trigger from CHF at the rating group level.
- Session-level URR is not associated to URRs that are derived from the first Charging Data.

N4 interface:

- Offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
- Online URR is derived from the first Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Online URR and offline URR are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the offline URR and has a service identifier.
- Second UUC is derived from the usage report of the online URR and does not have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.
- If URR is configured, URR rulebase is derived from eG-CDR and is linked to both the offline and the online URRs.

Offline-Online Method When Charging Data is Derived from Two PCC Rules with No Service Identifier

The offline and online reporting levels are at Service ID and Rating Group levels respectively.

Prerequisite: No Reporting Level from PCF

- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group

Note

- The SMF ignores the volume or time limit trigger from CHF at the rating group level.
- Session-level URR is not associated to URRs that are derived from the first Charging Data.

N4 interface:

- First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
- Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR_Online.
- URR_Online is derived from the second Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First offline URR and URR_Online are linked to the first PDR.
- Second offline URR and URR_Online are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first offline URR and has a service identifier.
- Second UUC is derived from the usage report of the second offline URR and has a service identifier.
- Third UUC is derived from the usage report of the URR_Online and does not have a service identifier.

Note

- Session-level URR is not associated to the configured URRs.
- If URR is configured, URR rulebase is derived from egcdr and is linked to both the first and second offline URRs along with URR_Online.

Limitations

This feature has the following limitations:

- Tight interworking mode is not supported for the service which is at the rating group level.
- One service at the rating group level and another service at service ID level are not supported.

Standards Compliance

The Different Reporting Level Support for Online and Offline Charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290

Failure Handling Scenarios

This section describes the different failure handling scenarios associated with the errors that occur during SMF charging.

Application Error and Result Code Handling

SMF supports the application error codes from CHF at command level as defined in 3GPP TS 32.291 specification, version 15.3.0, section 6.1.7.3. The SMF also supports RG-level result codes as defined in 3GPP 32.291 specification, version 15.3.0 section 6.1.6.3.14.

The following labels are defined in the "chf_appl_err_stats" counter to indicate the CHF response failures at the application level.

- http2_err_code—Includes the following values:
  - 403
  - 400
  - 404
- appl_err_code—Includes the following values:
  - END_USER_REQUEST_REJECTED
  - END_USER_SERVICE_DENIED
  - QUOTA_LIMIT_REACHED
  - CHARGING_NOT_APPLICABLE
- appl_err_action—Includes the following values:
  - drop_traffic
  - disable_charging
  - terminate
- appl_err_exchg_type—Includes the following values:
  - initial
  - update

N40 Application Error Codes

The following table provides details of the application error codes with the corresponding SMF action.

Application Error /Session Level	HTTP2 Code	SMF Action	CHF Expected Actions	Limitations
CHARGING_FAILED	400	Terminate	None	None
RE_AUTHORIZATION_FAILED	400	None	Take corrective action	-
CHARGING_NOT_APPLICABLE	403	Continue subscriber session without Charging (no offline charging as well)	None	None

Application Error /Session Level	HTTP2 Code	SMF Action	CHF Expected Actions	Limitations
USER_UNKNOWN	404	Terminate	None	None
END_USER REQUEST_DENIED	403	Terminate	None	None
QUOTA_LIMIT_REACHED	403	Drop traffic for the online services. Offline services are not impacted.	CHF sends notify (RAR) after this condition is recovered for the session	

Note

- The error code 403 is not configured in the failure handling template.
- CHARGING_NOT_APPLICABLE (Disable charging) for static and predefined rules, occurs when a proprietary IE “Charging Disabled” in subscriber params is sent in the N4 modification or establishment request. This request is sent to prevent UPF from generating Start of Traffic for the URRs pending for activation. This IE is no longer sent in 2023.01.0 release and beyond. For more information, see the Handling Charging Disable Functionality section.

Gy Application Error Codes

Gy supports application-level error codes in MSCC-level and Command-level supported by SMF from the OCS server.

MSCC-level Failures

The following tables list the MSCC-level failure codes:

Table 449: Transient Failures (4xxx)

Result Code	Description
4010	DIAMETER_END_USER_SERVICE_DENIED
4011	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE
4012	DIAMETER_CREDIT_LIMIT_REACHED

Table 450: Permanent Failures (5xxx)

Result Code	Description
5003	DIAMETER_AUTHORIZATION_REJECTED
5012	DIAMETER_UNABLE_TO_COMPLY
5030	DIAMETER_USER_UNKNOWN
5031	DIAMETER_RATING_FAILED

Table 451: Error Codes

ResultCode	Behaviour
4010/4012(CCAI)	• CCAI is received withc4010/4012. • PFCP_SESSION_ESTABLISHMENT_REQUEST is sent with CREATE FAR with APPLY ACTION as DROP:1, CREATE URR is sent with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0
4010/4012(CCAU)	• CCAI is received withc4010/4012. • PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR with APPLY ACTION as DROP:1,UPDATE URR is sent with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0.
4010/4012(CCRT)	• PFCP_SESSION_DELETION_REQUEST is received with usage report with "timqu" trigger. • CCRT is sent with 3GPP-Reporting-Reason as “FINAL”
4011(CCAI)	• CCAI is received with 4011. • PFCP_SESSION_ESTABLISHMENT_REQUEST is sent with CREATE FAR APPLY ACTION as DROP:1, CREATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10.

ResultCode	Behaviour
4011(CCAU)	• CCAI is received with 4011. • PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR APPLY ACTION as DROP:1, UPDATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 9223372036854775807, 'up_vol': 9223372036854775807, 'down_vol': 9223372036854775807}, TIME_QUOTA as 'tm_quta' : 2147483647, TIME_THRESHOLD as 'time_treshold' : 10.
4011(CCRT)	• PFCP_SESSION_DELETION_REQUEST received with usage report with "timqu" trigger. • CCRT is sent without MSCC.
5003/5012/5030/5031 (CCAI)	• CCAI is received with 5003/5012/5030/5031. • PFCP_SESSION_ESTABLISHMENT_REQUEST is ent with CREATE FAR with APPLY ACTION as DROP:1, CREATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0
5003/5012/5030/5031 (CCAU)	• CCAU is received with 5003/5012/5030/5031. • PFCP_SESSION_MODIFICATION_REQUEST is sent with UPDATE FAR with APPLY ACTION as DROP:1, UPDATE URR with REPORTING_TRIGGERS as "volqu, timqu" and VOLUME_QUOTA as 'volume_quota' : {'dlvol': 1, 'ulvol': 1, 'tovol': 1, 'total_vol': 0, 'up_vol': 0, 'down_vol': 0}, TIME_QUOTA as 'tm_quta' : 0.
5003/5012/5030/5031 (CCRT)	• PFCP_SESSION_DELETION_REQUEST is received with usage report with "timqu" trigger. • CCRT is sent with USU (time(0)+volume(0)) and 3GPP-Reporting-Reason as "FINAL"

Command-level Failures

The Diameter endpoint pod handles the failure handling configuration after receiving a command-level failure for a Gy message from OCS.

Following are the actions and subactions applicable for Gy:

- Continue
  - FHSubActionEnum_UNKNOWN
  - FHSubActionEnum_DISCARD_TRAFFIC
- Terminate
  - FHSubActionEnum_WITH_TERM_REQUEST
  - FHSubActionEnum_WITHOUT_TERM_REQUEST

You can configure a failure handling profile with the preceding actions and subactions for following failure types that are received in CCA-I, CCA-U, or CCA-T messages:

- Any
- Result-code

Note The value ranges from 3000 to 9999.

- Exp-result-code

Note The value ranges from 3000 to 9999.

- Local-error

RG-level Result Codes

The following table provides details of the result code with the corresponding SMF action.

RG-level Result code	HTTP Status Code	SMF Behaviour	CHF Expected Behaviour	Limitations
RATING_FAILED	200	Drop traffic corresponding to the rating group	None	None
QUOTA_MANAGEMENT_NOT_APPLICABLE	200	Convert to offline	None	None
USER_UNKNOWN	200	Ignored (supported only at session level)	Not expected from CHF	None

RG-level Result code	HTTP Status Code	SMF Behaviour	CHF Expected Behaviour	Limitations
END_USER SERVICE_DENIED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the rating group.	Traffic will be dropped for offline service as well for online or offline services.
QUOTA_LIMIT_REACHED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None
END_USER SERVICE_REJECTED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None

Handling Charging Disable Functionality

The SMF performs the following functions when the charging transactions are disabled on N40 interface:

- Deletes the already created Usage Reporting Rules (URR) on N4.
- Sends the proprietary IE "Charging Disabled" in subscriber params attribute through the N4 establishment or modification request.

This Custom N4 IE has some functional impact on other kinds of Charging like Radius-Accounting etc.

To eliminate the identified challenges at UPF, the SMF undergoes the following behavior changes when disabling the charging process:

- For newly loaded rules, SMF doesn't construct new dynamic URR.
- SMF stops sending the Charging Disabled IE to the UPF. The UPF continues to send the Usage Report (USAR) to the SMF for the other URRs.
- The SMF then acknowledges UPF with a successful response message. If the report demands usage quota, SMF relays infinite quota without requesting for the N40 usage details through N4 modification response.

Charging Server Reconciliation

The SMF falls back to the first available offline CHF server when the NF selected by NF discovery is unreachable. The CHF Reconciliation feature involves deleting the existing subscribers that are associated to a set of offline NFs, and the subscribers that are in offline fallback mode.

Note The CHF reconciliation is applicable only when CHF endpoint is selected by NRF through NF discovery service.

The CHF server reconciliation works when one of the following two conditions is met:

1. If the NRF detects that an offline CHF server is active.
2. If the RAR is received from the CHF server on an offline converted session.

For the second condition, the session gets deleted directly. With the NF discovery, this feature involves the following steps:

1. SMF subscribes for the notification of NF instance IDs from NRF through NF_LIB component of Rest-EP.
2. If the NF discovery query determines that all the NFs are down, the NF_LIB component treats these set of NFs as offline. If any one of the NFs is available again, the NRF triggers notification for the same to the SMF.
3. The SMF performs NF discovery after revalidation timer. If the NRF detects any new NF, the SMF receives the corresponding notification from the NRF.
4. When the SMF identifies that an NF is online with all the required NF discovery query parameters, then the SMF initiates the CHF server reconciliation.

The following labels are introduced as part of this feature:

- disc_pdurel_chf_reconciliation: This label is defined under SMF_DISCONNECT_STATS to show the reason of disconnection.
- chf_reconl_pdu_sess_rel: This label is defined under smf_service_stats metric to show the number of times the PDU session release procedure is initiated.

Dynamic Update of Charging Configurations

Feature Description

The Dynamic Configuration Change Support feature allows SMF to dynamically handle the configuration changes of the charging parameters while minimizing the configuration errors. The existing and new SMF Charging parameters allow implementation of the dynamic configuration updates. This feature supports the following charging configurations:

- Active Charging Service (ACS) Profile
  - Rulebase

    - Ruledef
    - Charging-Action
    - Credit-Control-group
- Charging Profile
- Charging Characteristics
- GTPP Group
- Upf-Apn Configuration Group

How it Works

This section describes how dynamic change in configuration works for the supported Failure Handling Profile and Charging Profile configuration.

ACS Profile

The SMF supports dynamic change in the ACS configuration during the run time. The ACS Profile configuration defines various parameters for the ACS profile.

The following table lists the SMF and UPF behavioral changes during the dynamic update of ACS configuration in different scenarios.

Table 452: ACS Profile Configurations and its Impact during Dynamic Update

Configuration	Config Applied on both SMF and UPF	Config Applied only on SMF	Config Applied only on UPF
Rulebase addition	**Existing Session**: Continue to use the current rulebase value **New Session**: No impact for the new session	**Existing Session**: Change in the rulebase gets rejected at UPF **New Session**: Session creation fails at UPF for this rulebase	**Existing Session**: Change in the rulebase gets rejected at SMF **New Session**: Session creation fails at SMF for this rulebase
Rulebase removal	**Existing Session**: Not allowed without node drain **New Session**: No impact for the new session	**Existing Session**: Not allowed without node drain After the configuration change, the rulebase configuration remains stale on SMF if the rulebase removal on UPF is missed **New Session**: No impact for the new session	**Existing Session**: Not allowed without node drain After the configuration change, the rulebase configuration remains stale on UPF if the rulebase removal on SMF is missed **New Session**: No impact for the new session

Ruledef addition	**Existing Session**: Activates the new rule successfully **New Session**: No impact for the new session	**Existing Session - Static Rule**: The UPF neither activates the rule nor sends the report for this rule. **Existing Session - Predefined Rule**: Fails to activate the new rule until the UPF receives it. **New Session**: Same as the existing session	**Existing Session - Static Rule**: The UPF activates this rule and reports the usage. The SMF has the charging data for this RG+ServID. It creates dummy ChargParam and associates URR to it. **Existing Session - Predefined Rule**: Fails to activate the new rule until the SMF receives it **New Session**: Same as the existing session
Ruledef deletion	**Existing Session**: The current flows remain as is. If the flow is not created, it will never be created for this session. The SMF or UPF does not remove the associated charging. **New Session**: No impact for the new session	**Existing Session - Predefined rule** : The SMF rejects this rule creation. **Static and Activated Predefined Rules:** Existing flows remain as is. The SMF or UPF does not remove the associated charging. The received usage is reported successfully. If the SMF has not received the first usage report and when the first report arrives, the SMF creates chargParam/Urr context from RG+ServID. **New Session**: Same as the existing session	**Existing Session - Predefined rule**: The SMF continues to allow this rule creation but fails at the UPF. **Static and Activated Predefined Rules**: The UPF continues with the created URR for these flows. The SMF reports the usage without any issue. **New Session**: Same as the existing session
Charging Action addition with new RG/Svc Id (With addition of new rules associated to that CA)	**Existing Session - Static Rule**: The SMF creates charging entry for this RG when the first URR is received. **Existing Session - Predefined Rule**: The SMF activates the rule based on the PCF trigger. **New Session**: No impact for the new session	**Existing Session - Static Rule**: The UPF does not activate this flow. The SMF never receives the usage. **Existing Session - Predefined Rule**: The UPF fails to install predefined rule due to the unavailability of ruledef info. **New Session**: Same as the existing session	**Existing Session - Static Rule**: The UPF activates this flow. The SMF creates the charging entry for this RG when the first URR is received. In this case, the SMF does not find Charging-action with this RG+ServID. It creates dummy ChargParam with the received RG+ServID. **Existing Session - Predefined Rule**: Same as mentioned for the static rule. **New Session**: Same as the existing session

Charging action (and associated rules) removal	**Existing Session - Static Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. **Predefined Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again. **New Session**: No impact for the new session	**Existing Session - Static Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. **Predefined Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again. **New Session**: Same as the existing session	**Existing Session - Static Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. **Predefined Rules**: The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again. **New Session**: Same as the existing session
RG/Svc Id, Online/Offline Config changed within CA	**Static Rules and Already Active Predefined Rules**: The UPF creates new URRs and reports them. The SMF reconciles from URR ID table and creates charging data for these URRs as and when reported. **Post config change activation of predefined rules**: No issues. Both SMF and UPF are in sync. **New Session**: No impact for the new session	**Static Rules and Already Active Predefined Rules**: The UPF continues reporting with old URR ID and the SMF continues to report it without any issue. **Post config change activation of predefined rules**: Same as Static Rules **New Session**: The UPF rejects the establishment request if the predefined rules are activated during session establishment.	**Static Rules and Already Active Predefined Rules**: The UPF creates new URRs and reports them. The SMF reconciles from URR ID table and creates dummy chargParam and associates URR to it. **Post config change activation of predefined rules**: Same as Static Rules **New Session**: The UPF rejects the establishment request if the predefined rules are activated during session establishment.
URR Id table entry addition (New RG addition)	No action needed on SMF	No action needed on SMF	The UPF creates URR.
URR Id table entry removal	No impact	No impact	The UPF creates URR. The removal has no impact on the created URR.

URR Id table entry modification	No impact	No impact	The UPF creates URR. Removal has no impact on the created URR. If the same URR-id is allocated to different RG+ServID, the removal impacts the URR. The UPF fails to create new URR for the new RG+ServId.

NOTES:

- If the online report includes service id and the ignore-service-id is not configured in credit control profile, the SMF drops the report.
- If the new online URR contains the same RG as an existing URR, then the SMF drops the usage report.
- If the new offline URR contains the same RG+service ID as an existing URR, the SMF drops the usage report.
- In the same usage report, if the next online URRs include the same RG and the next offline URRs include with the same RG + service ID, the SMF drops the usage report.

Charging Profile

The Charging Profile supports dynamically updating the configuration based on the values that you pass during the runtime. The refresh operation of the values takes place considering the following scenarios:

- **Configuration reflects in the next encounter to access:** If the values are updated while an operation is in-progress, the SMF ignores the new values and continues to use the old values. For example, Limits in Charg-Profile and CC triggers.
- **Configuration reflects only on a new session:** If the configuration is specific to a session and the session has already considered the values, then the SMF does not consider the new values. For example, PduContext (DB entry). This case indicates that any update to the configuration does not impact the sessions that are already created. For instance, Charging Method in Profile or Charg-Profile in Charging Characteristics.
- **Configuration reflects instantly:** Configurations immediately consider the dynamic values whenever they are updated. If SMF has already used a configuration and it is later updated, then it uses the latest values.

If a session is created using a Charging Profile, which later gets deleted from the Ops Center, the session might attempt to access the configuration structure of the deleted profile. In such cases, the Smf-Service pod maintains a default profile mapped to the sessions whose profiles are missing.

The Charging Profile is responsible for handling the SMF charging parameters.

The following table lists the configuration parameters with the dynamic configuration change and its impact on the existing sessions.

Table 453: Charging Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
limit rating-group duration	Allowed	New values are used during the new URR creation or the subsequent URR update for the existing sessions **Note** The dynamic configuration does not initiate a URR update.
max-charging-condition	Allowed	No impact
max-deferred-urr	Allowed	No impact
metering-method	Allowed	New values are used during the new URR creation for the existing sessions
method	Allowed	No impact
reporting-level	Allowed	No impact
requested-service-unit time	Allowed	No impact
tight-interworking-mode	Allowed	No impact
triggers session	Allowed	No impact
Request Quota	Allowed	No impact
session-failover	Allowed	No impact
dynamic-rules	Allowed	No impact
send charging-initial	Allowed	No impact
quota Validity-Time	Allowed	No impact
quota volume-threshold	Allowed	No impact
usage-reporting	Allowed	No impact
mscc-final-unit-action	Allowed	No impact
max-secondary-rat-reports	Allowed	Impact
egcdr losdv-max-containers	Allowed	Impact
egcdr service-data-flow	Allowed	No impact
egcdr closure-reason	Allowed	Impact
egcdr triggers	Allowed	Impact
egcdr suppress-cdrs zero-volume	Allowed	Impact

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
egcdr-final-record	Allowed	Impact

Charging-Characteristics Profile

The Charging-Characteristics Profile configuration defines the various parameters for managing the charging characteristics for SMF Charging.

The following table illustrates if the configuration parameters allow dynamic configuration change.

Table 454: Charging-Characteristics Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
charging-profile	Not Allowed	The configuration is used only once while setting up the session.

Charging-Action Profile

The Charging-Action Profile configuration defines the QoS and charging related parameters associated with the rule definitions.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 455: Charging-Action Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Rating group and Service ID	Allowed	No impact

Credit-Control-Group Profile

The Credit-Control-Group configuration defines the parameters to be used for subscribers who use the mapped rulebase.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 456: Credit-Control-Group Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ignore Service ID	Allowed	No impact

Rulebase Profile

The Rulebase configuration parameters define the protocol rules to match a flow and the associated actions to be taken for the matching flow.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 457: Rulebase Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ruledef association to Charging-action	Allowed	No impact
Credit-Control-Group	Allowed	The configuration is used only once while setting up the session

GTPP Group Profile

The GTPP Group Profile configuration specifies the parameters for creating the GTPP group.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 458: GTPP Group Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Limits for offline configured urrs	Allowed	New values are used during the new URR creation for the existing sessions.

UPF-APN Configuration Profile

The UPF-APN Configuration Profile configuration defines the various parameters for the UPF-APN profile.

The following table illustrates if the configuration parameters allow dynamic configuration change.

Table 459: UPF-APN Configuration Profile Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Association of GTPP Group	Allowed	The configuration is used only once while setting up the session.

Network Profile for Peer CHF

The network profile for peer CHF configuration defines the various network configurations.

The following table illustrates if configuration parameters allow dynamic configuration change.

Table 460: Network Profile for Peer CHF Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Set of CHFs configured	Allowed	No impact

Network Profile for Peer OCS

The network profile for peer OCS configuration is to enable Gy interface.

The following table illustrates whether the configuration parameters allow dynamic configuration change.

Table 461: Network Profile for Peer OCS Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Set of OCS servers configured	Allowed	No impact

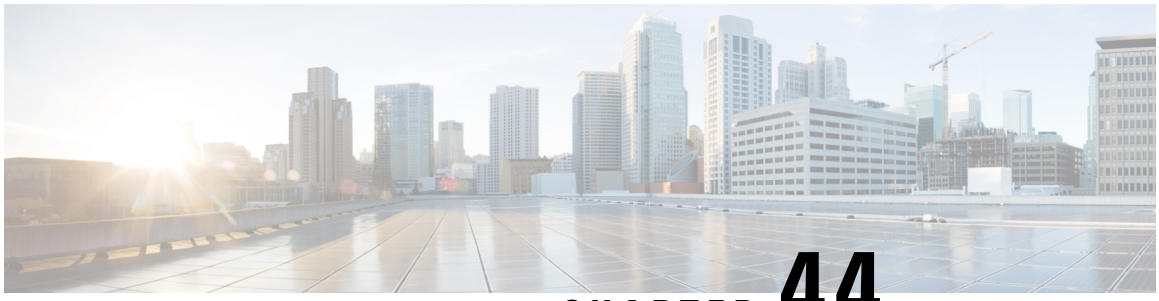
Network Profile for Peer OFCS

The network profile for peer OFCS configuration is to enable the Gz interface.

The following table illustrates whether the configuration parameters allow dynamic configuration change.

Table 462: Network Profile for Peer OFCS Parameters

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Set of OFCS servers configured	Allowed	No impact



CHAPTER 44

TAI Selection from AMF

- Feature Summary and Revision History, on page 1477
- Feature Description, on page 1477
- How it Works, on page 1478
- Configuring TAI Selection Feature, on page 1480

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 463: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The SMF provides optional configuration to configure locations based on the Tracking Area Identity (TAI) group and priority. When this configuration is available, the SMF sends the configured TAI, that is, TAIList

and TAIRangeList, to the Network Function (NF) Repository Function (NRF) during the SMF service registration. The SMF can register to the NRF with this TAI group and the priority.

Important Any change in the configuration results in SMF Service update towards the NRF with the new configured TAIList and TAIRangeList values.

When the AMF requests a list of SMFs from the NRF, it can make a selection based on the supported location and priority.

For more details on the NF registration and NF registration Update, see the NF Profile Update, on page 893 section in the NF Discovery and Management, on page 877 chapter.

How it Works

The SMF uses priority attribute that is added in the smfInfo data type to enable the discovery and selection of SMF. This functionality is based on the relative priorities registered by the target SMFs in different smfInfo entries with different TAI lists.

The following table lists the feature-specific attributes that are part of NFProfile and SMFInfo data types.

Table 464: NFProfile

smfInfo	SmfInfo	O	0..1	Specific data for the SMF (DNNs).
smfInfoList	map(SmfInfo)	O	1..N	Multiple entries of SmfInfo. This attribute provides additional information to the smfInfo. smfInfoList may be present even if the smfInfo is absent. The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259, with a maximum of 32 characters.
Note The absence of both the smfInfo and smfInfoList attributes in an SMF profile indicates that the SMF can be selected for any S-NSSAI, DNN, TAI, and access type.				

Table 465: SMFInfo

Attribute Name	Data Type	P	Cardinality	Description
sNssaiSmfInfoList	array(sNssaiSmfInfoItem)	M	1..N	List of parameters supported by the SMF per S-NSSAI.

Attribute Name	Data Type	P	Cardinality	Description
taiList	array(Tai)	O	1..N	The list of TAIs the SMF can serve. It contains the non-3GPP access TAI. The absence of this attribute and the taiRangeList attribute indicate that the SMF can be selected for any TAI in the serving network.
taiRangeList	array(TaiRange)	O	1..N	The range of TAIs the SMF can serve. It contains the non-3GPP access TAI. The absence of this attribute and the taiList attribute indicate that the SMF can be selected for any TAI in the serving network.
priority	integer	O	0..1	Priority (relative to other NFs of the same type) in the range of 0-65535, to be used for NF selection for a service request matching the attributes of the SmfInfo; lower values indicate a higher priority. See the precedence rules in the description of the priority attribute in NFProfile, if Priority is also present in the nfServiceList parameters or in NFProfile. The NRF overwrites the received priority value when exposing an NFProfile with the Nnrf_NFDiscovery service.
Note An SMF profile may contain multiple SmfInfo entries, with each entry containing a different list of TAIs and a different priority, to differentiate the priority to select the SMF based on the user location. The priority in SmfInfo has the least precedence, that is. it applies between SMFs or SMF Services with the same priority.				

NOTES:

- SmfInfo in NFProfile is sent if there's no change in configuration (all tai-groups data being sent without priority).
- SmfInfoList map is a new element in NFprofile.
- Each SmfInfoList entry doesn't contain all tai-group-list data. Each element contains entries of the same priority tai-groups per NSSAI.

Note All tai-groups under a slice is expected to be of the same priority.

- If tai-group-list has tai-groups of different priority configured under a slice, tai-groups are logically grouped based on priority. SmfInfo has data of tai-group of one priority and subsequent priority tai-group(s) data in each of SmfInfoList entry.
- If no tai-group is associated with any slice, then old behaviour prevails. If there's tai-group association for few slices and few without, then the smfinfolist entries of slices without tai-group have no TAI details.
- For any tai-group if priority isn't defined, it's grouped separately and sent as a SmfInfo entry or different SmfInfoList entry.
- Key for each SmfInfoList map element is incremental counter string.

Configuring TAI Selection Feature

Configuring TAI Group List

Use the following configuration to configure TAI Group List.

```
config
nssai name nssai_name
   sst sst ssd ssd
   dnn dnn
   tai-group-list tai_group_list
   end
```

NOTES:

- **tai-group-list** *tai_group_list* : Configures TAI group list.

Verifying TAI Group List

Use the following show command to verify TAI Group List:

```
show running-config nssai
```

```
nssai name slice1
sst 02
sdt Abf123
dnn [ dnn1 intershat intershat1 intershat2 ]
tai-group-list [ tai-group-1 tai-group-2 tai-group-3 ]
exit
```

```
nssai name slice2
sst 02
sdt abc456
dnn [ dnn1 intershat ]
tai-group-list [ tai-group-4 tai-group-5 tai-group-6 ]
exit
```

Configuring TAI Group

This section describes how to configure the TAI Group.

Configuring the TAI Group involves the following steps:

- Configuring TAC List, on page 1481
- Configuring TAC Range List, on page 1481

Configuring TAC List

To configure the TAC list within TAI profile, use the following sample configuration.

```
config
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac list [ tac_list_values ]
      end
```

NOTES:

- **mcc** *mcc_value* **mnc** *mnc_value*: Configure the Mobile Country Code (MCC) and Mobile Network Code (MNC).
  - **mcc** *mcc_value*: Specify the Mobile Country Code (MCC). *mcc_value* must be a string in the three-digit pattern.
  - **mnc** *mnc_value*: Specify the Mobile Network Code (MNC). *mnc_value* must be a string in the two-or-three-digit pattern.
- **tac list [** *tac_list_values* **]**: Configure the list of TAC values. For example, [1111 2222 3333]

Configuring TAC Range List

To configure the TAC range list within TAI profile, use the following sample configuration.

```
config
   profile tai-group tai_group_name
      mcc mcc_value mnc mnc_value
      tac range start start_value end end_value
      end
```

NOTES:

- **tac range start** *start_value* **end** *end_value*: Configure a specific TAC range or multiple TAC range lists. For example, **tac range start DDDD end EEEE**

  You can configure a maximum of 16 values in a range.

- Use the **no tac range start** *start_value* **end** *end_value* command to remove a specific TAC range or TAC ranges.

Verifying the TAI Group Configuration

To verify the TAI group configuration, use the following command:

show running-config profile tai-group *tai_group_name*

The following is an example of the configuration:

```
show running-config profile tai-group t1
profile tai-group t1
mcc 111 mnc 222
  tac list [ 1111 2222 3333 ]
  tac range start 4444 end 5555
  exit
exit
mcc 333 mnc 44
  tac list [ AAAA BBBB CCCC ]
  tac range start DDDD end EEEE
  exit
exit
exit
```

Configuring Priority

To configure the priority of TAI group, use the following sample configuration:

```
config
profile tai-group tai_group_name
   priority priority
   end
```

NOTES:

- **priority** *priority* : Specify the priority of the TAI group.

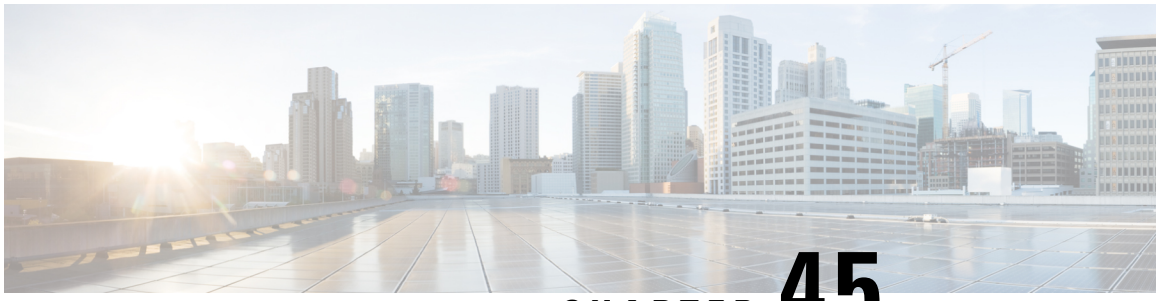
Verifying the Priority Configuration

To verify the configuration associated with TAI group priority, use the following show command:

show running-config profile tai-group

```
profile tai-group t1
mcc 123 mnc 456
priority 1
tac list [ 1234 789123 ]
tac range start 1234 end 1980
exit
exit
exit
profile tai-group t2
priority 1
mcc 456 mnc 123
tac list [ 0000 123456 ]
tac range start 3456 end 9000
exit
```

```
exit
exit
```



CHAPTER 45

UDM Integration

- Feature Summary and Revision History, on page 1485
- Feature Description, on page 1486
- How it Works, on page 1486
- Configuring UDM, on page 1486
- N10 Fail Open on Converged Core, on page 1489
- Configuration-based Control of Subscription Messages, on page 1490
- Configuration-based Control of UDM Registration Messages, on page 1492

Feature Summary and Revision History

Summary Data

Table 466: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Product(s) or Functional Area	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 467: Revision History

Revision Details	Release
Added the N10 fail open support.	2023.04.0
First introduced.	2020.02.2

Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network. The SMF explicitly subscribes to receive the notifications about the events that occur in the subscriber data such session terminate.

The N10 interface is between Unified Data Management (UDM) and SMF (Session Management Function). The UDM provides the following services to SMF via the Nudm interface:

- Nudm_SubscriberDataManagement Service
- Nudm_UEContextManagement Service

How it Works

This section describes how this feature works.

When the SMF skips UDM subscription, then it stops sending the following messages:

- Fetch-Subscription during session establishment
- Subscribe-for-Notification during session establishment
- Unsubscribe-to-Notification during session release and when the UDCM receives the UECM messages

The SMF allows any dynamic changes to the UDM subscription skip configuration. That is, new value is applicable for the new session being established. The existing sessions continue to use the old values.

Configuring UDM

This section provides all the configurations related to UDM:

Configuring Options for Controlling SDM Messages

This section describes how to configure controlling Subscription Data Management (SDM) messages over the N10 interface.

Configuring RAT Type

To configure the RAT type with the local authorization under the DNN profile, use the following sample configuration:

```
config
   profile dnn dnn_profile
      authorization local rat-type [ nr | eutra | wlan ]
      end
```

NOTES:

- **authorization local**: This command skips the SDM messages for EPS sessions only. Upon configuring this command under the selected DNN profile, the SMF skips the UDM interaction for fetch subscription. The SMF uses the values received in the Create Session Request message. The SMF skips the UDM interaction to receive 'Subscribe-for-Notifications' from the UDM.
- **rat-type [nr | eutra | wlan]**: This keyword skips the following SDM messages based on the specified RAT type.
  - udm subscription-fetch
  - subscribe-to-notifications
  - unsubscribe-to-notifications

  Upon configuring the RAT type with **authorization local** command in the selected DNN profile, then for sessions on that RAT-type, the SMF skips the UDM interaction for the following messages:
  - udm subscription-fetch during session establishment
  - subscribe-for-notifications during session establishment
  - unsubscribe-for-notifications during session release
- **no authorization local rat-type [nr | eutra | wlan]**: Disables the local authorization under the DNN profile.

Configuration Verification

To verify the configuration, use the **show running-config profile dnn** *dnn_profile_name* command.

The output of this show command displays all the configurations including the RAT type information that is configured within the specified DNN profile.

```
[smf] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV6 allowed [ IPV6 ]
authorization local rat-type nr
upf apn intershat
dcnr true
exit
```

Configuring Session Type

The SMF uses both subscription type data from UDM response and the session type configuration in DNN profile to allow or reject the call. The SMF selects the session type based on the initial look up of UE-requested PDN type in the UDM subscription data. Then, the SMF provisions session type for the session based on the selected session type and the session type configured in the DNN profile.

To configure the PDU session type in DNN profile, use the following sample configuration.

```
config
   profile dnn dnnprofile
```

```
      session type { IPV4 | IPV4V6 | IPV6 } allowed [ IPV4 | IPV4V6 |
IPV6 ]
      end
```

NOTES:

- **session type { IPV4 | IPV4V6 | IPV6 } allowed [IPV4 | IPV4V6 | IPV6]**: Specify the IP type for the PDU session. The **allowed** keyword allows you to specify two IP types other than the default session type.
- The SMF uses this session type configuration to process the call. For example, if the UE requested type is IPv4 and the UDM subscription type is IPv4v6, the SMF selects IPv4 in the first pass and subsequently checks against the session type configuration. If the configured session type is IPv6, then the SMF rejects the call with a cause "#51 - PDU session type IPv6 only= IPV4 allowed".
- If the IPAM configuration includes the IP address pool that is different from the finally selected PDU session type, the SMF rejects the call with a cause "#31 - request rejected, unspecified". For example, this cause value will be generated under the following conditions:
  - UeReq-PdnType = V4
  - UdmSubscription-PdnType = V4V6
  - SessionType-Config = V4V6
  - IP-Pool = V6

Configuration Verification

To verify the configuration, use the **show running-config profile dnn** *dnn_profile_name* command.

The output of this show command displays all the configurations including the session type information that is configured within the specified DNN profile.

```
[smf] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV6 allowed [ IPV6 ]
upf apn intershat
dcnr true
exit
```

Configuration to Disable Optional IEs

To disable optional IEs such as **epdgInd** and **registrationTime** attributes in the N10 Registration Request, use the following sample configuration:

```
config
  profile message-handling nf-type nf_ype
    mh-profile mh_profile_name
    service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau |
```

```
nudm-uecm }
     message type { UdmRegistrationReq | UdmSdmGetUESMSubscriptionData |
 UdmSdmSubscribeToNotification | UdmSdmUnsubscribeToNotification |
UdmSubscriptionReq | UdmUecmRegisterSMF skip optional-ies [ epdgInd |
registrationTime ] | UdmUecmUnregisterSMF }
    exit
  exit
exit
```

NOTES:

- **mh-profile** *mh_profile_name*: Specify the name of the message handling profile.
- **skip optional-ies [epdgInd | registrationTime]** : Skips ePDG indication and registration time in the Registration Request.

Note The **skip optional-ies [epdgInd | registrationTime]** command is available only with the UdmUecmRegisterSMF message.

N10 Fail Open on Converged Core

Table 468: Feature History

Feature Name	Release Information	Description
Minimizing SMF and UDM interactions on N10 interface through fail open support	2023.04	With the fail open feature, the SMF supports the ignore and continue failure handling actions as well for the call during the N10 message failures. These failures include the UDM registration, Subscriber Fetch, and Subscribe to Notify for all RAT types.

Feature Description

This feature provides the following support:

- Fail open—The SMF supports the ignore and continue failure handling actions as well for the call during the N10 message failures. These failures include the UDM registration, Subscriber Fetch, and Subscribe to Notify for all RAT types, which are LTE, NR and Wi-Fi.

  If the registration isn't performed or failed during the session creation, then based on the configured failure handling action, the SMF performs the N10 registration during handover. The failure handling action can either be ignore or continue. If you haven't configured the failure action to terminate the session, and the failure happens during handover, then SMF ignores the failure and continues with the handover procedure.

- Interaction with SCP Model-D—If you have configured the SCP failure handling as continue or ignore, then the preceding failure handling is applicable. If you have configured the SCP failure handling as a fallback and a failure happens after the fallback, then the action that you configured under UDM failure handling is applicable.

Configuration-based Control of Subscription Messages

Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network. The SMF explicitly subscribes to receive the notifications about the events that occur in the subscriber data such session terminate. When the SMF wants to stop receiving the notifications, it initiates the Unsubscribe-to-Notification messages to UDM. Upon receiving these messages, the UDM cancels the subscription by removing the notification subscription for the subscribed session.

Note The SMF does not receive notification when the UDM-triggered subscription change is observed. However, for UDM-triggered session terminations, the SMF receives notifications from UDM.

How it Works

This section provides a overview of how the SMF and UDM communicate over the Unsubscribe-to-Notifications message:

1. The NF, such as SMF, sends an Unsubscribe-to-Notifications request to the resource identified by the URI to the UDM. The SMF transacts the request to the UDM over the N10 interface. The Unsubscribe-to-Notifications request allows the SMF unsubscribe from notifications for a specific subscriber session. The SMF receives the URI details during the subscription creation process.

   The Unsubscribe-to-Notifications request contains the ‘SUPI’ and ‘subscriptionId’ in the URI.

2. The UDM processes the request, and based on the response; it sends a response code to the SMF. For example, if the unsubscription is successful, then UDM sends 204 code. If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the response body along with the additional error information.

3. The SMF handles the timeout and failure that occurs when sending the Unsubscribe-to-Notifications messages to the UDM. In case the Unsubscribe-to-Notifications request fails, the SMF continues to purge the corresponding sessions.

   The Unsubscribe-to-Notification message is required for sessions that are hosted on the EUTRA network. Being on this network may not be a requirement for sessions that are released on the NR and WLAN network. For these access types, the SMF sends the UDM registration and deregistration messages that include subscription to notifications through implicit-unsubscribe during the deregistration.

Standards Compliance

The Support for the Unsubscribe-To-Notifications Messages feature complies with the following standards:

- *3GPP TS 29.503 - 5G System; Unified Data Management Services*

Call Flows

This section describes the call flow for the Unsubscribe-To-Notifications message support.

Unsubscribe-to-Notifications Call Flow

This section describes the call flow on how the SMF sends a request to the UDM to unsubscribe from notifications of data changes.

Figure 267: Unsubscribe-to-Notifications Communication with UDM

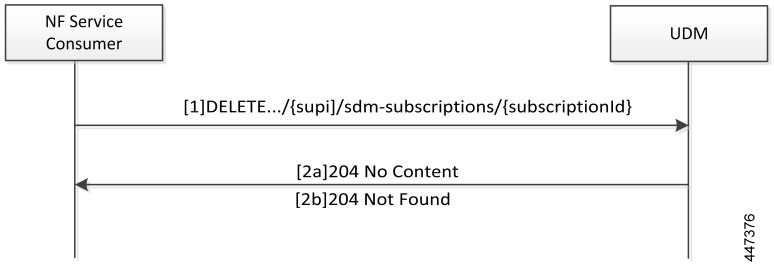


Table 469: Unsubscribe-to-Notifications Communication Call Flow Description

Step	Description
1	The NF service consumer, such as SMF, sends a request to the UDM to unsubscribe from notifications. By unsubscribing, the UDM no longer sends notifications to SMF when the data modifications occur in the respective subscriber session. The NF service consumer sends a DELETE request to the resource identified by the URI. The NF service consumer receives the URI when the subscription gets created.
2a	If the deletion of request is successful, the UDM responds with "204 No Content".
2b	If the subscription is invalid, which can be due to an unknown subscriptionId value, then the HTTP status code "404 Not Found" is returned along with the additional error information in the response body (as part of the "ProblemDetails" element). If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the DELETE response body along with the additional error information.

OAM Support for the Unsubscribe-To-Notifications Messages

This section describes operations, administration, and maintenance information for this feature.

Statistics Support

The SMF maintains the following labels on the smf-rest-ep pod for monitoring the number of unsubscribe-to-notifications messages that are initiated towards UDM:

- nfType – “udm”
- messageDirection – “outbound”
- apiName – “sdm_unsubscription_req”
- nfUri – “nf_uri”
- respStatus – “response_status”
- rspCause – “response_cause”

Configuration-based Control of UDM Registration Messages

Table 470: Feature History

Feature Name	Release Information	Description
Configuration-based Control of UDM Registration Messages	2024.01.2	SMF allows the user to ignore the UDM registration messages during the PDU setup and Wi-Fi attach procedures. With this controlled UDM registrations, the interactions between SMF and UDM over the N10 interface are minimized to handle the message overload and attach failures on the N10 interface. This feature introduces the new CLI command **skip-n10-registration rat-type [NR | WIFI | ALL]** in the DNN profile. **Default Setting:** Disabled – Configuration Required

Feature Description

When the UE attach failures are caused by message overload on N10 interface, SMF ignores the UE registration messages from reaching the UDM. This feature optimizes the N10 interactions in the 5G and Wi-Fi network. You can configure this feature through the **skip-n10-registration rat-type [NR | WIFI | ALL]** CLI command.

How it Works

When you configure the **skip-n10-registration rat-type [NR | WIFI | ALL]** CLI command, SMF ignores the UDM registration during session creation in the 5G and Wi-Fi network. The handover between 5G and Wi-Fi fails because ePDG doesn't find the target SMF that was handling the session. If the UE registration fails during 5G or Wi-Fi attach and if the UDM failure handling template (FHT) is configured as continue or ignore, then SMF reattempts the registration during Wi-Fi-to 5G and 5G to Wi-Fi handovers.

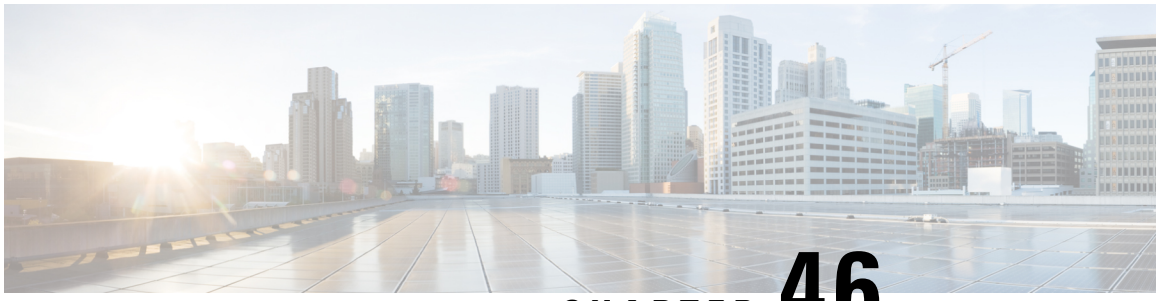
Configuring Control for UDM Registration Messages

To control the UDM registration messages, use the following sample configuration:

```
config
   profile dnn dnn_profile
      skip-n10-registration rat-type [ NR | WIFI | ALL ]
      exit
```

NOTES:

- **skip-n10-registration rat-type [NR | WIFI | ALL]**: Specify the RAT type for which you want to ignore the UDM registration.



CHAPTER 46

UP Session Activation and Deactivation Service Request Procedures

- Feature Summary and Revision History, on page 1495
- Feature Description, on page 1496
- UE-initiated Service Request Procedure, on page 1496
- Network-initiated Service Request Procedure, on page 1500
- Always-On PDU Session Support, on page 1512
- DLDR Handling for N3 Connection Reactivation, on page 1519

Feature Summary and Revision History

Summary Data

Table 471: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 472: Revision History

Revision Details	Release
IPv6 address support introduced to UPF tunnel end point address.	2022.04.0
Introduced support for the selection of UPF nodes based on the query parameters, such as DNN, location, and PDU session type.	2020.03.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

Connection Management (CM) includes the functions to establish and release a NAS signaling connection between a UE and the Access and Mobility Management Function (AMF) over the N1 interface. This signaling connection enables the NAS signaling exchange between the UE and the core network.

The 5GS CM states determine the NAS signaling connection of the UE with the AMF. The following are the CM states:

- **CM-Idle**—When a UE is in the CM-Idle state, the UE has no NAS signaling connection established with the AMF over the N1 interface. The AN signaling connection, N2 connection, and N3 connection do not exist in this state.
- **CM-Connected**—When a UE is in the CM-Connected state, the UE has a NAS signaling connection with the AMF over the N1 interface. A NAS signaling connection uses an RRC Connection between the UE and the NG-RAN and an NGAP UE association between the AN and the AMF for the 3GPP access.

The CM states for the 3GPP access and the non-3GPP access are independent of each other. It implies that both the access can be in the CM-Idle state and the CM-Connected state simultaneously.

The SMF supports the UE idle-to-active and active-to-idle transition procedures.

UE-initiated Service Request Procedure

The UE in CM-IDLE state initiates the Service Request procedure to send uplink signaling messages, user data, or as a response to a network paging request. After receiving the Service Request message, the AMF performs authentication. After the establishment of the signaling connection to an AMF, the UE or network sends signaling messages, for example, PDU session establishment from UE to the SMF, through the AMF.

The Service Request procedure is used by a UE in CM-CONNECTED to request activatation of a User Plane connection for PDU sessions and to respond to a NAS Notification message from the AMF. When a User Plane connection for a PDU session is activated, the AS layer in the UE indicates it to the NAS layer.

Feature Description

The SMF supports activation and deactivation of the user plane connection of a PDU session.

The Activation or Deactivation Service Request procedure is used by a UE in CM-IDLE state or the 5GC to request the establishment of a secure connection to an AMF. The Service Request procedure is also used both when the UE is in CM-IDLE and in CM-CONNECTED to activate a User Plane connection for an established PDU session.

Note The UE will not initiate a Service Request procedure if there is an ongoing Service Request procedure.

How it Works

This section describes how this feature works.

Deactivation of the User Plane Connection of a PDU Session

The deactivation procedure releases the logical NG-AP signaling connection and the associated N3 user plane connections, and (R)AN RRC signaling and resources.

The following reasons can trigger the initiation of AN release:

- (R)AN-initiated with cause

  For example, O&M intervention, unspecified failure, (R)AN (for example, Radio) link failure, user inactivity, inter-system redirection, request for establishment of QoS flow for IMS voice, release due to UE-generated signaling connection release, mobility restriction, and so on.

- AMF-initiated with cause

  For example, unspecified failure.

Limitations

The User Plane Deactivation functionality has the following limitations:

- SMF supports only UE-initiated deactivation.
- Location update is not supported.

Call Flow

This section describes the call flow for the User Plane Deactivation of a PDU session.

The following figure illustrates the User Plane Deactivation call flow.

Figure 268: Deactivation of the User Plane Connection Call Flow

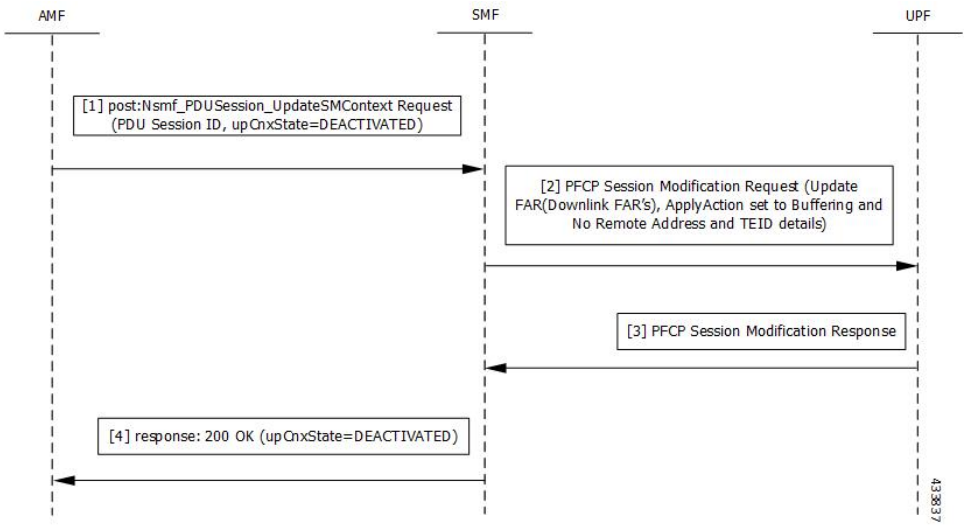


Table 473: Deactivation of the User Plane Connection Call Flow Description

Step	Description
1	NF Service Consumer requests the SMF to deactivate the user plane connection of the PDU session by sending a POST request with the following information: • upCnxState attribute set to DEACTIVATED. • User location and user location timestamp. • Cause of the user plane deactivation. The cause may indicate a cause received from the 5G-AN or due to an AMF internal event. • Other information (if required).
2	SMF deactivates and releases the N3 tunnel of the PDU session after receiving such a request. SMF initiates the PFCP Session Modification procedure towards UPF with downlink FAR updated with the following options: • Buffering Action is enabled without remote node "forwarding parameters" details, such as IP address and GTP-U F-TEID. **Note** NOCP (Notify the CP function) is not enabled. Support for notification is not supported on SMF.
3	SMF sets the upCnxState attribute to DEACTIVATED for the PDU session after receiving successful response from the UPF node.
4	SMF initiates a 200 OK response towards AMF including the upCnxState attribute set to DEACTIVATED.

Activation of the User Plane Connection of a PDU Session

The Service Request procedure is used when the UE is in CM-IDLE and CM CONNECTED states to activate a user plane connection for an established PDU session. The UE in CM IDLE state initiates the Service Request procedure to send uplink signaling messages, user data, or a response to a network paging request.

Call Flow

This section describes the call flow for the user plane activation of a PDU session.

The following figure illustrates the UE-initiated user plane activation call flow.

Figure 269: User Plane Connection Activation Call Flow

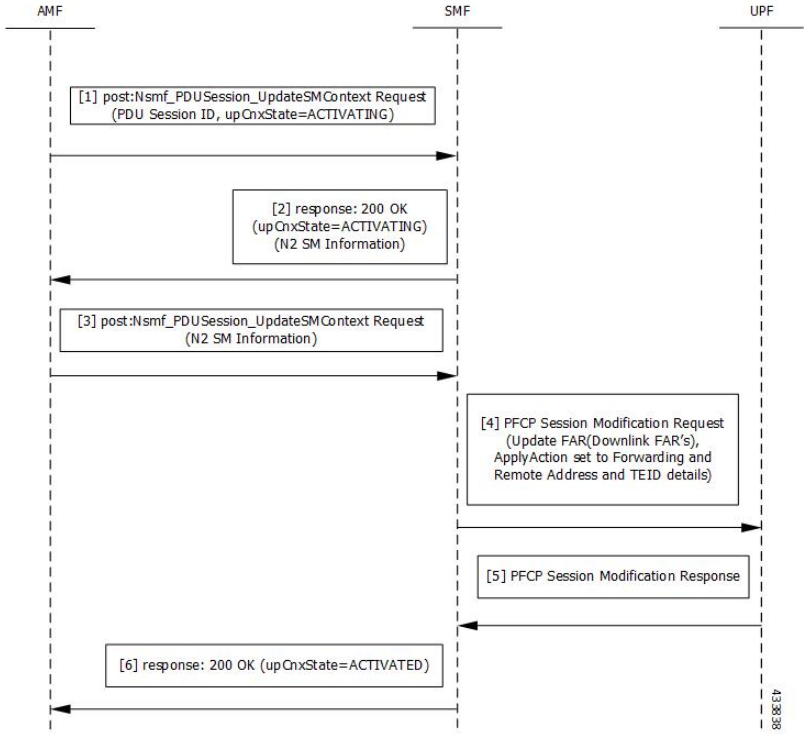


Table 474: UE-initiated Idle to Active Transition Call Flow Description

Step	Description
1	The AMF requests SMF to activate the user plane connection of the PDU session by sending a POST request with the following information: • upCnxState attribute set to ACTIVATING. • User location, user location timestamp, and access type associated to the PDU session (if modified) • Other information (if necessary)

2	Upon receipt of the request, the SMF starts activating the N3 tunnel of the PDU session. The SMF returns a 200 OK response with the following information:
	• upCnxState attribute set to ACTIVATING
	• N2 SM information with the following information to request the 5G-AN to assign resources to the PDU session.
	  • Transport layer address (IPv4 or IPv6 address of the UPF)
	  • Tunnel endpoint of the uplink termination point for the UP data of current PDU session (that is, GTP-U F-TEID of UPF for uplink traffic)

Step	Description
3	Then, the AMF requests the SMF by sending POST request with the N2 SM information. If the 5G-AN succeeded in establishing resources for the PDU sessions, the N2 SM information includes the following information: • Transport layer address • Tunnel endpoint of the downlink termination point for the user data of the current PDU session. That is, GTP-U F-TEID of 5G-AN for downlink traffic.
4	The SMF initiates PFCP Session Modification procedure towards UPF with downlink FAR updated with the following options: • Forwarding Action enabled along with remote node forwarding parameter details, such as the IPv4 or IPv6 address of RAN and GTP-U F-TEID.
5	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
6	The SMF initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF.

Network-initiated Service Request Procedure

The network-initiated service request procedure is used when the peer network needs to communicate (for example, User Plane connection activation for PDU sessions to deliver mobile terminating user data) with a UE. If the UE is in CM-IDLE state or CM-CONNECTED state in 3GPP access, the network initiates a Network Triggered Service Request procedure. If the UE is in CM-IDLE state, and asynchronous type communication is not activated, the network sends a Paging Request to (R)AN or UE. The Paging Request triggers the UE Triggered Service Request procedure in the UE. If asynchronous type communication is activated, the network stores the received message and forwards the message to the (R)AN and/or the UE (that is, it synchronizes the context with the (R)AN and/or the UE) when the UE enters CM-CONNECTED state.

Feature Description

The SMF sets up N3 tunnel to forward downlink packet to the UE for a PDU session when the UE is in the CM-Idle state.

The N3 tunnel profile helps in defining the Forwarding Action Rules (FAR) while moving from active to idle transition state.

The N3 tunnel profile configuration includes:

- Enabling control plane notification (notify)
- Enabling packet buffering on UPF (buffer UPF)

How it Works

When connected to the 5G core, a UE can be in CM-Connected with RRC Inactive state too. This state is between the CM-Idle and CM-Connected states.

The SMF cannot identify the UE CM state when the state is between UE and AMF. The SMF only identifies the user plane connection state. This state and the N1 and N2 transfer message response status control the behavior of SMF for network-initiated messages. These messages are for signaling modification or downlink data-related user plane activation procedures.

The following call flows describe the details for these procedures.

Call Flows

This section describes the following call flows:

- Network-initiated Idle to Active Transition Call Flow, on page 1501
- Network-initiated Service Request Rejection Call Flow, on page 1504
- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State
- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

Network-initiated Idle to Active Transition Call Flow

The following figure depicts the network-initiated idle to active transition call flow.

Figure 270: Network-initiated Idle to Active Transition Call Flow

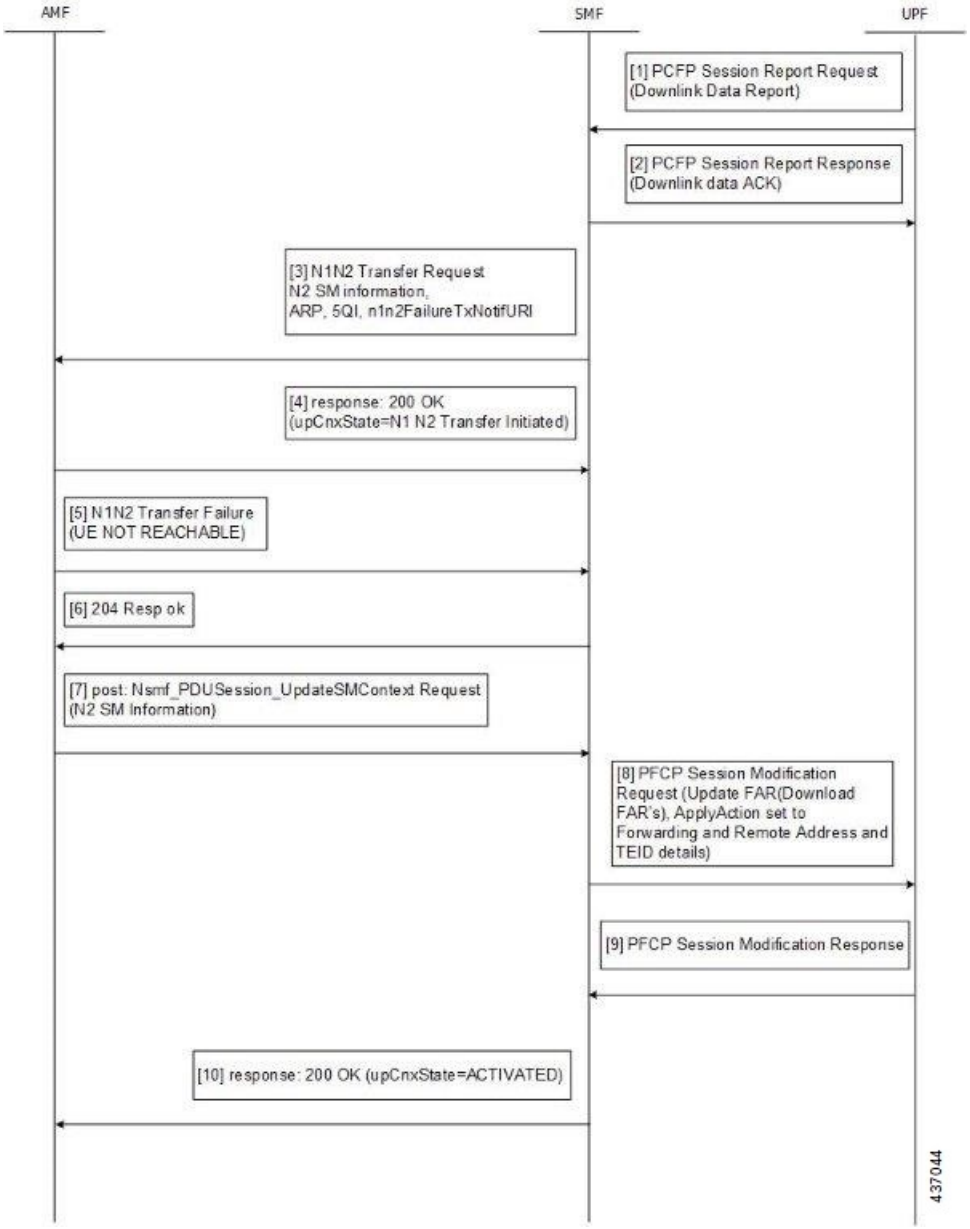


Table 475: Network-initiated Idle to Active Transition Call Flow Description

Step	Description
1	The UPF sends PFCP Session Report request to the SMF. • Report Type as DLDR (Downlink Data Report) • The Downlink Data Report IE contains corresponding PDR ID.
2	The SMF sends the PFCP Session Report response.

Step	Description

3	The SMF sends N1N2MessageTransfer to AMF with the following attributes:
	• SUPI, PDU Session ID
	• N2SMInformation as "ngapIeType":77 (id-PDUSessionResourceSetupListSUReq), "ngapMessageType":27 (id-PDUSessionResourceSetup)
	• PDUSessionResourceSetupListSUReq includes the following information:
	  • PDU session id
	  • QFI
	  • QoS profile
	  • GTP-U F-TEID of UPF for uplink traffic
	  • QFI
	  • QoS profile
	  • S-NSSAI
	  • User Plane Security Enforcement
	  • UE Integrity Protection Maximum Data Rate
	  • Cause
	• Area of validity for N2 SM information
	• ARP
	• Paging Policy Indication
	• 5QI
	• N1N2TransferFailure Notification Target Address (n1n2FailureTxfNotifURI)

4	The SMF receives N1N2 Transfer Response with the following status codes: • 200/202 OK and cause as "N1_N2_TRANSFER_INITIATED" (proceed to Step 6) • 409/504 and cause “UE_IN_NON_ALLOWED_AREA” (proceed to Step 7)
5	The AMF sends the N1N2 Transfer failure response. If the UE is not reachable, proceed to Step 7.

6	Then, the AMF requests the SMF by sending POST request with the following information:
	• N2 SM information received from the 5G-AN includes the following information if the 5G-AN succeeded in establishing resources for the PDU sessions.
	  • Transport layer address (IPv4 or IPv6 address of UPF)
	  • Tunnel endpoint of the downlink termination point for the user data for the current PDU session (that is, GTP-U F-TEID of 5G-AN for downlink traffic)

Step	Description

7	The SMF initiates PFCP Session Modification procedure towards UPF with downlink FAR updated with the following options:
	• If N2 Transfer is successful, Forwarding Action is enabled along with remote node forwarding parameter details, such as the IPv4 or IPv6 address of RAN and GTP-U F-TEID.
	• If the cause of transfer failure is ATTEMPTING_TO_REACH_UE or UE_IN_NON_ALLOWED_AREA:
	  • Update FAR > Apply Action > NOCP: 1
	  • Update FAR > Apply Action > DROP: 1
	  • PFCPSMReq-Flags > DROBU: 1
	• If the cause of transfer failure is UE_NOT_REACHABLE:
	  • Update FAR > Apply Action > NOCP: 0
	  • Update FAR > Apply Action > DROP: 1
	  • PFCPSMReq-Flags > DROBU: 1

8	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
9	The SMF then initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF (only if Step 6 is completed and response is received from Step 8).

Network-initiated Service Request Rejection Call Flow

During network-initiated service request, SMF handles the temporary reject for N1N2 response message from AMF as mentioned in 3GPP TS 23.502, section 4.2.3.3.

Figure 271: Temporary Rejection Call Flow for Network-triggered Service Request - 1

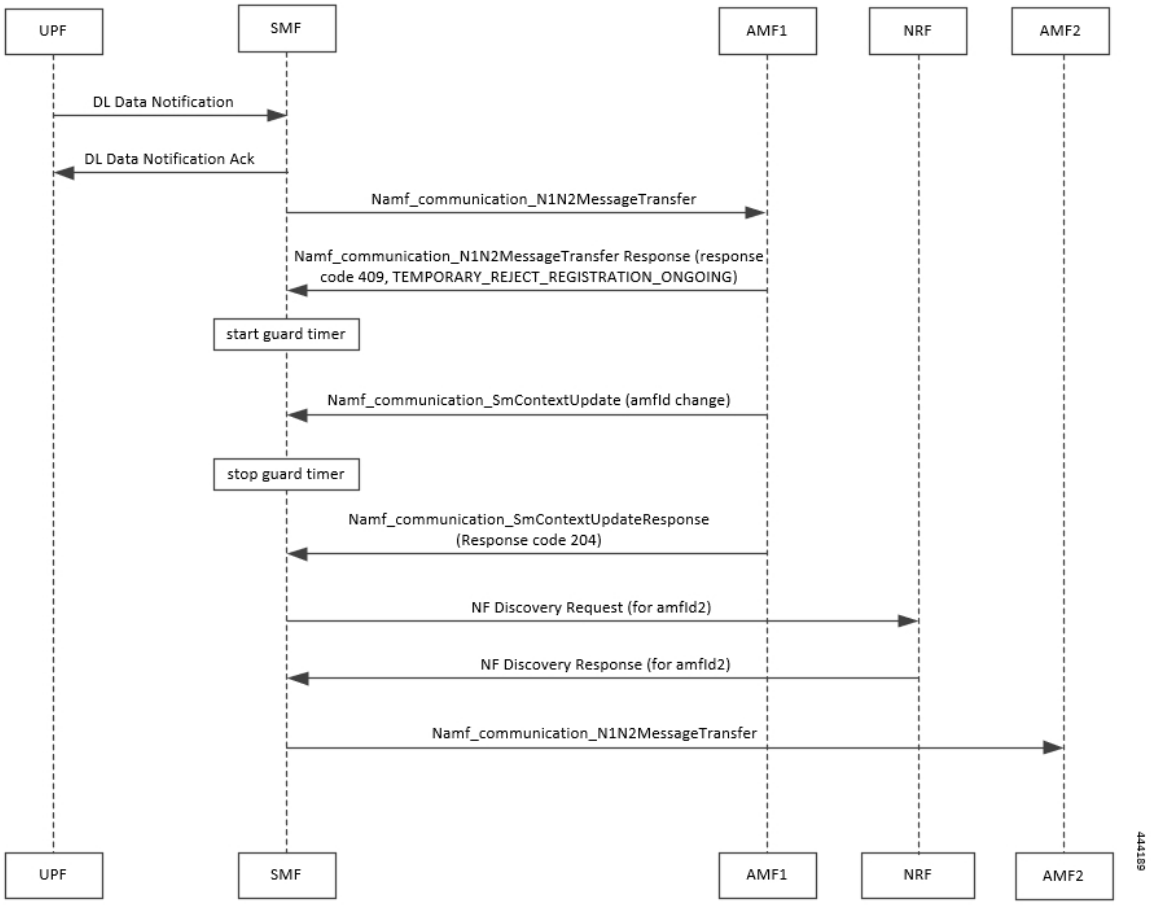


Table 476: Temporary Rejection Call Flow Description for Network-triggered Service Request - 1

Step	Description
1	On receiving a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of idle mode exit procedure.
2	If UE registration procedure with new AMF is in progress, then AMF responds with temporary reject for N1N2 message with response code 409 and cause as TEMPORARY_REJECT_REGISTRATION_ONGOING or TEMPORARY_REJECT_HANDOVER_ONGOING SMF.
3	On receiving the response, SMF starts a locally configured guard timer of 2 seconds.
4	While the guard timer is running, SMF expects either a SM Context Update with AMF ID change or SM Context Update for handover.

Step	Description
5	On receiving SM Context Update with AMF ID change, SMF: **1.** Stops the guard timer. **2.** Removes the reference to the discovery information for old AMF. **3.** Stores the new UE location information, PLMN information, and AMF information. **4.** Sends SM Context Update response success without content. **5.** Reinitiates N1N2 message transfer to the new AMF. This involves NF discovery and subsequent transmission to the new AMF.
6	On receiving SM Context Update for N2 handover, SMF: **1.** Starts the handover procedure. **2.** Suspends the idle mode exit procedure and stops the guard timer. **3.** Removes old AMF details and stores new AMF information as part of the handover procedure completion. **4.** Resumes idle mode exit procedure after handover procedure is complete. **5.** Reinitiates N1N2 message transfer, if required, to the new AMF. This involves NF discovery and subsequent transmission to the new AMF.

Figure 272: Temporary Rejection Call Flow for Network-triggered Service Request - 2

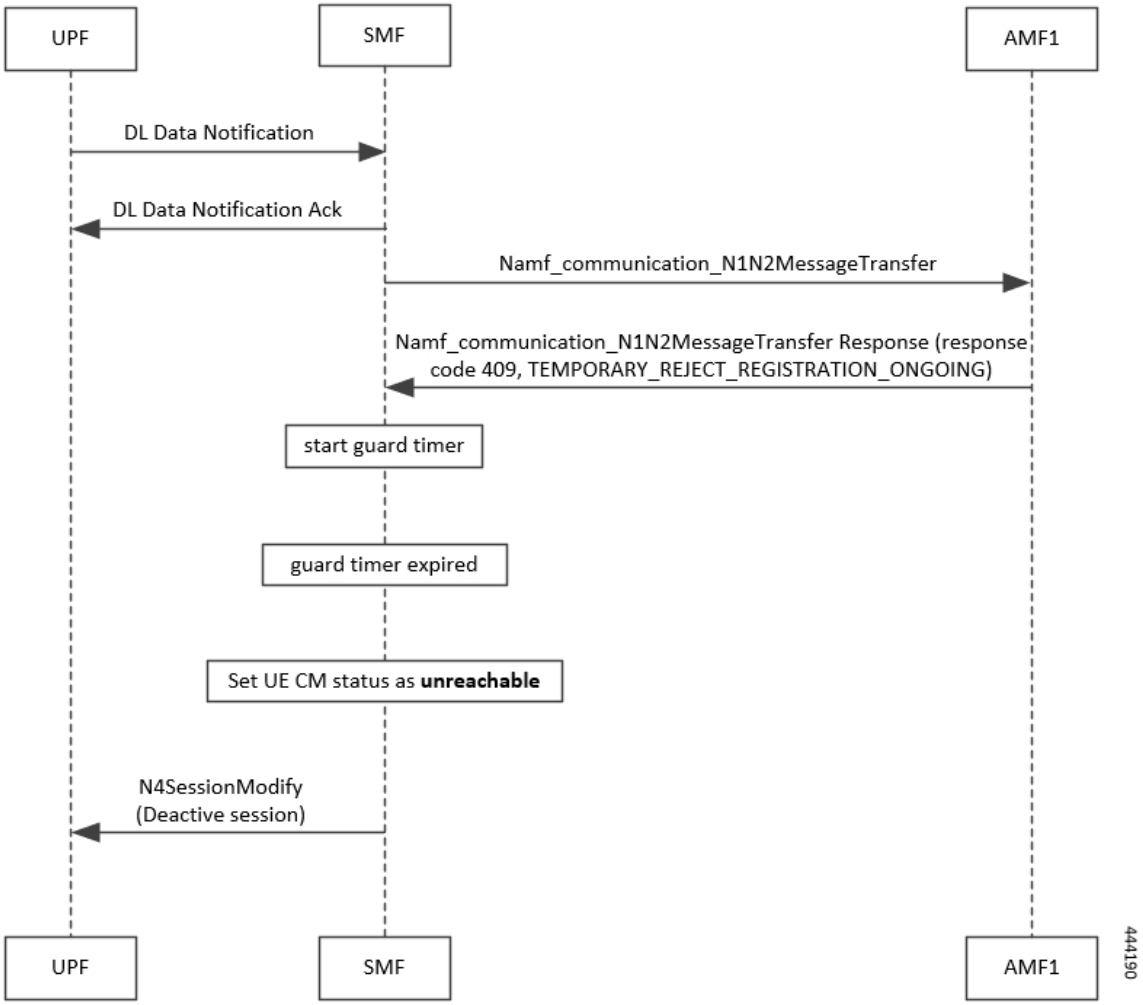


Table 477: Temporary Rejection Call Flow Description for Network-triggered Service Request - 2

Step	Description
1	On receiving a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of idle mode exit procedure.
2	If UE registration procedure with new AMF is in progress, then AMF responds with temporary reject for N1N2 message with response code 409 and cause as TEMPORARY_REJECT_REGISTRATION_ONGOING or TEMPORARY_REJECT_HANDOVER_ONGOING SMF.
3	On receiving the response, SMF starts a locally configured guard timer of 2 seconds.
4	Once the guard timer expires, SMF: **1.** Sets the UE CM status as *NotReachable*. **2.** Deactivates the UP session state.

Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

This section describes the user plane activation procedure for notification of downlink data when the UE is in the CM-Connected state.

The following figure depicts the downlink data notification user plane activation call flow when the UE is in CM-Connected state.

Figure 273: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

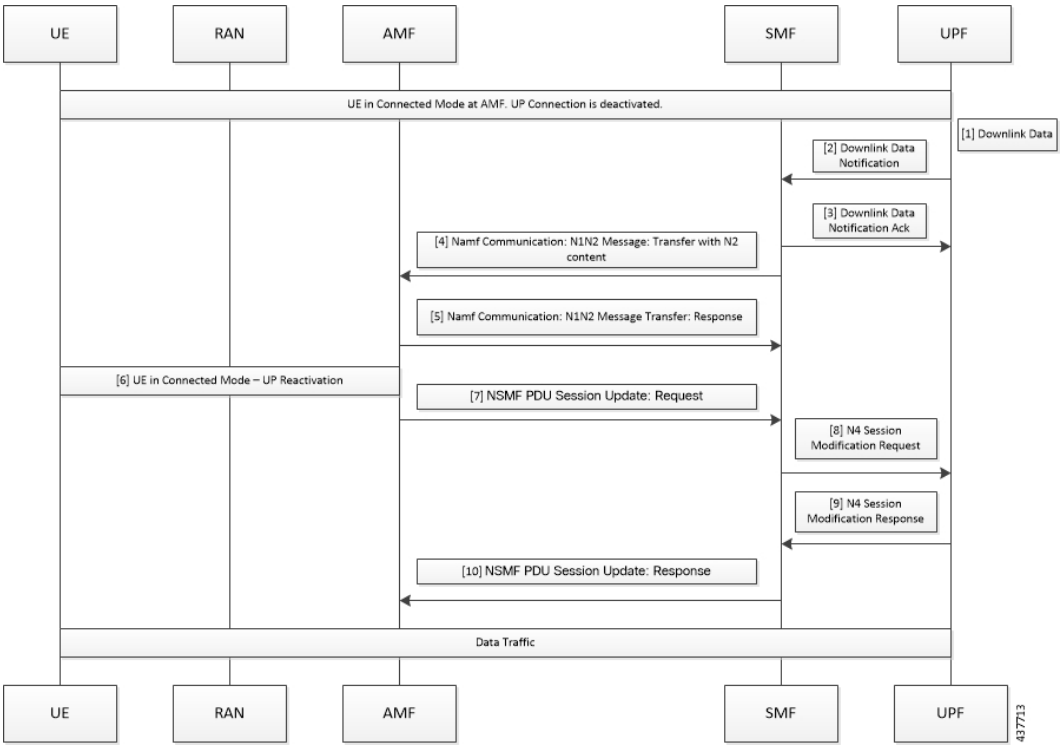


Table 478: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Connected State

Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, the UPF buffers the downlink data. The buffering is done based on the instruction from the SMF.
2	The UPF sends data notification towards SMF. This notification includes the N4 session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgment data notification to the UPF.

Step	Description
4	The SMF initiates the NAMF communication N1 and N2 message transfer towards the AMF. This message transfer includes the following details: • PDU session ID • N2 SM information (QFIs, QoS profiles) • CN N3 tunnel information • S-NSSAI • ARP • Paging Policy Indicator • 5QI • N1 and N2 transfer failure notification target address • PDU session resource setup request IE
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and the “N1_N2_TRANSFER_INITIATED” cause.
6	The User Plane Reactivation procedures begin. The reactivation procedures set up the radio resources and activate the user plane to establish the N3 tunnel.
7	The AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N2 interface. The connection state of user plane is Activated.
8	The SMF sends the N4 modification procedure toward the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and the set forward action.
9	The UPF modifies the session and sends the acknowledgment of the modification to the SMF.
10	The SMF responds to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with the connection state of user plane as Activated.

NOTES:

The following N1 and N2 response error cases are handled:

- For 404 Context Not Found status, a PDU session is released.
- For 504 or 403 status with the "UE_IN_NON_ALLOWED_AREA" and "NOT_REACHABLE" cause, an N4 modification request is sent to drop the buffered packets and exclude the CP notification for the downlink data.
- For the N1and N2 transfer notification failure, the N4 modification request is sent to drop the buffered packets and exclude the CP notification for downlink data.
- For 409 status code with the Retry After timer value, the N1 and N2 transfer is re-initiated after the timeout value.
- For the 409 status code with "HIGHER_PRIORITY_REQUEST_ONGOING" cause, the lower priority N1 and N2 transfers are not allowed. Only the higher priority transfers are communicated to the AMF.

Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

This section describes the user plane activation procedure for notification of downlink data when the UE is in the CM-Idle state.

The following figure depicts the downlink data notification user plane activation call flow when the UE is in CM-Idle state.

Figure 274: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

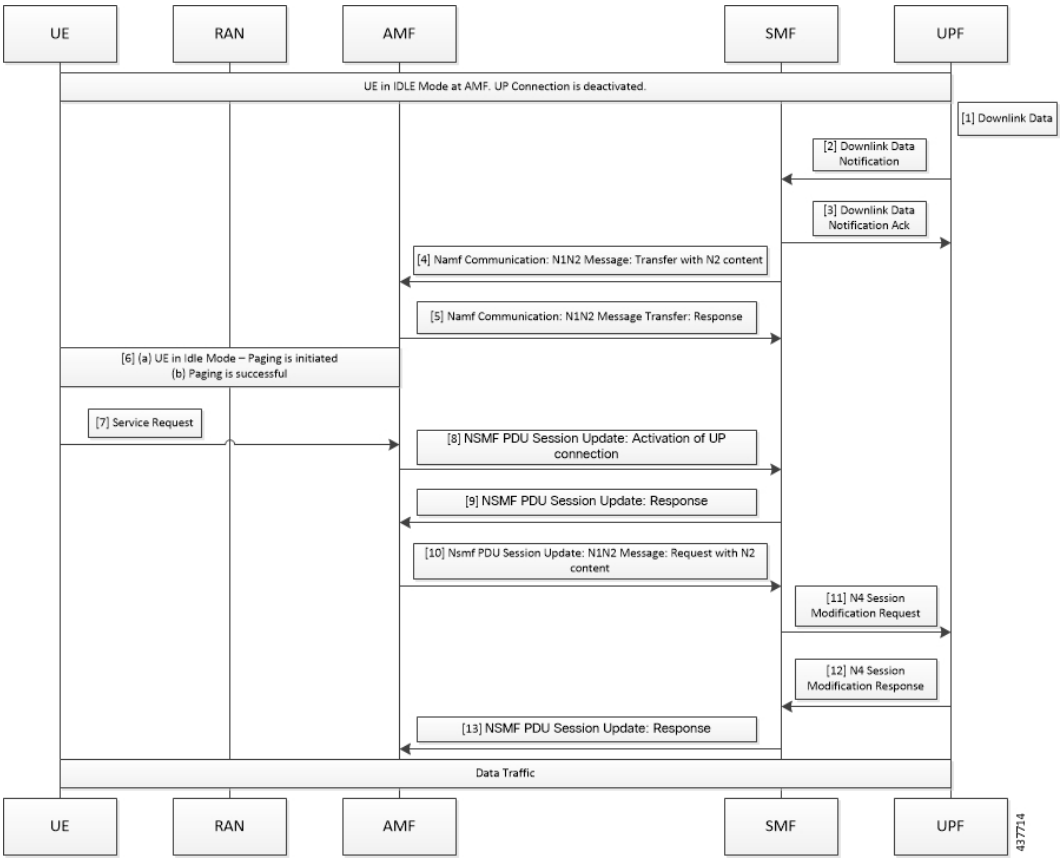


Table 479: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Idle State

Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, then based on the instruction from the SMF, the UPF buffers the downlink data.
2	The UPF sends data notification towards the SMF. This notification includes the N4 Session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgment data notification to the UPF.

Step	Description
4	The SMF initiates the NAMF communication N1 and N2 message transfer toward AMF. This message transfer includes the following details: • PDU session ID • N2 SM information (QFIs, QoS profiles) • CN N3 tunnel information • S-NSSAI • ARP • Paging Policy Indicator • 5QI • N1 and N2 transfer failure notification target address
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “202 Accepted” status code and “ATTEMPTING_TO_REACH_UE” cause.
6	The AMF triggers the paging procedure towards the UE.
7	The UE receives the paging request and initiates the requested service to activate the session.
8	The AMF initiates the NSMF PDU Session Update SM Context Request towards SMF with connection state of user plane configured as Activating.
9	The SMF responds to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request. This request includes the following details: • N2 SM information (QFIs, QoS profiles) • CN N3 tunnel information • S-NSSAI • ARP • Paging Policy Indicator • 5QI • N1 and N2 transfer failure notification target address • PDU session resource setup request IE
10	The AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface. The connection state of user plane is Activating.
11	The SMF initiates the N4 Modification procedure towards the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and set forward action.
12	The UPF modifies the session and sends the acknowledgment of the modification to the SMF.

Step	Description
13	The SMF responds to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with connection state of user plane as Activated.

Standards Compliance

The Network-initiated Service Request feature complies with the 3GPP TS 23.502, V15.6.0 (2019-10).

Limitations

SMF does not support location update and access-type changes.

Configuring N3 Tunnel Profile

Use the N3 tunnel profile for buffering or notifying actions towards SMF when the UPF receives the downlink data and the N3 tunnel is unavailable. To configure the N3 tunnel profile, use the following sample configuration:

```
config
   profile n3-tunnel n3_profile_name
      buffer upf
      notify
      end
```

NOTES:

- **profile n3-tunnel** *n3_profile_name*: Specify the N3 tunnel profile name. *n3_profile_name* must be a string.
- **buffer** *upf*: Configure buffering for Downlink Data.
- **notify**: Enable downlink data notification from UPF.

Always-On PDU Session Support

Feature Description

The always-on Protocol Data Unit (PDU) session means that the user plane is always active. Applications such as the IP Multimedia Subsystem (IMS) requires an always-on PDU session.

The UE requests the establishment of a PDU session as an always-on PDU session based on the request indication of the upper layers. It is the network that decides whether to establish a PDU session as an always-on PDU session.

How it Works

Call Flows

This section describes the call flows for Always-On PDU Session support.

PDU Session Establishment Call Flow

This section describes the PDU session establishment procedure involving a request for Always-on PDU session initiation in the Create Session Request.

The following figure illustrates the PDU Session Establishment call flow.

Figure 275: PDU Session Establishment Call Flow

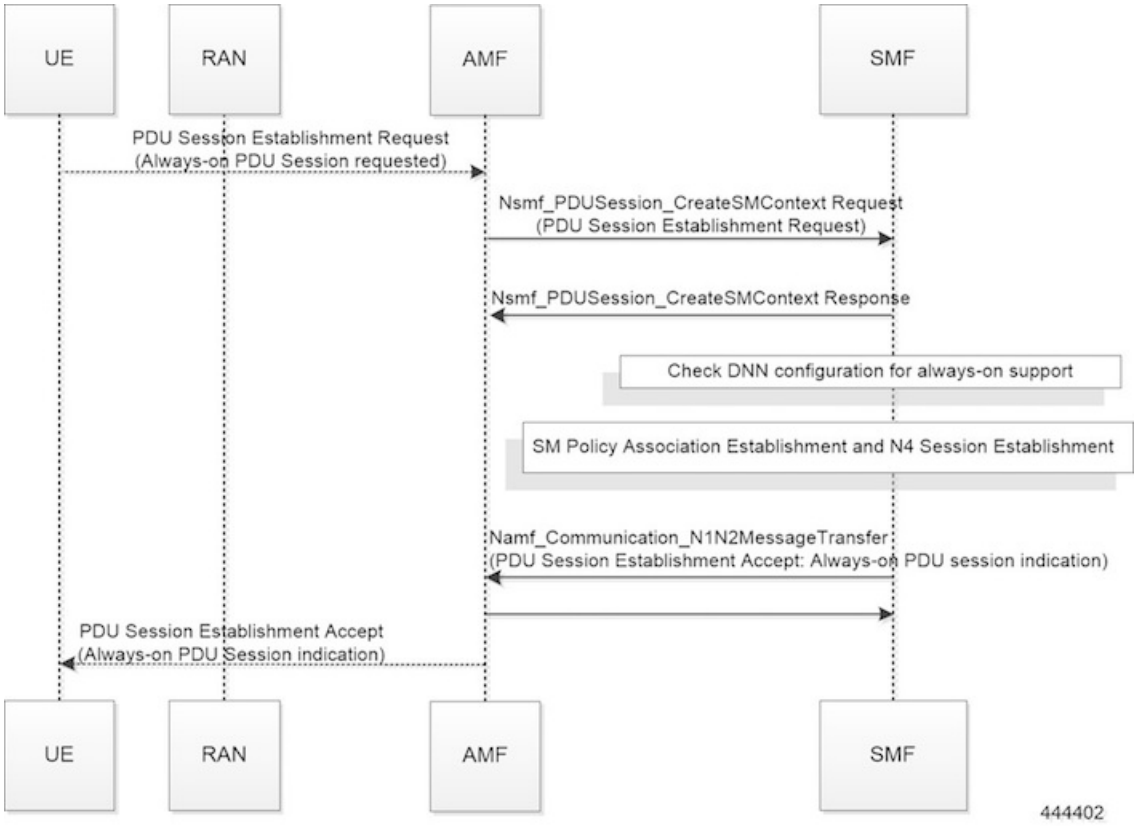


Table 480: PDU Session Establishment Call Flow Description

Step	Description
1	If the UE requests to establish an always-on PDU session, the UE includes an "Always-on PDU Session Requested" IE in the PDU Session Establishment Request message.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.
3	The SMF includes an "Always-on PDU Session Indication" IE in the PDU Session Establishment Accept message if one of the following is true: • "Always-on PDU Session Indication" is sent with value as "enabled" if the always-on configuration is enabled under the DNN profile. • "Always-on PDU Session Indication" is sent with value as "disabled" when the "Always-on PDU Session Request" IE is received and configuration is disabled.

Step	Description
4	The SMF does not include an "Always-on PDU Session Indication" only when both these conditions are true: • If the UE did not send an "Always-on PDU Session Requested" IE. • If the always-on configuration is disabled in the DNN profile.

UE-requested PDU Session Modification Call Flow

This section describes the UE-requested PDU session modification procedure in which the Always-on PDU session indication is sent.

The following figure illustrates the UE-requested PDU Session Modification call flow.

Figure 276: UE-requested PDU Session Modification Call Flow

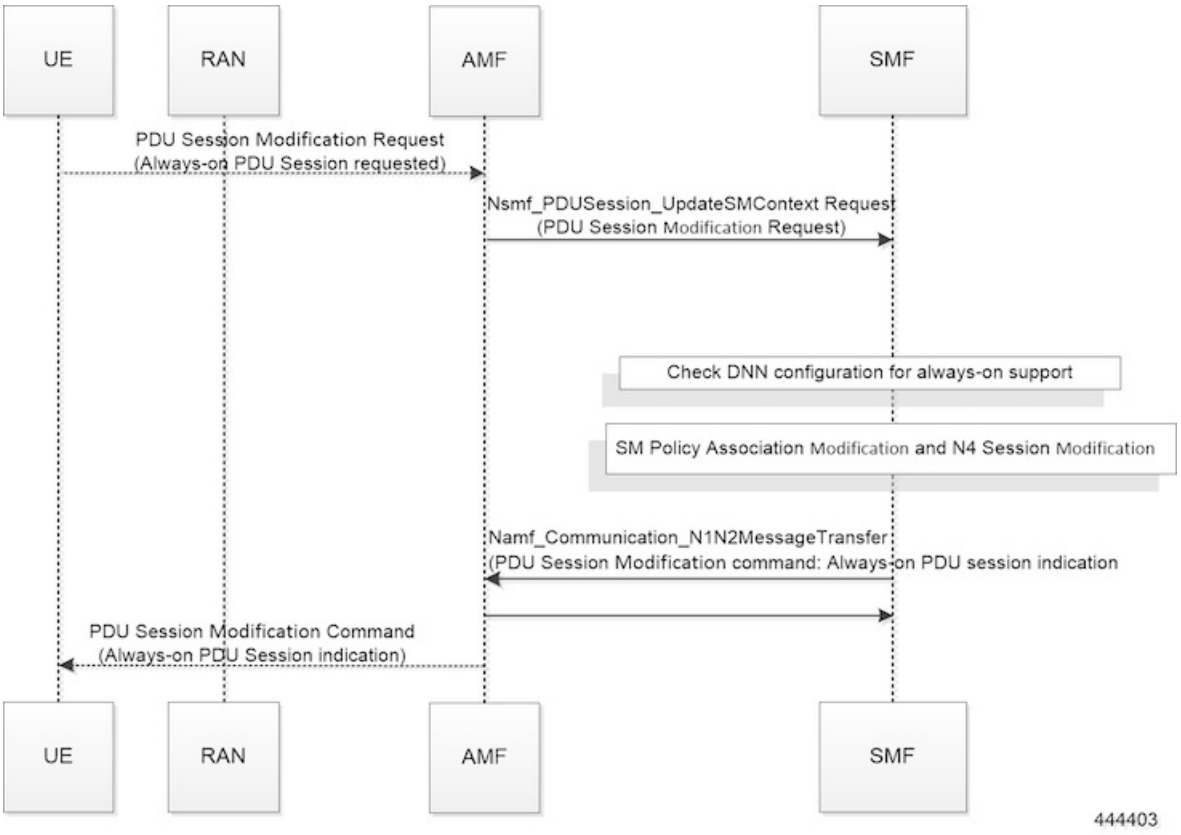


Table 481: UE-requested PDU Session Modification Call Flow Description

Step	Description
1	The UE sends an "Always-on PDU Session Requested" IE in the PDU Session Modification Request message.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.

Step	Description
3	The SMF includes "Always-on PDU Session Indication" in the PDU Session Modification Command when one of the following is true: • "Always-on PDU Session Indication" is sent with the value as "enabled" when the always-on configuration is enabled under the DNN profile. • "Always-on PDU Session Indication" is sent with the value as "disabled" when the "Always-on PDU Session Request" IE is received and configuration is disabled.
4	The SMF does not include the "Always-on PDU Session Indication" only when both these conditions are true: • If the UE did not send the "Always-on PDU Session Requested" IE. • If the always-on configuration is disabled in the DNN profile. **Note** As per *3GPP TS 23502*, for a PDU session that was established in the EPS, when the UE moves from EPS to 5GS for the first time, the UE includes an "Always-on PDU Session Requested" indication in the PDU Session Modification Request message if it wants to change the PDU session to an "always-on" PDU session.

Network-requested PDU Session Modification Call Flow

This section describes the network-requested PDU session modification procedure in which the Always-on PDU session indication is sent.

The following figure illustrates the network-requested PDU Session Modification call flow.

Figure 277: Network-requested PDU Session Modification Call Flow

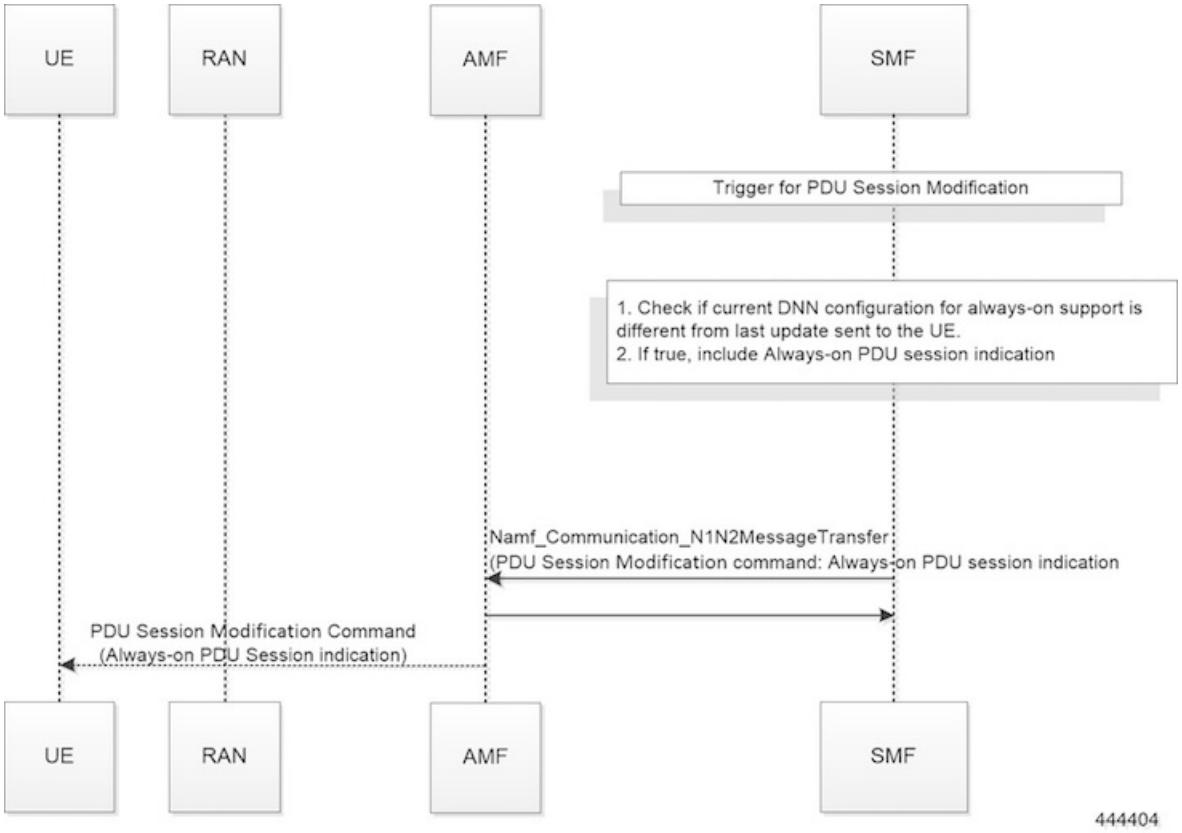


Table 482: Network-requested PDU Session Modification Call Flow Description

Step	Description
1	The SMF decides to trigger a PDU Session Modification due to PCF, UDM, or RAN initiated procedures.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.
3	The SMF determines whether the current DNN configuration for always-on is different from the last indication sent to UE. If it differs, the SMF includes the "Always-on PDU Session Indication" IE in the PDU Session Modification Command message.

Configuring Always-On PDU Session Support

To configure the parameter for always-on PDU session support, use the following sample configuration:

```
config
  profile dnn dnnprofile_name
    always-on { false | true }
    end
```

NOTES:

- **always-on { false | true }**: Configure the always-on PDU session support.
  - **false**: Disable always-on PDU session support.
  - **true**: Enable always-on PDU session support.
- The value of "Always-on PDU Session Indication" IE sent in the PDU Session Establishment Accept message is based on the always-on configuration in DNN profile. That is, if the always-on configuration is enabled under the DNN profile, then the "Always-on PDU Session Indication" IE is sent with value as "enabled".

Verifying Always-On PDU Session Support

To verify the always-on PDU session support., use the **show subscriber supi** *supi_id* **nf-service smf** CLI command.

The show output for always-on PDU session support displays one of the following options:

- “alwaysOn”: “UE Requested”
- “alwaysOn”: “Enabled”
- “alwaysOn”: “UE Requested & Enabled”

The following is a sample output of the command:

```
show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-123456789012345",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
   "accessType": "ACCESS_5G",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "123",
      "mnc": "456"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "209.165.201.4",
    "nrLocation": {
      "ncgi": {
        "mcc": "123",
        "mnc": "456",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "123",
        "mnc": "456",
        "tac": "1820"
      }
    }
    “alwaysOn”:  “UE Requested”
  },
  "accessSubData": {
    "amfID": "AFbe08",
    "amfPlmnId": {
```

```
      "mcc": "123",
      "mnc": "456"
    },
    "ueCmStatus": "UeCMConnected",
    "amfNrfID": "76517361-338e-4d77-bc76-713a79779574"
  },
  "policySubData": {
    "TotalDynamicRules": 1,
    "TotalFlowCount": 1,
    "TotalNonGBRFlows": 1,
    "pccRuleList": [
      {
        "pccRuleId": "defaultrule",
        "qfi": 1,
        "mbrDl": 125000000,
        "mbrUl": 100000000,
        "flowInformation": [
          {
            "flowDirection": 3,
            "flowDescription": "permit out ip from any to any"
          }
        ]
      }
    ],
    "qosFlow": [
      {
        "qfi": 1,
        "GBRFlow": "False",
        "bindingParameters": {
          "x5Qi": 5,
          "arp": {
            "preemptCap": 1,
            "preemptVuln": 1,
            "priorityLevel": 15
          },
          "priorityLevel": 1
        },
        "AggregatedULMFbr": 100000000,
        "AggregatedDLMFbr": 125000000,
        "pccRuleList": "defaultrule"
      }
    ]
  },
  "chargingData": {},
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 21790984727,
    "UPState": "Activated",
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel"
        }
      ]
    }
  }
}
```


Always-On PDU Session OAM Support

This section describes operations, administration, and maintenance information for this feature.

Bulk Statistics Support

The Always-On PDU Session feature supports the following bulk statistics.

Table 483: Always-On PDU Session Bulk Statistics

Bulk Statistics	Description
always-on-pdu	Tracks the number of always-on PDU sessions.
Always-on-pdu-requested	Requests the always-on PDU session.
always-on-pdu-accepted	Accepts the always-on PDU session request.
Always-on-pdu-rejected	Rejects the always-on PDU session request.
pdusetup_req_alwayson_requested	The number of Session Establishment Request messages received with "Always-On PDU Session Requested".
pdusetup_acc_alwayson_allowed	The number of Session Establishment Accept messages sent with "Always-On PDU Session Indication" enabled.
pdusetup_acc_alwayson_not_allowed	The number of Session Establishment Accept messages sent with "Always-On PDU Session Indication" disabled.
pdumod_req_alwayson_requested	The number of Session Modification Request messages received with "Always-On PDU Session Requested".
pdumod_cmd_alwayson_allowed	The number of Session Modification Command messages sent with "Always-On PDU Session Indication" enabled.
pdumod_cmd_alwayson_not_allowed	The number of Session Modification Command messages sent with "Always-On PDU Session Indication" disabled.
pdumod_cmd_nw_init_alwayson_allowed	The number of network-initiated Session Modification Command messages sent with "Always-On PDU Session Indication" enabled.
smf_session_counters	The gauge to show the number of active always-on PDU sessions.

DLDR Handling for N3 Connection Reactivation

Feature Description

When the SMF doesn't trigger the N1N2 setup request on the N11 interface when UPF received the Downlink Data Request (DLDR), the difference in the upContext state between SMF and UPF resulted in UPF triggering the DLDR. With the N3 in an inactive state, UPF used to send the session report request to SMF. With this feature, the SMF reactivates N3 when DLDR is received in N3 activated state.

How it Works

The **reactivate-n3-on-dupl-activation-dldr** CLI command is added in the supported features at SMF to reactivate the N3 when DLDR is received in the N3 activated state. After this CLI is enabled and if the DLDR is received in the ACTIVATED state, then SMF changes the upState to DEACTIVATED and reactivates the N3 connection.

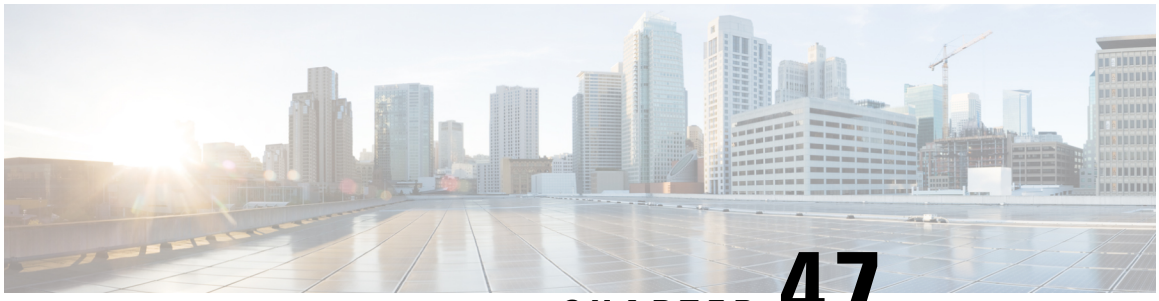
Configuring N3 Connection Reactivation

To configure N3 connection reactivation, use the following sample configuration.

```
config
  profile smf profile_name instances instance-id supported-features [
reactivate-n3-on-dupl-activation-dldr ]
      [ vsmf dtssa acscr]
```

NOTES:

- **supported-features [reactivate-n3-on-dupl-activation-dldr]**: Reactivate N3 when the DLDR received is in the N3 activated state in supported-features.



CHAPTER 47

UPF Path Management and Restoration

- Feature Summary and Revision History, on page 1521
- Feature Description, on page 1522
- How it Works, on page 1522
- Configuration Support for the UPF Path Management and Restoration, on page 1523
- OAM Support, on page 1527

Feature Summary and Revision History

Summary Data

Table 484: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 485: Revision History

Revision Details	Release
Heartbeat on Sx	2023.01.0
First introduced.	2020.02.0

Feature Description

The heartbeat monitors the status of a UPF node in terms of its responsiveness. It initiates a bilateral flow of request and response between the SMF and the UPF. It has the following actions:

- The SMF periodically sends a signal in the form of a heartbeat request to the registered UPF node. This action helps in determining if the SMF is in active or not.
- If the SMF doesn't receive a response from the UPF after the exhausted retransmission attempts, then the SMF recognizes a failure instance. It purges the UPF node-mapped subscribers.

You can control the following:

- The number of heartbeat requests that SMF sends to UPF.
- The interval between consecutive requests.
- The duration until which the SMF waits for a response.

The Heartbeat feature is also applicable for SMF with Diameter interfaces.

Standards Compliance

The heartbeat transmission between SMF and UPF complies with the following standards:

- *3GPP TS 23.527*
- *3GPP TS 23.007, version 15.4.0*

How it Works

You can configure the Heartbeat capability at the interface-level, UPF profile group-level, or both. The interface-level configuration is mandatory. If the interface-level configuration is unavailable, then the Heartbeat parameters get configured with the default values. The profile-level configuration overrides the interface-level configuration.

The Heartbeat feature also extends to achieve high-availability for the Node Manager.

Interface and profile-level Heartbeat

The SMF-UPF interaction to detect the UPF path failure using the Heartbeat messages involves the following steps:

1. The SMF sends a Heartbeat request message to the discovered UPF instances or profile groups based on the configured schedule.
2. If the UPF instance or profile is alive, it sends a Heartbeat response to the SMF indicating that it's operational. In case the UPF doesn't send a Heartbeat response, then the SMF retransmits the Heartbeat request. It's based on the configured interval and the number of permitted attempts.

3. After the configured count of Heartbeat message reattempts gets exhausted and the SMF doesn't receive a response from UPF, then the SMF starts the Session release procedure for the subscribers that are associated with that UPF.

Heartbeat and High-availability in Node Manager

Each UPF instance is associated with a primary and secondary Node Manager. The secondary Node Manager acts as a standby system on which the primary manager fails over. The primary Node Manager is responsible for the IP allocation and managing the association-specific messages such as association create, update, or delete request.

Configuration Support for the UPF Path Management and Restoration

This section describes how to configure the support for monitoring the UPF status.

Configuring the support for detecting the UPF status using the Heartbeat feature involves the following steps:

- Configuring the Heartbeat Parameters for the UPF—Lists out the configuration details for the Heartbeat parameters for the UPF at the interface level. For more information, see Configuring the Heartbeat at the Interface Level, on page 1523.
- Configuring the Heartbeat Parameters for the UPF Profile—Lists out the configuration details for the Heartbeat parameters for the UPF profile at the profile level. For more information, see Configuring the Heartbeat at the UPF Group Level, on page 1524.
- Associating UPF Group to Individual UPF Network Configuration—Lists out the configuration details for associating the UPF group to an individual UPF network. For more information, see Associating UPF Group to Individual UPF Network Configuration, on page 1525.
- Configuring the Sx/N4 Path Failure Detection Policy—Lists out the configuration details for the Sx/N4 Path Failure Detection Policy parameter. For more information, see Configuring the Sx/N4 Path Failure Detection Policy, on page 1526.

Configuring the Heartbeat at the Interface Level

To configure the Heartbeat at the interface-level, use the following sample configuration:

```
config
   instance instance-id gr_instance_id
      endpoint pfcp
         interface { n4 | sxa }
            heartbeat
               interval interval
                  max-retransmissions max_retry_count
                  retransmission-timeout retry_interval_count
                  end
```

NOTES:

- **instance instance-id** *gr_instance_id*—Specify the GR instance ID.

- **endpoint pfcp**—Specifies the endpoint configuration mode.
- **interface { n4 | sxa }**—Configures the N4 or Sxa interface over which the Heartbeat messages get exchanged between the SMF and the UPF.
- **Heartbeat**—Specifies the Heartbeat configuration.
- **interval** *interval*—Specify the Heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.

Note Setting the *interval* to 0, disables the Heartbeat feature.

- **max-retransmissions** *max_retry_count*—Specify the maximum retries for the Packet Forwarding Control Protocol (PFCP) Heartbeat request. Must be in the range of 0–10. The default value is 3.
- **retransmission-timeout** *retry_interval_count*—Specify the Heartbeat retransmission timeout in seconds. Must be in the range of 1–20. The default value is 5.

Verifying the Heartbeat Configuration for the SMF

This section describes how to verify the heartbeat configuration for the SMF.

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
show running-config instance instance-id 1  endpoint pfcp
 instance instance-id 1
  endpoint pfcp
   interface n4
    heartbeat
     interval               61
     retransmission-timeout 3
     max-retransmissions    5
     exit
    exit
   exit
 exit
exit
 interface sxa
  heartbeat
   interval               300
   retransmission-timeout 15
   max-retransmissions    0
   exit
  exit
exit
```

Configuring the Heartbeat at the UPF Group Level

To configure the Heartbeat at the UPF group level, use the following sample configuration:

```
config
   profile upf-group group_name
      heartbeat
```

```
interval interval
retransmission-timeout max_retry
max-retransmissions retry_count
end
```

NOTES:

- **profile upf-group** *group_name*—Specify the UPF group for which the Heartbeat feature must be enabled.
- **interface**—Configures the N4 interface over which the Heartbeat messages get exchanged between the SMF and the UPF.
- **heartbeat** —Specifies the Heartbeat configuration.
- **interval** *interval*—Specify the Heartbeat interval in seconds. Must be in the range of 60–360. The default value is 60 seconds.

  Setting the *interval* to 0, disables the Heartbeat feature.
- **max-retransmissions** *max_retry*—Specify the maximum retries for the Packet Forwarding Control Protocol (PFCP) Heartbeat request. Must be in the range of 0–10. The default value is 3.
- **retransmission-timeout** *retry_count*—Specify the Heartbeat retransmission timeout in seconds. Must be in the range of 1–20. The default value is 5.

Verifying the Heartbeat Configuration for the UPF Group Level

This section describes how to verify the heartbeat configuration for the UPF group level.

Use the **show running-config profile upf-group** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
show running-config profile upf-group
 profile upf-group upfGroup1
  heartbeat
   interval               62
   retransmission-timeout 3
   max-retransmissions    2
   exit
  exit
 exit
```

Associating UPF Group to Individual UPF Network Configuration

This section describes how to associate a UPF group with a UPF configuration.

In this scenario, each UPF network configuration includes the UPF profile that associates every UPF instance with a UPF profile.

To associate an UPF group profile with a network configuration, use the following sample configuration:

```
config
   profile network-element upf upf_profile_name
      upf-group-profile upf_group_name
      end
```

NOTES:

- **profile network-element upf** *upf_profile_name*—Configure the UPF network configuration.
- **upf-group-profile** *upf_group_name*—Specify the UPF group name that must be associated to the specified UPF network configuration.

Verifying the Association of the UPF Group with the Individual UPF

This section describes how to verify the association of the UPF group with the individual UPF.

Use the **show running-config profile network-element upf** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.238
 n4-peer-port      8805
 upf-group-profile upfGroup1
 dnn-list          [ intershat intershat1 intershat2 ]
 capacity          65535
 priority          65535
```

Configuring the Sx/N4 Path Failure Detection Policy

To configure the Sx/N4 Path Failure Detection policy, use the following sample configurations:

Use the following sample configuration to associate the Sx/N4 path failure detection policy:

```
config
   instance instance-id gr_instance_id
      endpoint pfcp
         sx-path-failure sx-detection-policy detection_policy_name
         end
```

Use the following sample configuration to set parameters for the Sx/N4 path failure detection policy:

```
config
   policy sx-path-failure-detection detection_policy_name
      ignore { heartbeat-retry-failure |
heartbeat-recovery-timestamp-change }
         end
```

NOTES:

- **instance instance-id** *gr_instance_id*—Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **endpoint pfcp** *endpoint_name*—Specify the endpoint name and the endpoint configuration mode for the selected interface.
- **sx-path-failure sx-detection-policy** *detection_policy_name*—Specify the name of the policy used, when the Sx path failure occurs as a result of the Heartbeat request timeout, and the default Sx action performs the cleanup activities.
- **policy sx-path-failure-detection** *detection_policy_name*—Specify the name of the policy used, when the Sx path failure occurs as a result of the Heartbeat request timeout detection.

- **ignore { heartbeat-retry-failure | heartbeat-recovery-timestamp-change }**—Detect the path failure mode, when there's an attempt to retry the Heartbeat messages time out, or whenever there’s a change in the recovery timestamp of the heartbeat request or a response message.

Verifying the Sx/N4 Path Failure Detection Policy

This section describes how to verify the Sx/N4 path failure detection policy.

Verifying the Association of the Sx/N4 Path Failure Detection Policy:

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** command to view and verify the association of the feature configuration.

The following is a sample output of the show command.

```
show running-config instance instance-id 1 endpoint pfcp
 instance    instance-id 1
  endpoint    pfcp
   replicas    1
   enable-cpu-optimization    true
   sx-path-failure sx-detection-policy sx1
   interface    n4
   heartbeat
    interval    0
    retransmission-timeout    3
    max-retransmissions    5
    exit
   vip-ip    209.165.201.24
   exit
  interface    gtpu
  vip-ip    209.165.201.24
  exit
 exit
exit
```

Verifying Parameters Settings for the Sx/N4 Path Failure Detection Policy:

To view and verify the configuration parameters settings for the Sx/N4 path failure detection policy, use the following commands:

Use the **show running-config policy sx-path-failure-detection** *detection_policy_name* command to view and verify the configuration parameters settings for the feature.

The following is a sample output of the show command.

```
show running-config policy sx-path-failure-detection
 policy sx-path-failure-detection sx1
 ignore heartbeat-retry-failure
 exit
exit
```

OAM Support

This section describes the operations, administration, and maintenance information for this feature.

Bulk Statistics

The following statistics are supported for the heartbeat-related UPF path management feature.

- **nodemgr_upf_heartbeat_fail_stats**
- **nodemgr_upf_hb_msg_stats**

The SMF maintains these bulk statistics triggered during the heartbeat request and response procedure.

nodemgr_upf_heartbeat_fail_stats

- Description:

  The counter that gets updated per UPF when it fails to respond to a heartbeat request.

- The `nodemgr_upf_heartbeat_fail_stats` counter supports the following labels:

  Labels:

  - Label: **upf_heartbeat_req_tx**

    Label Description: Label for the heartbeat request that the SMF sends.

  - Label: **upf_heartbeat_req_retx**

    Label Description: Label for the retransmitted heartbeat request

  - Label: **upf_heartbeat_rsp_rx**

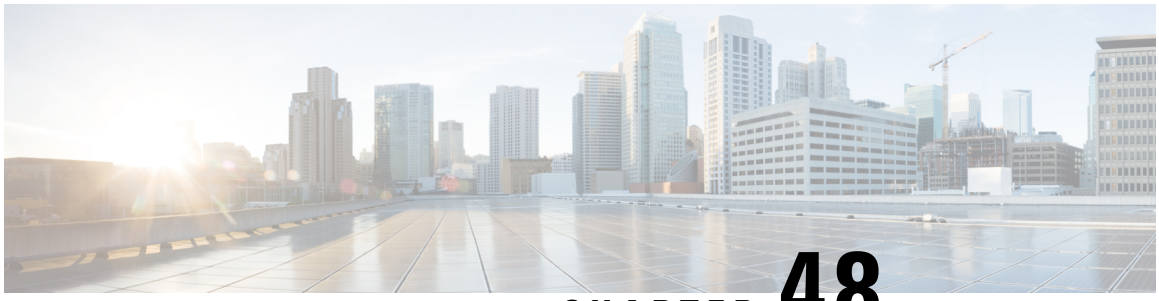
    Label Description: Label for the heartbeat response that the SMF receives.

nodemgr_upf_hb_msg_stats

- Description:

  The counter for all heartbeat messages for the specified UPF

For more information on bulk statistics support for SMF, see the *UCC 5G SMF Metrics Reference* document.



CHAPTER 48

Virtual Routing and Forwarding

- Feature Summary and Revision History, on page 1529
- Feature Description, on page 1530
- How it Works, on page 1530
- Configuring Virtual Routing and Forwarding, on page 1532
- OAM Support, on page 1536

Feature Summary and Revision History

Summary Data

Table 486: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 487: Revision History

Revision Details	Release
Added VRF support for Diameter interfaces.	2023.04.0
The following enhancements are introduced: • Extended the maximum number of VRFs to 129 • Static and Dynamic Policy Removal	2023.01.0

Revision Details	Release
Support overlapping AAA server addresses for PAPN use case	2022.04.0
First introduced.	2020.02.5

Feature Description

Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist within the same router at the same time. As the routing instances are independent, you can use the same or overlapping IP addresses without conflicting with each other.

In private APN (PAPN) deployments, the same SMF can support multiple PAPNs, requiring authentication and accounting with the enterprise AAA servers. As the AAA servers belong to different mobile virtual network operators (MVNOs), it's possible that their address ranges overlap. The SMF uses VRF to allow the overlapping AAA server addresses in PAPN or MVNO.

Important Currently SMF doesn't support the overlapping addresses for the AAA client.

SMF uses VRF to also remove the Dynamic and Static routes based on UDP interfaces that are optimized by using the default route of VRF. This action replaces the policies with one default route per interface to improve the operational performance.

SMF enables configuration of VRF in the IP pool. The SMF sends IP address details along with the configured VRF name to UPF. UPF maps the IP address to VRF configured within UPF.

SMF supports up to 129 VRFs with a scale of 2K TPS for private APNs and DNNs.

SMF supports the client-side VRF for the Diameter Gx and Gy interfaces. The profile Diameter endpoint refers to the VRF name and interface name that you configure from the Diameter endpoint. The Diameter endpoint uses the VRF name to create a TCP connection from the Diameter client.

Note This implementation is backward compatible if you haven't configured a VRF. In such a case, the creation of a TCP socket towards the Diameter server is applicable with no VRF name configuration.

How it Works

This section describes how the SMF uses the VRF technology for the following use cases:

- PAPN
- Static and dynamic policy removal

VRF Creation

To create the VRF, perform the following steps:

1. Create VRF with gateway through CLI configuration.

   VRF gets created with a default route in the VRF routing table.

2. For the PAPN use case, each PAPN is associated with its own VRF having the default route. Each PAPN VRF must be defined on SMF and leaf switch.

3. For the Static and Dynamic policy removal use case, VRF with default route is created on SMF to handle outbound routes through the default route added by VRF.

   SMF continues to use global VRF for L3 VIP advertisement toward leaf switch. Hence, on leaf, no specific VRF is required for this use case.

VRF Modification

To modify the device or gateway on the existing VRF, use the following steps:

1. Disassociate the VRF to be modified from endpoint and router.
2. Delete the VRF and apply the configuration changes.

Important Make sure you delete the VRF in running system only.

3. Create VRF with modified device or gateway.
4. Associate newly created VRF with modified device or gateway with the endpoint and router. Apply the configuration changes.

VRF Deletion

To delete the device or gateway on the existing VRF, use the following steps:

1. Disassociate the VRF to be deleted from the endpoint and router.
2. Delete the VRF and apply the configuration changes.

Important Make sure you delete the VRF in running system only.

3. If the VRF is shared across logical SMFs, delete the VRF from all logical SMFs to completely remove the VRF configuration from the interface. This is applicable only for static and dynamic use case.

Limitations

This feature has the following limitations:

- NAS-IP for authentication and accounting requests must be the same as the interface CoA-NAS VIP-IP in the RADIUS endpoint CoA-NAS interface configuration.
- The VRFs configured under RADIUS server-group and RADIUS endpoint must be the same.

- For the Disconnect Message (DM) request, the client VRF and the server VRF (CoA-NAS VIP VRF) must match. If there is a mismatch, the DM request is discarded.

Configuring Virtual Routing and Forwarding

VRF Configuration

The VRF configuration is applicable for both PAPN, and Static and Dynamic use cases.

To configure the VRFs in global configuration mode, use the following sample configuration:

```
config
   vrf name vrf_name gateway gateway_ipv4_address gatewayIpv6 gateway_ipv6_address
device interface_name linkDevice linked_device_name
   end
```

Important VRF creation and deletion operations are supported. To modify the existing VRF, VRF must be deleted and then added again.

NOTES:

- **vrf name** *vrf_name* —Specify the VRF name. The maximum VRF length supported is 15.
- **gateway** *gateway_ipv4_address*—Specify the IPv4 address of the gateway.
- **gatewayIpv6** *gateway_ipv6_address*—Specify the IPv6 address of the gateway.
- **device** *interface_name*—Specify the name of the public bonded interface.
- **linkDevice** *linkedDevice_name*—Specify the name of the private bonded interface. This field is applicable only for Static and Dynamic use case.

Configuration Example

The following are example configurations of VRFs with gateway:

```
vrf name papn_vrf_1 gateway 209.165.202.131 device bd2.radius.2161
vrf name papn_vrf_2  gateway 209.165.202.131 device bd2.radius.2162
vrf name vrf_s11 gateway 209.165.202.131 device bd1.s11.1692 linkDevice bd1.s11.1696
```

Endpoint Configuration

To configure the endpoint and associate with the VRF, use the following sample configuration:

```
config
   instance instance-id instance_id
       endpoint { gtp | pfcp | radius | diameter  }
          interface { coa-nas | s5 | s5e | s2b | s11 | n4 | gx | gy  }
            vip-ip ip_address [ vip-interface  interface_name| vip-port vip_port
```

```
 | vrf vrf_name ]
             end
```

NOTES:

- **endpoint { gtp | pfcp | radius | diameter }**—Specify the endpoint name. It can be GTP, PFCP protocol, RADIUS, or Diameter.

  For PAPN support, use the RADIUS endpoint. For the static and dynamic policy removal use case, select the GTP or PFCP protocol.

- **interface { coa-nas | s5 | s5e | s2b | s11 | n4 | gx | gy }**—Specify the interface based on the use case. For PAPN support, select **coa-nas** interface. For the policy removal use case, use any of the other available interfaces. For Diameter endpoint, select **gx** or **gy** interface.

- **vip-ip** *ip_address*—Specify the IPv4 address of the configured endpoint.

- **vip-interface** *interface_name*—Specify the interface name. Note that this is a bonded interface which is associated with VRF.

- **vip-port** *vip_port*—Specify the port number of endpoint.

- **vrf** *vrf_name*—Specify the VRF name defined using global VRF configuration.

Configuration Example

The following are example configurations:

```
instance instance-id 1 endpoint radius interface coa-nas vip-ip 209.165.202.131 vip-port
8112 vip-interface bd2.radius.2161 vrf papn_vrf_1

instance instance-id 1 endpoint radius interface coa-nas vip-ip 209.165.202.133 vip-port
8112 vip-interface bd2.radius.2162 vrf papn_vrf_2

instance instance-id 1 endpoint pfcp interface n4 vip-ip 209.165.202.134 vip-interface
bd2.n4.2105 vrf vrf_n4_ls1

instance instance-id 1 endpoint gtp interface s11 vip-ip 209.165.202.135 vip-interface
bd1.s11.1692 vrf vrf_s11

instance instance-id 1 endpoint diameter interface gx vip-ip 209.165.202.136 vip-interface
 d2.aaa.1212 vrf vrf_signaling
```

VRF Configuration in RADIUS Profile

To configure the VRF in RADIUS server group, use the following sample configuration:

```
config
   profile radius
      server-group group_name
         vrf vrf_name
         server-private { radius_server_ip_address port_number  | [ range ] }
            priority radius_server_priority
            secret radius_server_secret_key
            type { acct | auth }
            end
```

NOTES:

- **server-private {** *radius_server_ip_address port_number* **| [range] }** —Specify the IP address and port number of the private RADIUS servers used for accounting and authentication requests. This server is private to the specific server-group.

  Private servers in the server-group will be given priority over global servers that are associated to the group. If private servers are unreachable or dead, global servers will be selected to send authentication or accounting requests.

- **priority** *radius_server_priority*—Specify the priority of RADIUS server.

- **secret** *radius_server_secret_key*—Specify the RADIUS server shared secret key.

  Must be a string.

- **type { acct | auth }**—Specify the type of private RADIUS server used for accounting and authentication requests.

- **server-private {** *radius_server_ip_address port_number* **[priority** *radius_server_priority* **| secret** *radius_server_secret* **| type { acct | auth }] | [range] }**

- **range**—Specify the IP address range.

- **vrf** *vrf_name*—Specify the VRF name to be configured in AAA server group.

  If VRF is configured in server-group, it is recommended to configure servers using server-private and not associate the global servers.

To define the VRF in RADIUS Dynamic-authorization/COA configuration, use the following sample configuration:

```
config
   profile radius-dynamic-author
      client client_ip_address vrf vrf_name
         nas-identifier nas_identifier_port
         secret secret_key
         end
```

NOTES:

- **client** *client_ip_address*—Specify the RADIUS Dynamic-authorization client configuration.

- **vrf** *vrf_name*—Specify the VRF name to be configured in AAA server group.

  If VRF is configured in server-group, it is recommended to configure servers using server-private and not associate the global servers.

- **nas-identifier** *nas_identifier_port*—Specify the dynamic authorization NAS identifier.

- **secret** *secret_key*—Specify the dynamic authorization server shared secret key.

VRF Association for BGP Peering

To associate VRF with BGP for BGP peering, use the following sample configuration:

```
config
   router bgp bgp_name
       interface interface_name
```

```
vrf  vrf_name
end
```

NOTES:

- **interface** *interface_name*—Specify the local BGP interface.
- **vrf** *`vrf_name*—Specify the VRF details to be associated with BGP.

Configuration Example

The following is an example of BGP peering configuration with no VRF association:

```
interface enp94s0f0.3921
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3922
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

The following is an example of BGP Peering configuration with association with papn_vrf_1.

```
interface enp94s0f0.3923  leaf1
  vrf papn_vrf_1
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3924  leaf2
  vrf papn_vrf_1
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

The following is an example of BGP Peering configuration with association with papn_vrf_2.

```
interface enp94s0f0.3925
  vrf papn_vrf_2
  bondingInterface enp216s0f0
  bondingInterface enp94s0f0
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
interface enp94s0f1.3926
  vrf papn_vrf_2
  bondingInterface enp216s0f1
  bondingInterface enp94s0f1
  neighbor 209.165.202.254 remote-as 65141 fail-over bfd
exit
```

Configuration Verification

To view the VRF information, use the **show vrf-info all** command.

Following is a sample output of the **show vrf-info all** command.

```
                          GATEWAY                          TABLE
NAME        GATEWAY         IPV6    DEVICE      LINK DEVICE   ID     STATE  POD NAME
-------------------------------------------------------------------------------------
```

```
npapn-vrf12 209.165.200.225      bd2.npv12.756               2516    true  bgpspeaker-pod-1
papn-vrf18  209.165.200.226      bd2.pv18.1236               2621    true  bgpspeaker-pod-1
vrf_s11     209.165.200.227     bd1.s11.1692  bd1.s11.1696   2631    true  bgpspeaker-pod-1
vrf_n4_ls1  209.165.200.228      bd2.n4.2105   bd2.n4.3915    2630    true  bgpspeaker-pod-1
```

To view the VRF route information, use the **show vrf-route-info all** command.

Following is a sample output of the **show vrf-route-info all** command.

```
Vrf TableId Route
papn-vrf11 2614 default via 209.165.200.225 dev bd2.pv11.1229 proto 217 metric 217
papn-vrf11 2614 broadcast 209.165.200.226 dev bd2.pv11.1229 proto kernel scope link src
209.165.200.225
papn-vrf11 2614 209.165.200.227/29 dev bd2.pv11.1229 proto kernel scope link src
209.165.200.225
papn-vrf11 2614 local 209.165.200.225 dev bd2.pv11.1229 proto kernel scope host src
209.165.200.225
papn-vrf11 2614 broadcast 209.165.200.227 dev bd2.pv11.1229 proto kernel scope link src
209.165.200.225
papn-vrf11 2614 anycast fe80:: dev bd2.pv11.1229 proto kernel
papn-vrf11 2614 local fe80::42a6:b7ff:fe37:38 dev bd2.pv11.1229 proto kernel
papn-vrf11 2614 fe80::/64 dev bd2.pv11.1229 proto kernel metric 256
papn-vrf11 2614 ff00::/8 dev bd2.pv11.1229 proto 3 metric 256

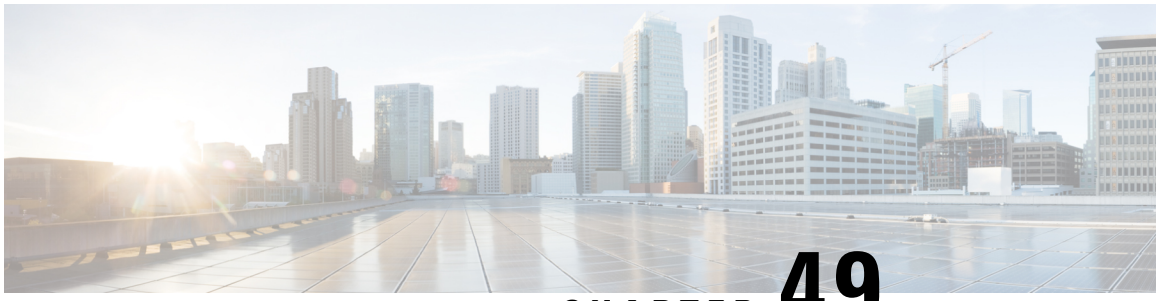
Vrf TableId Route
vrf_s5 2633 default via 209.165.200.225 dev bd1.s5.1691 proto 217 metric 217
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src 209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src 209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 209.165.200.226/24 dev bd1.s5.1691 proto kernel scope link src 209.165.200.225
vrf_s5 2633 local 209.165.200.225 dev bd1.s5.1691 proto kernel scope host src 209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 209.165.200.226/24 dev bd1.s5.1691 proto kernel scope link src 209.165.200.225
vrf_s5 2633 local 209.165.200.226 dev bd1.s5.1691 proto kernel scope host src 209.165.200.225
vrf_s5 2633 broadcast 209.165.200.226 dev bd1.s5.1691 proto kernel scope link src
209.165.200.225
vrf_s5 2633 anycast fe80:: dev bd1.s5.1691 proto kernel
vrf_s5 2633 anycast fe80:: dev bd1.s5.1691 proto kernel
vrf_s5 2633 local fe80::42a6:b7ff:fe37:39 dev bd1.s5.1691 proto kernel
vrf_s5 2633 local fe80::42a6:b7ff:fe37:39 dev bd1.s5.1691 proto kernel
vrf_s5 2633 fe80::/64 dev bd1.s5.1691 proto kernel metric 256
vrf_s5 2633 fe80::/64 dev bd1.s5.1691 proto kernel metric 256
vrf_s5 2633 ff00::/8 dev bd1.s5.1691 proto 3 metric 256
vrf_s5 2633 ff00::/8 dev bd1.s5.1691 proto 3 metric 256
```

OAM Support

Bulk Statistics Support

The following statistics are updated to support the VRF feature.

- bgp_outgoing_routerequest_total - This statistics includes "vrf" label to indicate the total count of successful BGP outgoing routes per VRF.
- bgp_outgoing_failedrouterequest_total - This statistics includes "vrf" label to indicate the total count of failed BGP outgoing routes per VRF.
- bgp_speaker_bfd_peer_status - This statistics includes "vrf" label to indicate the BFD peer status.



CHAPTER 49

Wireless Priority Services

Table 488: Feature History

Feature Name	Release Information	Description
SBI Message Priority Enhancement	2023.04	The SBI Message Priority (SMP) mechanism uses the "3gpp-Sbi-Message-Priority" custom HTTP header to set and carry the message priority between the client and the server. The custom HTTP header enforces the message priority end to end between the client and the server through one or more proxies. **Note** Stream Priority mechanism is not supported.

- Feature Summary and Revision History, on page 1539
- Feature Description, on page 1540
- How it Works, on page 1548
- 5QI Mapping Support, on page 1549
- Configuring Wireless Priority Services, on page 1550
- WPS OAM Support, on page 1559

Feature Summary and Revision History

Summary Data

Table 489: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI

Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 490: Revision History

Revision Details	Release
Enhancements to SBI Message Priority Mechanism and Message-Prioritization based on Procedures	2023.04.0
5QI Mapping support introduced	2023.03.0
UPF Interaction while Deleting WPS Dynamic Rule	2021.01.0
SBI Message Priority Mechanism and Message-Prioritization based on Procedures are introduced.	2021.01.0
The Wireless Priority Services feature is fully qualified in this release.	2020.03.0
First introduced. This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.0

Feature Description

The Wireless Priority Services (WPS) feature is supported on the SMF over 5GC. The SMF validates prioritization of WPS services for session creation or modification and various handover scenarios. The SMF also evaluates the WPS services for Paging-Policy Differentiation for Network Triggered Service Request procedures.

SMF also detects priority calls based on ARP through local configurations to classify sessions as WPS and allows users to use nonstandard QCIs in addition to ARP for WPS calls.

QoS properties corresponding to these nonstandard QCI values are configured locally on the gNB. SMF only supports values added on the SMF to map nonstandard QCI to DSCP values on the data path.

Important With release 2021.02.0, SMF will not set an MP flag in the N4 message while deleting the dynamic rule if no other existing rules ARP isn't matching wps-profile.

Use Cases

The WPS feature implements the 3GPP recommendations for wireless priority support for the following use cases in 5GS and EPS. The use cases are defined as per 3GPP TS 23.501 (sections 5.16.3, 5.16.4, 5.16.5, 5.16.6, 5.19, and 5.21).

WPS supports the following use cases:

- Multimedia Priority Services , on page 1541
- DSCP Marking for N3, S5-U, or S2-B over PFCP, on page 1546

Multimedia Priority Services

The Multimedia Priority Service (MPS) allows priority access to system resources to Service Users, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis. MPS includes signalling priority and media priority.

MPS provides the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions.

All MPS-subscribed UEs get priority for QoS Flows (for example, used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by configuring MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers and not On Demand MPS subscribers, based on regional or national regulatory requirements. On Demand service is based on Service User invocation or revocation explicitly and applied to the media QoS Flows being established. Not On Demand MPS service does not require invocation and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

Priority treatment for MPS includes priority message handling for Mobility Management procedures. Priority treatment for MPS session requires appropriate ARP and 5QI setting for QoS Flows according to the operator's policy.

MPS priority mechanisms can be classified as subscription-related mechanism and invocation-related mechanism. Subscription-related mechanisms can be applied as "always applied" and "conditionally applied".

Subscription-related mechanisms that are conditionally applied include:

- UDM—One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is configured to an appropriate ARP priority level.
- PCF—The "IMS Signalling Priority" information is configured for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling.

Invocation-related mechanisms can be applied for mobile-originated SIP call or sessions, for mobile-terminated SIP call or sessions, and for Priority PDU connectivity services.

On-Demand MPS Service

The invocation-related priority mechanisms for prioritized services are based on communication with an Application Server and between the Application Server and the PCF over Rx or N5 interface (as described in 3GPP TS 23.228, clause 5.21, in the case of MPS using IMS).

Invocation-related mechanisms for Mobile Originations (for example, through SIP or IMS) are explained as follows:

- PCF:
  - When an indication for a session reaches over the Rx or N5 interface and the UE does not have priority for the signaling QoS Flow, the PCF derives the ARP and 5QI parameters plus associated QoS characteristics as appropriate, as per the Service Provider policy (specified in 3GPP TS 23.503, clause 6.1.3.11).
  - For MPS sessions, when establishing or modifying a QoS Flow as part of the session origination procedure, the PCF selects the ARP and 5QI parameters, and the associated QoS characteristics, as appropriate, to provide priority to the QoS Flows.
  - When all active sessions to a particular DN are released and the UE is not configured for priority treatment to that particular PDU session, the PCF downgrades the IMS Signaling QoS Flows from appropriate settings of the ARP and 5QI parameters and the associated QoS characteristics, as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations (for example, through SIP or IMS) are explained as follows:

- PCF: When an indication for a session reaches over the Rx or N5 interface, the mechanisms as described above for Mobile Originations are applied.
- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE, the UPF sends a "Data Notification" including the information to identify the QoS Flow for the DL data packet to the SMF (specified in 3GPP TS 23.502, clause 4.2.3.3.
- SMF: If the SMF receives the "Data Notification" message for a QoS Flow associated with an ARP priority level value for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "N1N2MessageTransfer" message (specified in 3GPP TS 23.502, clause 4.2.3.3).
- AMF: If the AMF receives the "N1N2MessageTransfer" message containing an ARP priority level value for priority use, the AMF handles the request with priority. AMF also includes the "Paging Priority" IE in the N2 "Paging" message configured to a value assigned to indicate about an existing IP packet at the UPF requiring higher priority (specified in 3GPP TS 23.502, clause 4.2.3.3).
- SMF: For a UE that is not configured for a higher priority, upon receiving the "N7 Session Management Policy Modification" message from the PCF with an ARP priority level for priority use, the SMF sends an "N1N2MessageTransfer" to update the ARP for the Signaling QoS Flows (specified in 3GPP TS 23.502, clause 4.3.3.2).
- AMF: After receiving the "N1N2MessageTransfer" message from the SMF with an ARP priority level for priority use, the AMF updates the ARP for the Signaling QoS Flows (specified in 3GPP TS 23.502, clause 4.3.3.2).
- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging during congestion at the (R)AN (specified in 3GPP TS 23.502, clause 4.2.3.3).

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF:
  - If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flows controlled by the Priority PDU connectivity services are established or modified to have the service appropriate configuration of the ARP and 5QI parameters and the associated QoS

characteristics, using the PDU Session Modification procedure (specified in of 3GPP TS 23.502, clause 4.3.3).

- If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flows controlled by the Priority PDU connectivity services are modified from service appropriate configuration of the ARP and 5QI parameters and the associated QoS characteristics, to those entitled by the UE as per subscription, using the PDU Session Modification procedure (specified in 3GPP TS 23.502 clause 4.3.3).

Message-Priority Indication over GTP-C

An overloaded node performs message prioritization when handling incoming messages during an overloaded condition. This condition is based on the relative GTP-C message priority signaled in the GTP-C header.

When message throttling is performed:

- GTP requests related to priority traffic (eMPS as described in 3GPP TS 22.153) and emergency have the highest priority. Depending on regional or national requirements and the network operator policy, these GTP requests are the last to be throttled when applying traffic reduction. The priority traffic is exempted from throttling due to GTP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, message throttling considers the relative priority of the messages so that low priority messages are considered for throttling before the other messages. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent (as specified in clause 12.3.9.3.2) or derived from the session parameters such as APN and ARP.

The high priority messages are given lower preference to throttle and low priority messages are given higher preference to throttle. An overloaded node also applies these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of the self-protection mechanism.

A sending GTP-C entity determines the relative message priority to signal in the message according to either procedure based or session parameters. If the message affects multiple bearers (for example, Modify Bearer Request), the relative message priority considers the highest priority ARP among all the bearers.

A GTP-C entity sets the same message priority in a Triggered message or Triggered Reply message as received in the corresponding Initial message or Triggered message respectively. For incoming GTP-C messages that do not have a message priority in the GTP-C header, the receiving GTP-C entity:

- Applies a default priority if the incoming message is an Initial message.
- Applies the message priority sent in the Initial message or Triggered message if the incoming message is a Triggered message or Triggered Reply message.

The nodes in the network homogenously support this feature to prevent an overloaded node to process initial messages received from the non-supporting nodes. These messages are received according to the default priority. The overloaded node processes initial messages that are received from the supporting nodes according to the message priority signaled in the GTP-C message.

Message-Prioritization based on Session Parameters

Message prioritization is also performed based on the session parameters, such as APN and ARP. The procedures and messages associated with the higher priority sessions are given lesser priority while throttling than the procedures and messages associated with the lower priority sessions. Within each group of sessions,

the messages are further prioritized based on the category of the procedure for which the message is being sent.

Message Prioritization Based on Procedures

Message prioritization is performed based on the relative priority of the procedure for which the message is being sent. Procedures are grouped into various categories and each of these categories are assigned a priority. In addition, within a given category of procedures, messages can be further prioritized based on session parameters, such as APN, QCI, ARP or LAPI.

Messages with a high priority are given lower preference to throttle and messages with low priority are given higher preference to throttle. The grouping of the procedures isn't performed based on an individual GTP-C entity but while considering all the procedures in general. A GTP-C entity considers the procedures applicable to it and prioritizes message throttling based on the category of the procedure. The categories are listed in decreasing order of priority with category 1 having the highest priority. For each category, a nonexhaustive list of messages is provided. Any existing or newly defined message in future is considered based on the category of the procedure for which the message is sent. Following are the categories of a procedure:

1. UE session mobility within and across 3GPP or non-3GPP access—Procedures involving active or idle mode UE mobility, such that GTP-C signalling involved are classified under this category. Some examples are X2 or S1 based handover with or without an SGW change, TAU or RAU with a change of MMEor SGSN with or without an SGW change, and 3GPP access to trusted non-3GPP access handover. Throttling of these messages during the procedures related to UE session mobility results in the failure of the corresponding procedures. This failure can cause PDN disconnection or the interruption of the services. As a result, the following messages, when sent during the procedures belonging to this category, must be considered with the highest priority. Hence, these messages are given the lowest preference to throttle.
   - Create Session Request.
   - Create Session Request with "handover" indication bit set.
   - Modify Bearer Request.
   - Modify Bearer Request with "handover" indication bit set.
   - Modify Access Bearer Request.
2. Release of PDN connection or bearer resources—Procedures resulting in the deactivation of an existing PDN connection, the deactivation of bearers or of data forwarding tunnel of an UE leads to freeing up of the resources at the overloaded node. These procedures ease the overload situation as the freed up resources can be used for serving the remaining of the UEs. Hence, the following messages that belong to this category and cause the deactivation of PDN connection or bearers or data forwarding tunnels, must be treated with the next lower level of priority. Hence, these messages are given the corresponding preference whilst throttling:
   - Delete Session Request.
   - Delete Bearer Request.
   - Delete Bearer Command.
   - Delete Indirect Data Forwarding Tunnel Request.
3. Miscellaneous session management procedures—This category consists of the session management procedures, except the PDN connection creation and bearer creation or modification procedures. Some examples are location reporting, when it isn't combined with other mobility procedures and Service request

and S1 release procedure. These procedures do not impact the ongoing service of the UE. Hence, the following messages when sent during the procedures identified under this category, must be treated with the next lower level of priority. Hence, these messages are given the corresponding preference whilst throttling.

- Release Access Bearer Request.
- Modify Bearer Request.
- Change Notification.
- Suspend Notification.
- Resume Notification.

4. Request for new PDN Connection or bearer resources or modification of existing bearer resources—This category consists of the procedures requesting the creation of PDN connection, creation or modification of bearers, or creation of data forwarding tunnel. Throttling of the messages belonging to this category cause denial of new services while continuing with the existing services. In this overload condition, an overloaded node, due to lack of resources, isn't able to provide new services while trying to maintain the existing services. When the following messages are sent during the procedures belonging to this category are considered with the lowest level of priority. Hence, these messages are given highest preference to throttle:
   - Create Session Request during PDN connection request.
   - Create Bearer Request.
   - Update Bearer Request.
   - Bearer Resource Command.
   - Modify Bearer Command.
   - Create Indirect Data Forwarding Tunnel Request.
   - Downgrade the DSCP marking of the data packets for the session when quota exhausts.

Message-Priority Header for PFCP

When the message throttling is performed:

- PFCP requests related to priority traffic (that is, eMPS as described in 3GPP TS 22.153) and emergency have the highest priority. Depending on regional or national requirements and network operator policy, these PFCP requests are the last to be throttled when applying traffic reduction. Throttling exempts the priority traffic due to PFCP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, the message throttling considers the relative priority of the messages so that the messages with low priority are first considered for the throttling. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent or derived from the session parameters such as APN and ARP.

A PFCP entity determines whether to configure and use the message priority in PFCP signalling, based on operator policy. A sending PFCP entity determines the relative message priority to signal in the message which are derived from the session parameters, such as APN and ARP. If the message affects multiple bearers,

the relative message priority is determined considering the highest priority ARP among all the bearers. A PFCP entity must configure the same message priority in a Response message as received in the corresponding Request message.

For incoming PFCP messages that do not have a message priority in the PFCP header, the receiving PFCP entity:

- Applies a default priority if the incoming message is a Request message.
- Applies the message priority sent in the Request message if the incoming message is a Response message.

The SMF and UPF functions in the network homogenously support this feature to prevent an overloaded node to process the Request messages received from the non-supporting nodes according to the default priority. With this support, an overloaded node does not need to process the Request messages received from supporting nodes according to the message priority signalled in the PFCP message.

DSCP Marking for N3, S5-U, or S2-B over PFCP

Transport Level Marking

Transport level marking is the process of marking traffic with a DSCP value based on the locally configured mapping from the QCI and optionally the ARP priority level. For EPC, the S-GW and PGW-C perform transport level marking on a per EPS bearer basis. For 5GC, the S-GW and PGW-C perform transport level marking on a per QoS flow basis.

The UPF performs transport level marking with a DSCP value based on the mapping from the 5QI, the Priority Level (if explicitly signaled), and optionally the ARP priority level configured at the SMF. The CP function controls transport level marking by providing the DSCP in the ToS or Traffic Class within the Transport Level Marking IE in the FAR (associated to the PDR matching the traffic to be marked).

The UP function performs transport level marking for the detected traffic and sends the marked packet to the peer entity. The CP function changes transport level marking by changing the Transport Level Marking IE in the related FAR.

WPS Profile Support

The SMF+PGW-C supports the WPS profile defined with ARP and DSCP marking value to be configured for GTP-C and PFCP Protocol IP-headers. Use the WPS profile to configure the message priority in the GTP-C and PFCP protocols.

The SMF+PGW-C allows a maximum of 64 WPS profiles and each WPS profile is associated in the DNN profile. For more information, see the Configuring Wireless Priority Services, on page 1550 section.

SBI Message Priority Mechanism

The primary usage of SBI Message Priority (SMP) is to provide guidance to 5GC NF acting as HTTP/2 clients or servers while making throttling decisions related to overload control. You can use the priority information for routing in the proxies. Eventually a server uses the priority information to process higher-priority requests before lower-priority requests. The SMP mechanism uses the "3gpp-Sbi-Message-Priority" custom HTTP header to set and carry the message priority between the client and the server. The custom HTTP header enforces the message priority end to end between the client and the server through one or more proxies.

Note Stream Priority mechanism is not supported.

The header contains the HTTP/2 message priority value: The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

```
3gpp-Sbi-Message-Priority = "3gpp-Sbi-Message-Priority" ":" (DIGIT / %x31-32 DIGIT / "3"
%x30-31)
```

A message with

```
3gpp-Sbi-Message-Priority "0"
```

has the highest priority.

Example:

```
3gpp-Sbi-Message-Priority: 10
```

How it works

The SBI Message Priority Mechanism functions in the following way:

- A client, proxy, and a server uses the **3gpp-Sbi-Message-Priority** value while configuring or evaluating the priority of a message.
- The client assigns the request priority by adding the **3gpp-Sbi-Message-Priority** custom HTTP header to the message and setting its value.
- If the server assigns a different priority to the response message then the server assigns the response priority by adding the **3gpp-Sbi-Message-Priority** custom HTTP header to the message and setting its value.

For more information on the configurations, see the *Configuring Message Priority Profile* and *Association of Message Priority Profile* .

WPS Session Critical Information

Following are the important WPS session critical information:

- SMF does not identify a session as WPS during establishment and hence priority tagging based on establishment is not possible on the SMF. SMF is not aware of MCS and MPS subscription or establishment causes.
- SMF does not support any special access rights enforcement for WPS session configuration or for WPS session monitoring.
- SMF does not support any hardware isolation between WPS and non-WPS users.
- IPSEC support on N4 is not supported for WPS. IPSEC is enabled at interface/peer level.
- Upgrade the UPF before the SMF for the SBI message priority feature to work smoothly. Otherwise, configure the new priority values on the SMF only after UPF is upgraded. UPF supports Message Priority (MP) values 1 to 3 in older releases. If SMF gets upgraded first, and new configuration gets applied on the N4 interface, then UPF ignores new values and treats those sessions as normal call.
- If new priority values are configured post upgrade, then on the UPF, old sessions uses old MP values that were applied before the upgrade and new sessions uses new MP values. Due to this there can be

conflicting MP values for sessions of same type and session recovery based on the priority does not work as expected untill MP values of old sessions gets updated. MP values of old sessions gets updated during subsequent N4 modification from SMF.

- If a message priority profile is associated to any QoS profile or DNN profile or WPS profile, SMF enables this SBI message priority feature. Else, the SBI message priority feature remains disabled and SMF sends the hardcoded values as before on N4 and GTP interfaces.

Session Type Conflict Resolution at SMF

Under the following criteria there can be session type conflict resolution at SMF:

- SMF tags a session as emergency, if the DNN is tagged to emergency or if a session gets created automatically.
- SMF tags a session as IMS, when a Bearer/flow gets created with the QCI configured as IMS under the DNN profile.
- SMF tags a session as WPS based on the ARP received from PCF.

When a session satisfies multiple conditions, a session type gets tagged based on the following criteria.

```
WPS > Emergency > IMS
```

SMF does not send any session type to the UPF. UPF maps the session to priority through configuration. For more information, see the *UPF Configuration Guide*.

WPS Session VLAN Tagging

SMF does not allocate a separate VLAN for WPS during session establishment. SMF supports configuration of nexthop address per address range in an ip-pool. UPF maps nexthop to the VLAN.

How it Works

This section describes how Wireless Priority Service (WPS) feature works.

Standards Compliance

The Wireless Priority Services feature complies with the following standards:

- 3GPP TS 22.153
- 3GPP TS 23.228
- 3GPP TS 23.282
- 3GPP TS 23.379
- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 24.301

5QI Mapping Support

Feature Description

SMF currently detects priority calls (WPS) based on ARP. To use QCI in addition to ARP for WPS calls, SMF supports 5QI Remapping functionality to enable mapping of nonstandard QCI with the standard QCI, which UE can understand.

The SMF facilitates the following functions:

- **Seamless handover to 4G**: The SMF remaps the QCI sent in a mapped EPS QoS parameter with a mapped EPS bearer context to the configured value.
- **Seamless handover to 5G**: The SMF remaps the QCI sent in QoS Flow description in the protocol configuration option in the Create Session Response, Create Bearer Request, and Update Bearer Request.

QCI Modification for Dynamic Rules

In certain scenarios, existing sessions can be upgraded from non-WPS to WPS or downgraded from WPS to non-WPS. In such cases, the PCF sends an N7 notification to the SMF along with a new QCI/ARP (QoS Class Identifier/Allocation and Retention Priority).

If the new QCI is configured to be NAS-remapped, the SMF includes the remapped QCI in the parameter list of QoS Flow Descriptions within the N1 modification command message sent to the UE (User Equipment) if it is connected to a 5G RAT (Radio Access Technology).

For UEs connected to 4G or Wi-Fi RATs, the remapped QCI is sent within the QoS Flow Description as part of the protocol configuration option in the Update Bearer request.

During Wi-Fi Handover, if the PCF sends a nonstandard QCI for which the SMF has a remapping configuration, the remapped QCI specified in the configuration is sent to the UE in the N1 PDU (Protocol Data Unit) establishment response, the Create Session response, or the Create Bearer Request.

SMF remaps configuration and any run time configuration change is applied only during the following procedures:

- New default bearer session creation
- New QoS flow or bearer creation request from PCF
- QCI upgrade or downgrade from PCF
- Wi-Fi handover

For more information, see the Remapping Nonstandard QCI to Standard QCI, on page 1552.

Collision Between Original QCI and Remapped QCI

If there is a collision between existing bearer with new bearer with the same QCI or mapped QCI, SMF rejects some QoS flow configurations based on the following conditions:

- If the PCF sends a QCI, which gets remapped to an existing QCI associated with a flow or bearer, the SMF rejects the creation of the bearer or any QCI upgrade or downgrade request.
- If the PCF sends a QCI for the creation of a new bearer/flow, and there is already an existing flow/bearer with the same remapped QCI, the SMF rejects the PCF's request for creating the new bearer.
- Given that the SMF is configured to remap QCI=x to QCI=y and QCI=z to QCI=y, if the PCF sends a rule with QCI=x, resulting in the creation of a flow/bearer, any subsequent request from the PCF with QCI=z is rejected by the SMF.

Example: The following remapping configuration is not allowed/accepted by the system:

- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 131
  ```
- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 132
      qosflow qi5 132 nas-remap 131
  ```
- ```
  profile qos qosp-ims
      qosflow qi5 131 nas-remap 132
      qosflow qi5 132 nas-remap 133
  ```

For more information, see the Remapping Nonstandard QCI to Standard QCI.

Configuring Wireless Priority Services

This section describes how to configure the Wireless Priority Services feature.

Configuring the WPS Profile

Use the following sample configuration to configure the WPS profile.

```
config
  profile wps wps_profilename
     arp arp_value
    dscp [ n3 n3_value | message-priority { [ { gtpc | pfcp } [ arp | dscp
 ] ] }
     end
```

NOTES:

- **profile wps** *wps_profilename*: Accesses the Wireless Priority Services Profile configuration. *wps_profilename* must be an alphanumeric string of 1 to 63 characters.
- **arp** *arp_value*: Specifies the range of ARP levels. *arp_value* must be an integer from 1 to 15 separated either by "," or "-".

Important If you are upgrading SMF from Release 2023.03.0 to a later release, make sure you manually reconfigure the ARP parameter in the WPS profile after the upgrade is complete.
```

- **dscp [n3** *n3_value* **]** : Specifies the DSCP marking value for the N3 interface. The N3 value indicates the UP DSCP marking value within the range 0 to 0x3F.
- **message-priority { gtpc pfcp }**: Specifies the message priority for GTP-C and PFCP.

Verifying the WPS Profile Configuration

This section describes how to verify the WPS Profile configuration.

Run the **show running-config** command to view the configuration.

The following is an example of the **show running-config** command output.

```
show running-config profile wps wps1
   profile wps wps1
   arp 1,4-6,9
   dscp n3 10
   message-priority [ pfcp gtpc ]
   exit
```

Associating WPS Profile under DNN Profile

Use the following sample configuration to associate the WPS profile with the configured DNN profile.

```
config
   profile dnn profile_dnn_name
      wps-profile wps_profile_name
      end
```

NOTES:

- **wps-profile** *wps_profile_name*: Enables the Wireless Priority Services Profile configuration. This profile is configured under the existing DNN profile configuration.

Verifying WPS Profile under DNN Profile

This section describes how to verify the WPS profile configuration under the DNN profile.

Execute the **show running-config** command to view the configuration.

The following is an example of the **show running-config** command output.

```
show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
wps-profile wps1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
exit
```

Configuration Verification

To view the WPS parameters per subscriber session, use the **show subscriber** command.

The following is an example output of the **show subscriber** command.

```
show subscriber supi imsi-123456789012345 nf-service smf
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-123456789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "intershat",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        },
        "sScMode": 1,
        "uetimeZone": "UTC+12:00",
        "allocatedIp": "209.165.200.233",
        "nrLocation": {
          "ncgi": {
            "mcc": "123",
            "mnc": "456",
            "nrCellId": "123456789"
          },
          "tai": {
            "mcc": "123",
            "mnc": "456",
            "tac": "1820"
          }
        },
        "alwaysOn": "None",
        "dcnr": "None",
        "wps": "Wps Session",
        "ratType": "NR",
        "ueType": "NR Capable UE",
        "sessTimeStamp": "2021-05-28 12:46:11.165805357 +0000 UTC",
        "callDuration": "2.925145554s",
        "ipPool": "poolv4",
        "commonId": 11,
        "snssai": {
          "sd": "Abf123",
          "sst": 2
        },
        .
        .
        .
```

Remapping Nonstandard QCI to Standard QCI

Use the following sample configuration to enable and remap the QCI sent in the QoS Flow parameter list to the needed configuration value. This remapping process is applicable for N1 PDU Establishment Accept and PDU Session Modification procedures.

```
config
   profile qos qos_profile_name
      dscp-map qi5 qos_id
      qosflow qi5 nonstandard_value nas-remap standard_value
      arp-priority-level arp_value uplink user-datagram dscp-marking
dscp_marking_value
      arp-priority-level arp_value downlink { encsp-header { copy-inner |
dscp-marking dscp_marking_value } | user-datagram dscp-marking dscp_marking_value
 } }
      commit
```

NOTES:

- **dscp-map qi5** *qos_id*: Specify the ID for the authorized QoS parameters. *qos_id* must be an integer in the range of 1–255.
- **qosflow qi5** *nonstandard_value* **nas-remap** *standard_value*: SMF remaps the 5QI that is sent in the parameter list in the QoS Flow descriptions to the configured value. **nas-remap** *standard_value* accepts the mapped 5QI value in the range 1–255. For example, **qosflow qi5** *131* **nas-remap***1*.
- **arp-priority-level** *arp_value* **uplink user-datagram dscp-marking** *dscp_marking_value*: Configure the ARP priority level and then set the DSCP value in the inner IP header in the uplink direction. This DSCP value is applied to the packets with the configured 5QI value.

  arp_value must be an integer in the range of 1–255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.
- **arp-priority-level** *arp_value* **downlink { encsp-header { copy-inner | dscp-marking** *dscp_marking_value* **} | user-datagram dscp-marking** *dscp_marking_value* **} }**: Configure the ARP priority level and then set the DSCP value to be applied to the encapsulation header or user datagram.

  If **encsp-header** is configured, set the DSCP in the outer-ip header in the downlink direction or copy the DSCP value from the inner IP header to the outer IP header.

  If **user-datagram** is configured, set the DSCP in the inner IP header in the downlink direction.

  arp_value must be an integer in the range of 1–255.

  dscp_marking_value must be a hexadecimal number from 0x00 through 0x3F.

The following is an example configuration.

```
[smf] smf(config)# profile qos qos_A5972
[smf] smf(config-qos-qos_A5972)# qosflow qi5 1
Possible completions:
  arp-priority-level
  downlink
  gfbr
  mfbr
  nas-remap
  uplink
[smf] smf(config-qos-qos_A5972)# qosflow qi5 1 nas-remap 2
```

Configuring Message Priority Profiles

Use the following sample configuration to configure a message-priority for all interfaces.

```
config
     profile message-priority msg_priority_profile_name
     interface [ any | pfcp | gtp | sbi [ { create | update | delete } ]
 ]
       priority value range
     exit
```

NOTES:

- **interface [any | pfcp | gtp | sbi [{ create | update | delete }]]**:
  - **interface [any | pfcp | gtp | sbi]** : Specify priority value per interface. For example, for the SBI interface, configure as per procedure. If a procedure is not configured, same value is applied for all procedures. Interface type is optional and if not configured, the same value is applied across all interfaces.
  - **priority** *value*: Specifies the range of priority levels 0–31 for sbi or 0–15 for pfcp, gtp, or any, where 0 indicates the highest priority, while 31 or 15 indicates the lowest priority.

Note Priority is not populated in outbound messages, which are selftriggered. For example, outbound messages triggered by timer expiry.

Verifying Message Priority Profile

The following is the example output of the **Show running-config for profile message-priority** command.

```
Show running-config for profile-> message-priority :

profile message-priority test

  interface pfcp,any priority value 15

 interface gtp priority value 10

 interface sbi priority value 20

 interface sbi procedure create priority value 0

 interface sbi procedure update priority value 10

 interface sbi procedure delete priority value 20

exit
```

Associating Message Priority Profiles

Associate Message Priority for WPS

You can associate WPS profile with ARP and message priority profile using the following configuration.

```
config
  profile wps wps_profile_name
     arp  arp_value [ qci ] message-priority-profile profile_name
  exit
```

NOTES

- **profile wps** *wps_profile_name*: Accesses the Wireless Priority Services Profile configuration. *dynamic_wps* must be an alphanumeric string of 1 to 63 characters.
- **arp** *arp_value* **message-priority-profile** *profile-name*: Specify an ARP value in the range from 1 to 15.
- **qci message-priority-profile** *profile_name*: Wireless Priority session is decided based on the ARP and optionally on the QCI.
- **message-priority-profile** *profile_name* : This parameter is used only if the message priority profile is not associated. For example, **message-priority-profile** *[pfcp gtpc]*.

Verifying Message Priority Profiles under WPS

To view WPS parameters based on message priority profiles, use the **show full-configuration profile wps** command.

The following is an example output of the **show full-configuration profile wps** command.

```
[smf] smf(config)# show full-configuration profile wps

profile wps test

  arp 1,8

  arp 5-7 message-priority-profile test

exit
```

Associate Message Priority Profile with QoS

You can associate message priority profile to a QoS profile and to the QCI or ARP in the QoS profile. The following configuration works for emergency calls coming with dedicated DNN, for example, “sos”.

```
config
  profile qos  qos-profile-name
      message-priority-profile profile_name
      qosflow qi5  nonstandard_value arp-priority-level arp_value
message-priority-profile profile_name
 exit
```

NOTES:

- **message-priority-profile** *profile_name* : Associates message priority profile to qos profile.
- **qosflow qi5** *nonstandard_value* : Message priority profile associated to QCI and the one associated to QoS profile.
- **arp-priority-level** *arp_value* : Message priority profile associated to ARP. Specify the ARP value in the range between 1 to 255.

  The Message priority profile associated to QCI or ARP or QoS profile, or message priority profile associated to WPS are negotiated to find the one which has the better priority.

Note If there is no message priority profile associated to a default bearer/flow, QCI or ARP, then message priority value is considered from message priority profile that is associated to a QoS profile for the IMS and emergency calls. When a dedicated bearer/flow gets created, message priority is considered from message priority profile associated to QCI or ARP depending on the configuration.

Verifying Profile QoS Configuration

To view QoS flow based on message priority profiles, use the **show full-configuration profile qos** command.

The following is an example output of the **show full-configuration profile qos** command.

```
[smf] smf(config)# show full-configuration profile qos test

profile qos test

  message-priority-profile test

  qosflow qi5 5 arp-priority-level 5 message-priority-profile mpp1

exit
```

Associate Message Priority Profile for Emergency

If there is a PDU session establishment with some other DNN, say “IMS” and if a session type is set to emergency, use the following sample configuration to specify a specific priority to an emergency call.

```
config
  profile dnn dnn_profile_name
    emergency-message-priority-profile profile_name
  exit
```

NOTES:

- **emergency-message-priority-profile** *profile_name* : Enables message priority negotiation with emergency message priority profile.

Note Message Priority (MP) value of IMS-Inactive is derived from IMS-Active where,

$MP_{IMS\text{-}Active}$ = MP selected for IMS dedicated bearer/flow.

$MP_{IMS\text{-}Inactive} = MP_{IMS\text{-}Active} + 1$

Verifying Message Priority Under DNN

The following is an example output of the **Show running-config for profile dnn** command.

```
Show running-config for profile-> dnn :

profile dnn intershat

 emergency-message-priority-profile test

exit
```

Configuring SMF to Exclude WPS Sessions from Overload Throttling

Use the sample configuration to exclude WPS sessions from overload throttling for the GTP interface.

Note Overload exclusion is based only on the ARP/5QI/DNN/MP and not based on DSCP.

```
config
  profile overload ovld_ctrl_prfl
    overload-exclude-profile self-protection ovld_exclude_wps
    node level
      tolerance minimum minimum_value
      tolerance maximum maximum_value
      reduction-metric minimum minimum_value
      reduction-metric maximum maximum_value
    advertise
      interval value
      change-factor value
      validity-period value
     exit
    interface interface_name
      overloaded-action [ advertise ]
     exit
   exit
  exit
profile overload-exclude ovld_exclude_wps
   dnn-list dnn_list
   arp-list arp_list
   qi5-list qi5_list
   message-priority priority_value
exit
```

NOTES:

- **overload-exclude-profile self-protection** *ovld_exclude_wps*: Excludes WPS sessions from overload throttling.
- **profile overload-exclude** *ovld_exclude_wps* **message-priority** *priority_value*: Allows GTP overload exclude support.

Configuring Overload Exclusion at an Endpoint Level

Use the following configuration to configure overload exclusion at an endpoint level for the SBI interface.

```
config
   instance instance-id instance_id
     endpoint sbi
        overload-control threshold threshold_limit threshold_range action
action_status action_code range exclude message-priority value
```

```
    commit
  end
```

NOTES:

- **overload-control**: Specify the overload control at endpoint level.
- **threshold** : Specify the threshold limit and range.
- *threshold_limit*: Specify the threshold limit. *threshold_limit* must be one of the following:
  - *low*: Specify the low threshold limit for overload protection.
  - *high*: Specify the high threshold limit for overload protection.
  - *critical*: Specify the critical threshold limit for overload protection.
- *thershold_range*: Specify the threshold range. *threshold_range* must be an integer in the range of 10 – 100000.
- **action** : Specify the action to be taken for the threshold limit.
- *action_status*: Specify the action for the threshold limit. *action_status* must be:
  - **reject**: Reject the inbound messages if the specified threshold range is met.
- *action_code*: Specify the action status code. *action_code* must be:
  - **reject-code**: Specify the reject status code.
- *range*: Specify the range of the action code. *range* must be an integer in the range of 100 – 600.
- **exclude message-priority** *value*: Specify the SBI MP overload exclude value.

The following is an example configuration:

```
profile overload ovld_ctrl_prfl
 overload-exclude-profile self-protection ovld_exclude_wps
 node-level
  tolerance minimum 80
  tolerance maximum 95
  reduction-metric minimum 10
  reduction-metric maximum 100
  advertise
   interval        60
   change-factor   5
   validity-period 600
  exit
  interface gtpc
   overloaded-action [ advertise ]
  exit
 exit
exit

profile overload-exclude ovld_exclude_wps
 dnn-list [ sos ]
 arp-list [ 2 3 4 ]
 qi5-list [ 1 2]
 message-priority s5 upto <unsignedInt, 0 .. 15>
exit
```

```
config
  instance instance-id 1
    endpoint sbi
      overload-control threshold high 10000 action reject reject-code 200 exclude
message-priority <value>
    exit
  exit
exit
```

WPS OAM Support

SMF Session Gauge Counters

The "wps" label is introduced at the SMF service for session-level gauage counters that support WPS and non-WPS functionality.

For example:

```
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="non_wps"}
 10
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="wps"}
 20
```

N4 Interface Metrics

The N4 interface counters related to message priority include:

- SESSION_DELETION_REQUEST
- SESSION_ESTABLISHMENT_REQUEST
- SESSION_MODIFICATION_REQUEST

An example of the N4 interface metrics:

```
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_DELETION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 4
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_ESTABLISHMENT_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 6
proto_pfcp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_MODIFICATION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 20
```

GTPv2 Metrics

The GTPv2 counters related to message priority include:

- NumCreateBearerSuccess
- NumRxCreateBearerRes
- NumTxCreateSessionReq

An example of the GTPv2 metrics:

```
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumCreateBearerSuccess",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumRxCreateBearerRes",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumTxCreateSessionReq",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
 2
```

KPIs

Following KPIs are supported for this feature:

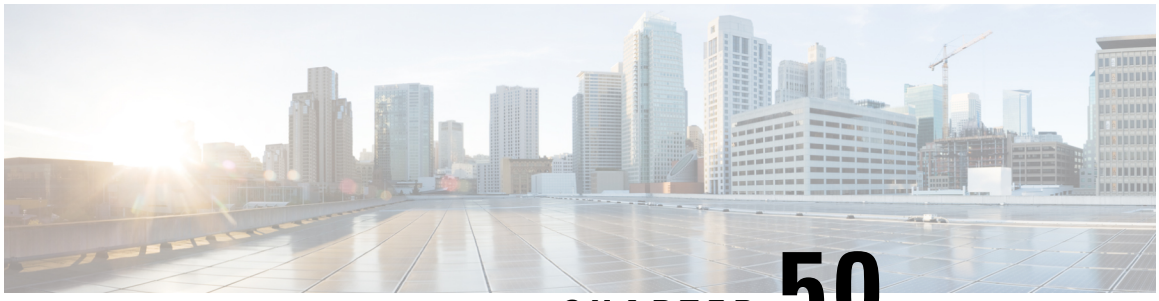
```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="attempted"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="success"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="failure"})
```

Table 491: Statistics for Tracking the Number of Times QCI or ARP is Modified

KPI Name	Type	Description or Formula	Label
policy_dynamic_pcc_rules_total	counter	Total number of dynamic pcc rules added, modified, or deleted as part of different procedures.	pccrule_change_type,status



CHAPTER 50

Troubleshooting Information

- Feature Summary and Revision History, on page 1561
- Description, on page 1563
- Using CLI Data, on page 1563
- Alerts, on page 1594
- Metrics, on page 1617
- Logs, on page 1621
- Dispatcher, on page 1627

Feature Summary and Revision History

Summary Data

Table 492: Summary Data

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 493: Revision History

Revision Details	Release
Added the wait time display for ongoing bulk clear subscriber CLI and blocking the consecutive CLI.	2023.04.0

Revision Details	Release
Added the following support: • Enabling UPF Monitor Subscriber from SMF. • Session Count per slice and NSSAI.	2023.03.0
As part of the IP pool allocation per slice and DNN feature, added example configuration to configure NSSAI labels of smf_service_stats metrics.	2022.04.0
Introduced support for classification and configuration of application metrics	2021.02.3
Added support for the following enhancements: • The **show subscriber nf-service smf** *smf_url* command to show subscriber details based on the IP address value of the vSMF or hSMF. • The **clear subscriber nf-service smf** *smf_url* command to clear subscriber details based on the IP address value of the vSMF or hSMF. • The **clear subscriber nf-service smf** *smf_url* command to clear subscriber details based on the IP address value of the vSMF or hSMF. • The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **full** command to show detailed subscriber information for roaming-specific use case as hSMF and vSMF. • The **show subscriber supi** *supi_id* **nf-service smf psid** *psid_value* **summary** command to show detailed information about subscriber sessions for roaming-specific use case as hSMF and vSMF.	2021.02.2
Added support for the following enhancements: • The **show subscriber supi** *supi_value* **nf-service smf psid** *psid_value* **summary** command to provide detailed information about subscriber sessions. • The **clear subscriber nf-service smf** and **show subscriber nf-service smf** commands with supported keywords and filters. • The **clear subscriber** and **clear subscriber nf-service smf** commands to support the **reactivation** keyword to clear sessions when release cause as reactivation-required is configured. This enhancement also supports disconnect and release reasons. • The **imei** keyword for **monitor subscriber**, **clear subscriber**, and **show subscriber** CLI commands.	2021.02.0
First introduced.	Pre-2020.02.0

Description

This chapter provides information on using the command line interface (CLI) commands, alerts, metrics, monitor tools, and logs for troubleshooting any issues that may arise during system operation.

Using CLI Data

This section describes the show and clear commands and the monitor commands that are used for troubleshooting.

Show and Clear Commands

show Commands

This section lists some of the key show commands that are available for troubleshooting the issues. The output of these show commands provides specific configuration and status information.

show config-error

Use this command to display the configuration error-related information for all pods in the cluster. The following sample output is for the **show config-error** command:

```
[smf] smf# show config-error
ERROR
COMPONENT       ERROR DESCRIPTION
--------------------------------------------------------------------------------
RuleBase        Default bandwidth policy does not exist in rulebase <rba1> for charging
action <ca1> .Dropping ruleDef <rda1>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda60>
RuleBase        Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda61>
ChargingAction  Packet filter <pkt1234> configured for charging action <ca4> associated
with rulebase <rb1> does not exist
BandWidthPolicy Uplink peak data rate less than commited data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

*Table 494: Output Field Descriptions for the **show config-error** Command*

Field	Description
Error Component	Specifies the error component.
Error Description	Specifies the description of the Error.

show diagnostics

Use this command to display the diagnostics information. The following sample output is for the **show diagnostics** command:

```
[smf] smf# show diagnostics
POD INSTANCE       DIAGNOSTIC           COMPONENT  START TIME               STATUS   RETRIES
-------------------------------------------------------------------------------------------
bgpspeaker-pod-1   Topology             AppInfra   2022/03/08 20:36:24.674  Success  0
bgpspeaker-pod-1   System Topology      AppInfra   2022/03/08 20:36:24.676  Success  0
sgw-service-0      Topology             AppInfra   2022/03/08 20:36:17.152  Success  0
sgw-service-0      System Topology      AppInfra   2022/03/08 20:36:17.154  Success  0
sgw-service-0      Cache Pod            AppInfra   2022/03/08 20:36:27.223  Success  0
sgw-service-0      SESSION_DB Datastore AppInfra   2022/03/08 20:36:17.155  Success  0
li-ep-0            Topology             AppInfra   2022/03/08 20:36:20.743  Success  0
li-ep-0            System Topology      AppInfra   2022/03/08 20:36:20.741  Success  0
smf-service-1      Topology             AppInfra   2022/03/08 20:36:19.216  Success  0
smf-service-1      System Topology      AppInfra   2022/03/08 20:36:19.218  Success  0
smf-service-1      Cache Pod            AppInfra   2022/03/08 20:36:26.276  Success  0
smf-service-1      SESSION_DB Datastore AppInfra   2022/03/08 20:36:19.220  Success  0
dns-proxy-0        Topology             AppInfra   2022/03/08 20:36:21.885  Success  0
dns-proxy-0        System Topology      AppInfra   2022/03/08 20:36:21.887  Success  0
protocol2-1        System Topology      AppInfra   2022/03/08 20:36:24.858  Success  0
protocol2-1        Cache Pod            AppInfra   2022/03/08 20:36:25.937  Success  0
protocol2-1        Topology             AppInfra   2022/03/08 20:36:24.856  Success  0
nodemgr-0          System Topology      AppInfra   2022/03/08 20:36:14.831  Success  0
nodemgr-0          Cache Pod            AppInfra   2022/03/08 20:36:26.485  Success  0
nodemgr-0          SESSION_DB Datastore AppInfra   2022/03/08 20:36:14.833  Success  0
nodemgr-0          Topology             AppInfra   2022/03/08 20:36:14.835  Success  0
nodemgr-1          Topology             AppInfra   2022/03/08 20:36:23.068  Success  0
nodemgr-1          System Topology      AppInfra   2022/03/08 20:36:23.071  Success  0
nodemgr-1          Cache Pod            AppInfra   2022/03/08 20:36:26.690  Success  0
nodemgr-1          SESSION_DB Datastore AppInfra   2022/03/08 20:36:23.066  Success  0
```

*Table 495: Output Field Descriptions for the **show diagnostics** Command*

Field	Description
Component	Specifies the component name.
Diagnostics	Specifies the diagnostics details.
Pod Instance	Specifies the instance information of the pod.
Retries	Specifies the retry count.
Start Time	Specifies the start time of the application.
Status	Specifies if the diagnostics status is successful or not.

show endpoint all

Use this command to display the list of all internal and external endpoints running on all pods in the cluster. The following sample output is for the **show endpoint all** command:

```
[smf] smf# show endpoint all

                        START    STOPPED
GR INSTANCE               ENDPOINT            ADDRESS  TYPE     STATUS
   INTERFACE  INTERNAL  TIME     TIME
```

```
cache-pod                  xx.xx.xx.xx:0000     Grpc     Started  cache-pod
   true       4 weeks   <none>   0
cache-pod                  xx.xx.xx.xx:0000     Grpc     Started  cache-pod
   true       4 weeks   <none>   0
internal-admin-ep          xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
   true       4 weeks   4 weeks  0
internal-admin-ep          xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
   true       4 weeks   <none>   0
internal-admin-ep          xx.xx.xx.xx:0000     Rest     Started  internal-admin-ep
   true       4 weeks   <none>   0
:
:
keep-alived-ep             xx.xx.xx.xx:0000     Tcp      Started  keep-alived-ep
   true       2 weeks   <none>   0
keep-alived-ep             xx.xx.xx.xx:0000     Tcp      Started  keep-alived-ep
   true       2 weeks   <none>   0
oam-grpc-ep                xx.xx.xx.xx:0000     Grpc     Started  oam-grpc-ep
   true       4 weeks   <none>   0
oam-rest-ep                xx.xx.xx.xx:0000     Rest     Started  oam-rest-ep
   true       4 weeks   <none>   0
```

*Table 496: Output Field Descriptions for the **show endpoint all** Command*

Field	Description
Address	Specifies the host and port of the endpoint.
Endpoint	Specifies the name of the endpoint.
GR Instance	Specifies the GR instance.
Interface	Specifies the interface name of the endpoint.
Internal	Specifies the type of the endpoint (Internal or External).
Start Time	Specifies the start time of the endpoint.
Status	Specifies current status of the endpoint.
Stopped Time	Specifies the end time of the endpoint.
Type	Specifies the type of the endpoint.

show endpoint info

Use this command to display the list of endpoints running on all pods in the cluster. The following sample output is for the **show endpoint info** command:

```
[smf] smf# show endpoint info
                                                                                                    START
 STOPPED  GR
ENDPOINT                  ADDRESS              TYPE  STATUS   INTERFACE  INTERNAL  TIME
 TIME     INSTANCE
-------------------------------------------------------------------------------------------------------
sbi                     xxx.xxx.xxx.xxx:0000  Rest  Started  rest       false     2 weeks
 <none>   0
sbi                     xxx.xxx.xxx.xxx:0000  Rest  Started  rest       false     2 weeks
 <none>   0
```

*Table 497: Output Field Descriptions for the **show endpoint all** Command*

Field	Description
Address	Specifies the host and port of the endpoint.
Endpoint	Specifies the name of the endpoint.
GR Instance	Specifies the GR instance.
Interface	Specifies the interface name of the endpoint.
Internal	Specifies the type of the endpoint (Internal or External).
Start Time	Specifies the start time of the endpoint.
Status	Specifies current status of the endpoint.
Stopped Time	Specifies the end time of the endpoint.
Type	Specifies the type of the endpoint.

show geo-maintenance-mode

Use this command to display whether the maintenance mode is enabled or disabled. The following sample output is for the **show geo-maintenance-mode** command:

```
[smf] smf# show geo-maintenance-mode
result "geo-maintenance-mode is disabled"
```

```
[smf] smf# show geo-maintenance-mode
result "geo-maintenance-mode is enabled"
```

show georeplication checksum instance-id

Use this command to display replication details for etcd and cache-pod data. The following sample output is for the **show georeplication checksum instance-id** command:

```
[smf] smf# show georeplication checksum instance-id
Value for 'instance-id' (<string>): 1
checksum-details
--      ----  --------
ID      Type  Checksum
--      ----  --------
1       ETCD  1646812528
IPAM    CACHE 1646812528
NRFMgmt CACHE 1646812528
```

show georeplication-status

Use this command to display the replication status between two racks in a Geo setup.

The following sample output displays, if the connection is successful:

```
[smf] smf# show georeplication-status
result "pass"
```

The following sample output displays, if there is an error:

```
[smf] smf# show georeplication-status
result "fail: [424] checksum missmatch"
```

show helm

The **show helm** command displays the version information for the SMF system image.

show ipam pool

Field	Description
PoolName	Name of the Address Pool.
Ipv4Utilization	Utilization percentage for IPv4 address for this pool.
Ipv6AddrUtilization	Utilization percentage for IPv6 address for this pool.
Ipv6PrefixUtilization	Utilization percentage for IPv6 prefix address for this pool.

show ipam pool <pool-name>

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this pool) / Number of used address / Utilization percentage for IPv4 address.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 address.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 prefix

show ipam pool <pool-name> ipv4-addr

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

show ipam pool <pool-name> ipv6-addr

Field	Description
StartAddress	Start address of the range.

Field	Description
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

show ipam pool <pool-name> ipv6-prefix

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane this address range is allocated.
Flag	Flag Indicates whether pool is Static or if it is offline, S(Static) and O(Offline).

show ipam dp

Field	Description
DpName	Name of the data plane which is registered.
Ipv4Utilization	Utilization percentage for IPv4 by this data plane.
Ipv6AddrUtilization	Utilization percentage for Ipv6 address by this data plane.
Ipv6PrefixUtilization	Utilization percentage for Ipv6 prefix by this data plane.

show ipam dp <dataplane-name>

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv4.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6 prefix.

show ipam dp <dataplane-name> ipv4-address

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
Route	Route allocated for this data plane.
N/P	Display the NodeMgr instance IDs from which it received routes Flag Indication S(Static) and O(Offline).

show ipam pool <pool-name> ipv6-addr

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

show ipam

Field	Description
PoolName	Displays Ipv4Utilization, Ipv6AddrUtilization, and Ipv6PrefixUtilization.
DpName	Displays Ipv4Utilization, Ipv6AddrUtlization, and Ipv6PrefixUtlization.

show nrf registration-info

Table 498: show nrf registration-info Command Output Description

Field	Description
NF Status	Displays the NRF registration information.
Registration Time	Displays the time of registration with NRF.
Active MgmtEP Name	Displays the active NRF management endpoint name.
Heartbeat Duration	Displays the heartbeat duration.
Uri	Displays the Uri information.

Field	Description
Host Type	Displays the NRF host type information.
GR Instance ID	Displays the GR instance ID.

show nrf subscription-info

Table 499: show nrf subscription-info Command Output Description

Field	Description
NF Instance Id	Displays the NF instance identity.
SubscriptionID	Displays the subscription identity information.
Actual Validity Time	Displays the actual validity time received from NRF server.
Requested Validity Time	Displays NF requested validity subscription time.
GR Instance ID	Displays the GR instance ID.

show nrf discovery info

Table 500: show nrf discovery info Command Output Description

Field	Description
NF Type	Displays the NF type information.
Number of Discovery Filters	Displays the number of discovery filters.
Number of NF Profiles	Displays the number of NF profiles.
GR Instance ID	Displays the GR instance ID.

show nrf discovery-info AMF discovery-filter

Table 501: show nrf discovery-info AMF discovery-filter Command Output Description

Step	Description
Discovery Filter	Displays the discovery filter information.
Expiry Time	Displays the expiry time for discovery filter.
GR Instance ID	Displays the GR instance ID.

show nrf discovery-info AMF discovery-filter <discovery_filter>

Table 502: show nrf discovery-info AMF discovery-filter <discovery_filter> Command Description

Field	Description
NF InstanceId	Displays the NF Instance Identity.
NF Type	Displays the NF Type Information.
Discovery Filter	Displays the Discovery Filter Information.
NF Status	Displays the NF Status Information.
Priority	Displays the Priority Information.
Capacity	Displays the NF Profile Capacity Information.
Load	Displays the Load Information.
Locality	Displays the Locality Information.
ipv4 address	Displays IPv4 Address received from the discovery response for this NF profile.
ipv6 address	Displays the IPv6 Address received from the discovery response for this NF profile.

show nrf discovery-info AMF discovery-filter <discovery_name> nf-discovery-profile <nf_discovery_profile> nf-service

Table 503: show nrf discovery-info AMF discovery-filter <discovery_name> nf-discovery-profile <nf_discovery_profile> nf-service Command Output Description

Field	Description
ServiceInstanceId	Displays the NF Service Instance ID.
ServiceName	Displays the NF Service Name.
UriScheme	Displays the Uri Scheme Information.

show peers all

Use this command to display the list all external inbound and outbound connections that are established by SMF. Only the key information is displayed. The following sample output is for the **show peers all** command:

```
[smf] smf# show peers all
GR                                                                    POD
CONNECTED                                    INTERFACE
INSTANCE  ENDPOINT      LOCAL ADDRESS   PEER ADDRESS     DIRECTION  INSTANCE     TYPE  TIME
       RPC     ADDITIONAL DETAILS       NAME       VRF
-------------------------------------------------------------------------------------------
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
hours   UDM     <none>                     n10
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
hours   UDM     <none>                     n10
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
hours   CHF     <none>                     n40
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
```

```
hours   PCF     <none>                      n7
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
hours   PCF     <none>                      n7
1         <none>        xx.xx.xx.xx    xx.xx.xx.xx:0000  Outbound   rest-ep-0    Rest  25
hours   AMF     <none>                      n11
```

Table 504: Output Fields Description for the show peers all Command

Field	Description
Additional Details	Specifies the additional details for the peer such as status or type.
Connected Time	Specifies the duration of the connected peer.
Direction	Specifies if peer connection direction is inbound or outbound.
Endpoint	Specifies the name of the endpoint.
GR Instance	Specifies the GR instance.
Interface Name	Specifies the interface name for the endpoint.
Local Address	Specifies the local IP address and port of the instance. For endpoint, it is the endpoint address and port. For RPC, it is the instance IP.
Peer Address|	Specifies the host and port of peer address.
Pod Instance	Specifies the pod for the peer.
RPC	Specifies the rpc of the specific peer.
Type	Specifies the type of peer.

show resources

Use this command to display the list of resource information for all pods in the cluster. The following sample output is for the **show resources** command:

```
[smf] show resources
                          TOTAL    USED     DISK
                          NODE     POD      USAGE   GO                GC
                    CPU   MEMORY   MEMORY   IN      ROUTINES  GC      PAUSE
POD INSTANCE        USAGE IN MB    IN MB    KBPS    COUNT     COUNT   IN NS
-------------------------------------------------------------------------------
bfdmgr-1            0     32117    56       0       56        1950    56
bfdmgr-2            0     32117    55       0       56        1935    55
bfdmgr-3            1     32117    54       0       56        2636    54
bfdmgr-4            0     32117    55       0       56        1946    55
bgpspeaker-pod-1    1     32117    104      0       94        9315    104
bgpspeaker-pod-2    1     32117    102      0       78        9300    102
cache-pod-1         4     7962     96       0       325       778     96
cache-pod-2         10    32117    91       0       325       778     91
gtpc-ep-0           2     32117    82       0       160       777     82
internal-gr-pod-1   2     32117    124      0       317       63      124
internal-gr-pod-2   1     32117    93       0       182       63      93
li-ep-0             0     32117    64       0       68        2723    64
nodemgr-0           3     32117    113      0       270       784     113
nodemgr-1           2     32117    115      0       252       784     115
oam-pod-0           3     7962     121      0       249       2110    121
```

```
protocol-0          2       32117   82      0       159         777     82
radius-ep-0         5       32117   76      0       145         782     76
rest-ep-0           3       32117   105     0       298         779     105
sgw-service-0       9       32117   138     0       262         779     138
smf-service-0       3       32117   228     0       347         2645    228
udp-proxy-0         0       32117   72      0       112         778     72
udp-proxy-1         0       32117   72      0       112         778     72
```

*Table 505: Output Field Descriptions for the **show resources** Command*

Field	Description
CPU Usage	Specifies CPU Usage In Percentage.
Disk Usage In Kbps	Specifies disk usage in Kbps.
GC Count	Specifies garbage collection cycle count.
GC Pause In NS	Specifies garbage collection pause in nanoseconds.
Go Routines Count	Specifies count of go routines.
Pod Instance	Specifies the instance info of the pod.
Total Node Memory In MB	Specifies total node memory usage in MB.
Used Pod Memory In MB	Specifies the consumption of pod memory in MB.

show rpc all

Use the **show rpc all** command to display the list of all the RPCs from all the pods with RPC and remote host information.

The following sample output is for the **show rpc all** command:

```
[smf] smf# show rpc all | tab | nomore
```

```
PROCESSING

                                                        CONNECTED  DISCONNECTED  MONITOR
INSTANCE
POD INSTANCE       NAME                          REMOTE ADDRESS             REMOTE HOST
    TYPE                    SET NAME          STATUS    TIME       TIME          RPCHOST
INFO                                              VERSION
-------------------------------------------------------------------------------------------
cache-pod-1        cache-pod-affinity            xx.xx.xx.xx:0000           cache-pod_20
    Grpc                    cache-pod_2       Started   4 weeks    <none>        false
<none>                                            <none>
cache-pod-1        cache-pod-affinity            xx.xx.xx.xx:0000           cache-pod_10
    Grpc                    cache-pod_1       Started   4 weeks    <none>        false
```

```
<none>                                              <none>
cache-pod-1        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_10
    GrpcServerClientStream  cache-pod_1      Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-1        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_20
    GrpcServerClientStream  cache-pod_2      Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-1        oam-pod                     xx.xx.xx.xx:0000          oam-pod
    GrpcStream              <none>           Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-1        Replication                 xx.xx.xx.xx:0000          cachepod_1
    GrpcStream              <none>           Started   3 weeks    <none>        false
<none>                                              <none>
cache-pod-1        Replication                 xx.xx.xx.xx:0000          cachepod_2
    GrpcStream              <none>           Started   3 weeks    <none>        false
<none>                                              <none>
cache-pod-2        cache-pod-affinity          xx.xx.xx.xx:0000          cache-pod_10
    Grpc                    cache-pod_1      Started   4 weeks    <none>        false
<none>                                              <none>
:
:
cache-pod-2        cache-pod-affinity          xx.xx.xx.xx:0000          cache-pod_20
    Grpc                    cache-pod_2      Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-2        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_20
    GrpcServerClientStream  cache-pod_2      Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-2        stream_cache-pod-affinity   xx.xx.xx.xx:0000          cache-pod_10
    GrpcServerClientStream  cache-pod_1      Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-2        oam-pod                     xx.xx.xx.xx:0000          oam-pod
    GrpcStream              <none>           Started   4 weeks    <none>        false
<none>                                              <none>
cache-pod-2        Replication                 xx.xx.xx.xx:0000          cachepod_1
    GrpcStream              <none>           Started   3 weeks    <none>        false
<none>                                              <none>
cache-pod-2        Replication                 xx.xx.xx.xx:0000          cachepod_2
    GrpcStream              <none>           Started   3 weeks    <none>        false
<none>                                              <none>
example-rest-ep-1  example-service               example-service:0000      example-service0
    Grpc                    example-service  Started   2 weeks    <none>        true
example.example-service.cluster1.example-data.12  <none>
```

Table 506: Output Field Descriptions for the show rpc Command

Field	Description
Connected Time	Specifies the duration when the RPC host is connected.
Disconnected Time	Specifies the duration when the RPC host is disconnected.
Monitor RPC Host	Indicates whether the RPC host is being monitored for connection status.
Name	Displays the name of the RPC registered in pod.
Pod Instance	Displays the instance information of the pod.
Processing Instance Info	Indicates the processing instance name, if available.

Field	Description
Remote Address	Displays IP address and port of remote endpoint.
Remote Host	Displays the name of the RPC host.
Set Name	Displays the RPC set name for a group of RPC hosts.
Status	Displays the current status of the RPC host. The status values are Started, Starting, and Stopped.
Type	Displays the type of connection such as Rest, Grpc, and GrpcStream.
Version	Displays the version of the RPC host API, if available.

show running-status

Use this command to display the running status related information for all the pods in system. The following sample output is for the **show running-status** command:

```
[smf] smf# show running-status
                    RUNNING  SYSTEM  START
POD INSTANCE        STATUS   HEALTH  TIME
-----------------------------------------------
bfdmgr-1            Started  Normal  2 hours
bfdmgr-2            Started  Normal  2 hours
bgpspeaker-pod-1    Started  Normal  2 hours
bgpspeaker-pod-2    Started  Normal  2 hours
cache-pod-1         Started  Normal  2 hours
cache-pod-2         Started  Normal  2 hours
dns-proxy-0         Started  Normal  2 hours
dns-proxy-1         Started  Normal  2 hours
gtpc-ep1-1          Started  Normal  2 hours
gtpc-ep1-2          Started  Normal  2 hours
gtpc-ep2-1          Started  Normal  2 hours
gtpc-ep2-2          Started  Normal  2 hours
internal-gr-pod-1   Started  Normal  2 hours
internal-gr-pod-2   Started  Normal  2 hours
li-ep-0             Started  Normal  2 hours
li-ep-1             Started  Normal  2 hours
nodemgr-0           Started  Normal  2 hours
nodemgr-1           Started  Normal  2 hours
oam-pod-0           Started  Normal  2 hours
protocol1-1         Started  Normal  2 hours
protocol1-2         Started  Normal  2 hours
protocol2-1         Started  Normal  2 hours
protocol2-2         Started  Normal  2 hours
radius-ep-0         Started  Normal  2 hours
radius-ep-1         Started  Normal  2 hours
rest-ep-0           Started  Normal  2 hours
rest-ep-1           Started  Normal  2 hours
sgw-service-0       Started  Normal  2 hours
sgw-service-1       Started  Normal  2 hours
sgw-service-2       Started  Normal  2 hours
sgw-service-3       Started  Normal  2 hours
sgw-service-4       Started  Normal  2 hours
sgw-service-5       Started  Normal  2 hours
smf-service-0       Started  Normal  2 hours
smf-service-1       Started  Normal  2 hours
smf-service-2       Started  Normal  2 hours
```

```
smf-service-3      Started  Normal  2 hours
smf-service-4      Started  Normal  2 hours
smf-service-5      Started  Normal  2 hours
udp-proxy-0        Started  Normal  2 hours
udp-proxy-1        Started  Normal  2 hours
```

*Table 507: Output Field Descriptions for the **show running-status** Command*

Field	Description
Pod Instance	Specifies the instance info of the pod.
Running Status	Specifies the system running status (Starting, Started, Stopping, or Stopped).
Start Time	Specifies the start time of the application.
System Health	Specifies the health status of the application.

show sessions affinity

Use this command to display affinity count, pod instance wise. This affinity count defines the affinity of sessions toward the pod. The following sample output is for the **show sessions affinity** command:

```
[smf] smf# show sessions affinity
POD
INSTANCE    COUNT
-------------------
service-1   10
service-11  12
service-12  15
service-13  12
service-14  15
service-2   15
service-3   14
service-4   19
```

*Table 508: Output Field Descriptions for the **show sessions affinity** Command*

Field	Description
Count	Specifies the affinity count.
Pod Instance	Specifies the instance info of the pod.

show sessions commit-pending

Use this command to display the current number of sessions per pod along with the sessions that are pending commit in the database. The following sample output is for the **show sessions commit-pending** command:

```
[smf] smf# show sessions commit-pending
                                          DB
               GR                PENDING  BINARY  LAST DB SYNC
POD INSTANCE   INSTANCE  COUNT   COMMIT   SIZE    TIME
-------------------------------------------------------------------------
sgw-service-1  1         0       0        0       Less than a second
sgw-service-1  2         0       0        0       Less than a second
sgw-service-2  1         0       0        0       Less than a second
sgw-service-2  2         0       0        0       Less than a second
sgw-service-4  1         0       0        0       Less than a second
```

```
sgw-service-4  2         0      0        0       Less than a second
sgw-service-5  1         0      0        0       Less than a second
sgw-service-5  2         0      0        0       Less than a second
smf-service-0  1         0      0        0       Less than a second
smf-service-0  2         0      0        0       Less than a second
smf-service-1  1         0      0        0       Less than a second
smf-service-1  2         0      0        0       Less than a second
smf-service-2  1         0      0        0       Less than a second
smf-service-2  2         0      0        0       Less than a second
smf-service-4  1         0      0        0       Less than a second
smf-service-4  2         0      0        0       Less than a second
smf-service-5  1         0      0        0       Less than a second
smf-service-5  2         0      0        0       Less than a second
```

*Table 509: Output Field Descriptions for the **show sessions commit-pending** Command*

Field	Description
Count	Specifies the count.
DB Binary Size	Specifies the DB binary Size.
GR Instance	Specifies the GR Instance ID.
Last DB Sync Time	Specifies the previous DB sync time.
Pod Instance	Specifies the instance info of the pod.

show subscriber

This commands displays the existing show subscriber CLI output with the newly added CLI output.

Table 510: show subscriber Command Output Description

Field	Description
all	Displays the information for all SUPIs or IMEIs.
amf	Displays the AMF address.
chf	Displays the CHF address.
count	Displays the number of sessions.
debug	Displays the debugging information.
dnn	Displays the DNN value.
gr-instance	Displays the Geographic Redundancy (GR) instance.
gtp-peer	Displays the GTP-peer address.
imei	Displays the IMEI containing 15 or 16 digits.

Field	Description
namespace	**Important** This keyword is deprecated in release 2021.02.0 and replaced with the **nf-service** keyword. Displays the product namespace under which to search. Default: none.
nf-service { none | sgw | smf }	Displays the network function service under which to search. Default: none. **Important** This keyword is mandatory with the **show subscriber** command to display the output.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
roaming-status	Displays the UE roaming status—homer, visitor-lbo, visitor-hr, roamer.
supi	Displays the SUPI value.
udm	Displays the UDM address.
upf	Displays the UPF address.
rulebase	Displays the subscriber using the rulebase.
|	The output modifiers.

show subscriber all

Use this command to display all the sessions for all the SUPIs and NF services. The following sample output is for the **show subscriber all** command:

```
[smf] smf# show subscriber all
subscriber-details
{
  "subResponses": [
    [
      ""
    ],
    [
      "id-index:1:0:32768",
      "id-value:16777505",
      "imsi:imsi-123456123456123",
      "msisdn:msisdn-123456123456123",
      "imei:imei-310220000000000",
      "upf:xx.xx.xx.xx",
      "upfEpKey: xx.xx.xx.xx: xx.xx.xx.xx ",
      "s5s8Ipv4: xx.xx.xx.xx ",
      "s11Ipv4: xx.xx.xx.xx",
      "namespace:sgw",
      "nf-service:sgw"
    ],
    [
      "roaming-status:roamer",
      "ue-type:4g-only",
      "supi:imsi-123456123456123",
      "gpsi:msisdn-123456123456123",
      "pei:imei-310220000000000",
```

```
      "psid:69",
      "dnn:papn1.com",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "auth-status:authenticated",
      "pcfGroupId:PCF-*",
      "policy:2",
      "pcf: xx.xx.xx.xx",
      "ipv4-addr:pool-static1-v4/xx.xx.xx.xx",
      "ipv4-pool:pool-static1-v4",
      "ipv4-range:pool-static1-v4/xx.xx.xx.xx",
      "ipv4-startrange:pool-static1-v4/",
      "id-index:1:0:32768",
      "id-value:8/310",
      "upf:xx.xx.xx.xx",
      "chfGroupId:CHF-*",
      "chf:209.165.202.133",
      "gtp-peer:xx.xx.xx.xx",
      "peerGtpuEpKey:xx.xx.xx.xx:xx.xx.xx.xx",
      "namespace:smf",
      "nf-service:smf"
    ],
    [
      ""
    ]
  ]
}
```


Table 511: show subscriber Command Output Description

Field	Description
subscriber-details	Displays the details for all subscribers in JSON format.

show subscriber count

This command displays the CLI options for the count CLI command.

Table 512: show subscriber count Command Output Description

Field	Description
all	Displays all the SUPIs.
amf	Displays the AMF address.
apn	Displays the APN value.
auth-status	Displays the RADIUS Authentication Status - authenticated or unauth status.
chf	Displays the CHF address.
connectivity	Displays the connectivity - 4g or 5g.
dnn	Displays the DNN value.
emergency	Displays the Emergency Session indication - true or false.

Field	Description
gpsi	Displays the GPSI value.
gr-instance	Displays the subscriber's from the provided GR Instance.
gtp-peer	Displays the GTP peer address.
ipv4-addr	Displays IPv4 address in the format:- <poolName> or <ipv4-addr>.
ipv4-pool	Displays the IPv4 pool name.
ipv4-range	Displays the IPv4 address range.
ipv6-pfx	Displays IPv6 prefix in the format <poolName> or <ipv6-pfx>
ipv6-pool	Displays the IPv6 pool name.
ipv6-range	Displays the IPv6 prefix range.
msid	Displays the MSID value.
msisdn	Displays the MSISDN value
namespace	Displays the deprecated option, use nf-service instead (default: none).
nf-service	Displays the network function service (SMF, S-GW) under which to search (default: none). This parameter can be used with the slice name or the NSSAI filter for SMF in the following format: **nf-service smf** *slice-name* or **nf-service smf** *nssai*.
pcf	Displays the PCF address.
peerGtpuEpKey	Displays the GTPU peer address in <upf_addr:gptu-peer-addr> format.
pei	Displays the PEI - Permanent Equipment Identifier.
policy	Displays the Subscriber Policy Information.
rat	Displays the RAT type as 4G or 5G.
roaming-status	Displays the UE roaming status – homer/roamer/visitor-hr/lbo-visitor.
smf	Displays the SMF address.
supi	Displays the specific SUPI value.
udm-sdm	Displays the UDM-SDM Address.
udm-uecm	Displays the UDM-UECM Address.
ue-type	Displays the device capability - 4g-only or nr-capable.
upf	Displays the UPF address.

Field	Description
rulebase	Displays the subscriber using the rulebase.
|	Displays the output modifiers.

show subscriber count all

Use this command to display the total number of sessions for all the SUPIs. The following sample output is for the **show subscriber count all** command:

```
[smf] smf# show subscriber count all
subscriber-details
{
  "sessionCount": 20
}
```

*Table 513: Output Field Descriptions for the **show subscriber count all** Command*

Field	Description
subscriber-details	Displays the count for all subscribers in JSON format.

show subscriber debug-info

This command displays the debug information for the specific SUPI value where the PSID value is optional.

Table 514: show subscriber debug-info Command Output Description

Field	Description
gpsi	Displays GPSI value.
gr-instance	Displays the subscriber's from the provided GR Instance.
imsi	Displays the IMSI value.
msid	Displays the MSID value.
msisdn	Displays the MSISDN value.
namespace	Deprecated option, Use nf-service instead (default: none)
nf-service	Displays the network function service (SMF, SGW) under which to search (default: none).
pei	Displays the PEI or IMEI value.
supi	Displays the SUPI value, value must include the imsi- prefix.
|	Displays the output modifiers.

show subscriber gpsi

Table 515: show subscriber gpsi

Field	Description
policy	Displays the policy information.
ipv4-addr	Displays the IPv4 pool name.
dnn	Displays the DNN value.
pcf	Displays the PCF Address.
rat	Displays the RAT Type—nr, e-utran, or wlan information.
connectivity	Displays the connectivity—4G or 5G.
ipv4-range	Displays the IPv4 address range.
chf	Displays the CHF address.
pei	Displays the Permanent Equipment Identifier (PEI).
udm	Displays the UDM address.
upfEpKey	Displays the UPF address EP key information.
ipv6-pfx	Displays the IPv6 prefix information.
ipv6-pool	Displays the IPv6 pool name.
chfGroupId	Displays the CHF address group ID information.
gpsi	Displays the Generic Public Subscription Identifier (GPSI).
pcfGroupId	Specifies PCF Address group ID.
upf	Displays the UPF address.
ipv4-pool	Displays the IPv4 pool name.
ipv6-range	Displays the IPv4 address range.
amf	Displays the AMF address.
supi	Displays the SUPI value.
access	Displays the access information.
gr-instance	Displays the GR instance.

show subscriber nf-service smf

Important The wildcard input is not supported with the listed filters.

Table 516: show subscriber nf-service smf Command Output Description

Field	Description
apn	Displays the APN value.
msid	Displays the MSID value.
msisdn	Displays the MSISDN value.
roaming-status	Displays the UE roaming status—homer, visitor-lbo, visitor-hr, roamer.

smf	Displays the subscriber details based on the IP address value of the vSMF or hSMF.
	For example:
	`[smf] smf# show subscriber nf-service smf smf <smf_url> subscriber-details`
	`{}`

rulebase	Displays the subscriber using the rulebase.

show subscriber pei

Table 517: show subscriber pei

Field	Description
policy	Displays the policy information.
ipv4-addr	Displays the IPv4 pool name.
dnn	Displays the DNN value.
pcf	Displays the PCF Address.
rat	Displays the RAT Type—nr, e-utran, or wlan information.
connectivity	Displays the connectivity—4G or 5G.
ipv4-range	Displays the IPv4 address range.
chf	Displays the CHF address.
pei	Displays the Permanent Equipment Identifier (PEI).
udm	Displays the UDM address.
upfEpKey	Displays the UPF address EP key information.

Field	Description
ipv6-pfx	Displays the IPv6 prefix information.
ipv6-pool	Displays the IPv6 Pool name.
chfGroupId	Displays the CHF address group ID information.
gpsi	Displays the Generic Public Subscription Identifier (GPSI).
pcfGroupId	Displays the PCF address group ID.
upf	Displays the UPF address.
ipv4-pool	Displays the IPv4 pool name.
ipv6-range	Displays the IPv4 address range.
amf	Displays the AMF address.
supi	Displays the SUPI value.
access	Displays the access information.
gr-instance	Displays the GR instance.
rulebase	Displays the subscriber using the rulebase.

show subscriber supi <supi_value> nf-service smf psid <psid_value> full

This command displays detailed subscriber information.

Table 518: show subscriber supi <supi_value> nf-service smfpsid <psid_value> full Command Output Description

Field	Description
sessTimeStamp	Displays the connected time of the session.
callDuration	Displays the call duration.
commonId	Displays the call ID equivalent for the session (common ID).
ipPool, ipv6Pool	Displays the IP pool from which the address has been allocated.
linkedEbi	Displays the linked EBI for a session.
snssai	Displays the sNssai details.
smfIwkEpsInd	Displays the SMF EPS IWK decision based on AMF and UDM data.
TotalNumberOfPdrs	Displays the number of associated PDRs.
TotalNumberOfFars	Displays the number of associated FARs.
TotalNumberOfQers	Displays the number of associated QERs.

Field	Description
TotalNumberOfUrrs	Displays the number of associated URRs.
upfSeid	Displays the remote SEID for a particular UPF session.
epsInterworking Indication	Displays the EPS interworking indication status of AMF.
ebi	Displays the ERAB ID allocated for each flow.
revalidationTime	Displays the revalidation timer information for a session.

show subscriber supi <supi_value> nf-service smfpsid <psid_value> summary

This command displays detailed information about subscriber sessions. This command improves usability and can be used for debugging purposes.

Table 519: show subscriber supi <supi_value> nf-service smf psid <psid_value> summary Command Output Description

Field	Description
supi	Displays the 5G Subscription Permanent Identifier.
pduSessionId	Displays the PDU session identifier.
pduSesstype	Displays the PDU session type.
accessType	Displays the access type.
dnn	Displays the DNN profile name.
allocatedIp/ allocatedIpv6	Displays the allocated IP address details.
ratType	Displays the RAT type.
sessTimeStamp	Displays the connected Time of the session.
TotalDynamicRules/ TotalStaticRules/ TotalPredefinedRules	Displays the number of Dynamic rules or Static rules or Predefined rules.
TotalGBRFlows/ TotalNonGBRFlows	Displays the number of GBR flows or non-GBR flows.
pcfInteraction	Displays the PCF interaction status.
ruleBase	Displays the rulebase name.
chargingId	Displays the charging descriptor name.
offlineConverted	Displays the online charging parameters converted to offline.
chargingDisabled	Displays the charging parameters when charging is disabled.
dropTraffic	Displays the charging parameters when traffic is dropped.

Field	Description
gtppGrp	Displays the EGCDR configuration for GTPP name.
profileName	Displays the charging profile name.
deferredUsageCount	Displays the number of deferred multi-unit usages.
smfSeid	Displays the local SEID for a particular UPF session.
upfSeid	Displays the remote SEID for a particular UPF session.
TunnelID	Displays the GTPU peer tunnel ID.
TunnelName	Displays the GTPU peer tunnel name.
RemoteTeid (teid/ipAddr)	Displays the GTPU peer TEID and IP address.
TotalNumberOfPdrs	Displays the number of associated PDRs.
TotalNumberOfFars	Displays the number of associated FARs.
TotalNumberOfQers	Displays the number of associated QERs.
TotalNumberOfUrrs	Displays the number of associated URRs.

clear Commands

This section lists some of the key clear commands that are available for troubleshooting the issues.

Important The SMF Ops center allows you to issue only one **clear subscriber all** command at a time. The Ops center restricts the subsequent **clear subscriber all** and other variants of **clear subscriber** commands until the ongoing **clear subscriber all** command is complete.

Note The Ops Center displays the expected waiting time for an ongoing bulk **clear subscriber** CLI command. In addition, the clear subscriber CLI gets blocked while the processing of the earlier CLI is in progress.

clear subscriber

"`clear subscriber`" command displays the list of subscriber SMF fields.

Table 520: clear subscriber Command Output Description

Field	Description
all	Clears all the sessions information.
amf	Clears subscriber based on AMF address information.
chf	Clears subscriber based on CHF address information.

Field	Description
dnn	Clears subscriber based on DNN value.
gr-instance	Clears subscriber based on the specified Geographic Redundancy (GR) instance information.
gtp-peer	Clears subscriber based on GTP-PEER address information.
ipv4-pool	Clears subscriber based on IPv4 pool name.
ipv4-range	Clears subscriber based on IPv4 address-range value.
ipv6-pool	Clears subscriber based on IPv6 pool name information.
ipv4-range	Clears subscriber based on IPv6 prefix-range value.
ipv6-range	Clears subscriber based on IPv6 prefix-range value.
namespace	**Important** This keyword is deprecated in release 2021.02.0 and is replaced with the **nf-service** keyword. Clears subscriber based on the respective namespace. Default: none.
nf-service { none | sgw | smf }	Clears subscriber based on the specified network function service. Default: none. **Important** This keyword is mandatory with the **clear subscriber** command to display the output.
pcf	Clears subscriber based on PCF address information.
policy	Clears subscriber information based on policy.
purge	Clears true, if purged locally.
reactivation [true | false]	Clears subscriber based on the Reactivation Required cause value. This option is set to true if reactivation is requested.
roaming-status	Clears subscriber based on the UE roaming status—homer, visitor-lbo, visitor-hr, roamer values.
sgw	Clears subscriber information based on the S-GW address information.
smf	Clears subscriber information based on the SMF address information.
supi	Clears subscriber based on the SUPI value.
rulebase	Clears subscriber using the rulebase.
|	The output modifiers.

clear subscriber nf-service smf

Important The wildcard input is not supported with the listed filters.

"`clear subscriber nf-service smf` " command displays the list of nf-service SMF fields.

Table 521: clear subscriber nf-service smf Command Output Description

Field	Description
apn	Clears subscriber based on the APN value.
dnn	Clears subscriber based on the DNN value.
msid	Clears subscriber based on the MSID value.
msisdn	Clears subscriber based on the MSISDN value.
reactivation [true | false]	Clears subscriber based on the Reactivation Required cause. This option is set to true if reactivation is requested.
roaming-status	Clears subscriber based on the UE roaming status—homer, visitor-lbo, visitor-hr, roamer.

rulebase	Clears subscriber based on the rulebase value.
	This keyword is used as a secondary filter. Ensure that the rulebase value includes the rulebase prefix.
	For example:
	`[smf] smf# clear subscriber nf-service smf dnn <dnn_val> rulebase <rulebase_value>`
	`result`
	`ClearSubscriber Request submitted`

rulename	Modifies session based on the rulename value.
	This keyword is used as a secondary filter. Ensure that the rulename value includes the rulename prefix.
	For example:
	`[smf] smf# clear subscriber nf-service smf dnn <dnn_val> rulename <rulename_value>`
	`result`
	`ClearSubscriber Request submitted`

smf	Clears subscriber based on the IP address value of the vSMF or hSMF.
	For example:
	`[smf] smf# clear subscriber nf-service smf smf <smf_url>`
	`result`
	`ClearSubscriber Request submitted`

Field	Description

x5qi	Modifies session based on 5QI for 5G sessions, and QCI for 4G and WLAN sessions. This keyword is used as a secondary filter.
	For example:
	`smf] smf# clear subscriber supi <supi_val> x5qi <x5qi_value>`
	`result`
	`ClearSubscriber Request submitted`
	
	`[smf] smf# clear subscriber apn <apn_val> x5qi <x5qi_value>`
	`result`
	`ClearSubscriber Request submitted`

clear subscriber supi imsi <imsi_value>

"`clear subscriber supi imsi` *`imsi_value`*" command displays the list of subscriber SUPI IMSI value SMF fields.

Table 522: clear subscriber supi imsi <imsi_value> Command Output Description

Field	Description
ebi	Clears subscriber based on EPS bearer ID value.
imsi	Clears subscriber based on IMSI information.
purge	Clears true, if purged locally.
|	Output modifier.

clear subscriber supi imsi <imsi_value> psid <psid_value>

"`clear subscriber supi imsi` *`imsi_value`* `psid` *`psid_value`*" command displays the list of subscriber SUPI IMSI and PSID value SMF fields.

Table 523: clear subscriber supi imsi <imsi_value> psid <psid_value> Command Output Description

Field	Description
ebi	Clears subscriber based on EPS bearer ID value.
imsi	Clears subscriber based on IMSI information.
psid	Clears subscriber based on Service ID value.
purge	Clears true, if purged locally.
|	Output modifier.

Monitor Subscriber and Monitor Protocol

Feature Description

The SMF supports the Monitor Subscriber and Monitor Protocol on the Kubernetes environment. The monitor tools allow you to capture messages of subscribers and protocols.

This section provides information on CLI commands for monitoring the health of SMF.

Configuring the Monitor Subscriber and Monitor Protocol Feature

Monitoring the Subscriber Session

To monitor the subscriber in the SMF, use the following CLI command:

monitor subscriber [capture-duration *duration* **| gr-instance** *gr_instance_id* **| imei** *imei_id* **| imsi** *imsi_value* **| internal-messages [yes] | namespace [sgw | smf] | nf-service [sgw | smf] | supi** *supi_id* **| transaction-logs [yes]]**

NOTES:

- **capture-duration** *duration*: Specify the duration in seconds during which monitor subscriber is enabled. The default value is 300 seconds (5 minutes). This is an optional parameter.
- **gr-instance** *gr_instance_id*: Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **imei** *imei_id*: Specify the subscriber IMEI. For example: 123456789012345, *
- **imsi** *imsi_value*: Specify the subscriber IMSI. For example: 123456789, *
- **internal-messages [yes]**: Enable internal messages when set to **yes**. By default, it is disabled. This is an optional parameter.
- **namespace [sgw | smf]**: Enable the specified namespace. By default, namespace is set to none. This is an optional parameter.

Important This keyword is deprecated in release 2021.02.0 and replaced with **nf-service** keyword.

- **nf-service [sgw | smf]** : Enable the specified NF service. By default, nf-service is set to none. This is a mandatory parameter.

Important The **nf-service** keyword replaces the **namespace** keyword in release 2021.02 and beyond.

- **supi** *supi_id*: Specify the subscriber identifier. For example: imsi-123456789, imsi-123*
- **transaction-logs [yes]**: Enable transaction logs when set to **yes**. By default, it is disabled. This is an optional parameter.

To view the transaction history logs, use the **dump transactionhistory** command.

Note The most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

The **monitor subscriber** CLI command can be run simultaneously on multiple terminals. For example, run the CLI simultaneously in two SMF Ops Center terminals for two subscribers (for example, imsi-123456789012345 and imsi-456780123456789) to implement the following:

- Monitor the duration when the monitor subscriber is enabled
- View internal messages for the specified subscriber
- View transaction logs for the specified subscriber

Terminal 1: The following command monitors and displays subscriber messages for the specified subscriber.

```
monitor subscriber supi imsi-123456789012345 capture-duration 1000 internal-messages yes
```

Terminal 2: The following command monitors and displays transaction logs for the specified subscriber.

```
monitor subscriber supi imsi-456780123456789 capture-duration 500 internal-messages yes
transaction-logs yes
```

After the capture duration is completed, stop the CLI by using the **Ctrl+C** keys. The captured messages are reordered and stored in a file. To retrieve the list of stored files, use the **monitor subscriber list** CLI command.

For example:

```
monitor subscriber list
RELEASE_NAMESPACE: 'smf'
'monsublogs/subscriberID_imsi-*_AT_2019-10-22T09:19:05.586237087.txt.sorted'
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

Monitoring Subscriber Dump

To view the sorted file on the SMF Ops Center screen, use the following CLI command:

monitor subscriber dump filename *filename*

For example:

```
monitor subscriber dump filename
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

Monitoring the Interface Protocol

To monitor the interface protocol on the SMF, use the following CLI command:

monitor protocol { interface *interface_name* **[capture-duration** *duration* **| gr-instance***gr_instance* **| pcacp yes | |] | list [|] }**

NOTES:

- **interface** *interface_name*—Specify the interface name on which PCAP is captured. This CLI allows the configuration of multiple interface names in a single CLI command.
- **capture-duration** *duration*—Specify the duration in seconds during which pcap is captured. The default is 300 seconds (5 minutes).

- The configured interface names can be retrieved using the **show endpoint** CLI command.
- **gr-instance** *gr_instance_id*—Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **pcap yes**—Configure this option to enable PCAP file generation. By default, this option is disabled.
- **list**—Monitor protocol list files.

Important The **monitor protocol** command in Exec mode is restricted based on pod's CPU utilization configured through **monitor protocol cpu-limit** *threshold_percentage* command in the Global Configuration mode.

The **monitor protocol** CLI can be run simultaneously on multiple terminals. Also, the **interface** *interface_name* CLI allows the configuration of multiple endpoint names in a single CLI command.

For example:

```
monitor protocol interface sbi,N4:209.165.200.241:8805,gtpc
capture-duration 1000
```

UPF Monitor Subscriber from SMF

Feature Description

SMF sends the tracing trigger to the selected UPF automatically. Sending the trigger from SMF facilitates in parsing minimum files for troubleshooting across Control Plane and User Plane.

Note

- The operator can configure a maximum of five subscribers at a time on SMF for monitoring.
- When the data tracing is enabled, the available VPP, FCAP, and MEH are captured on the UPF PCAP.
- When the protocol tracing is enabled, the following options are enabled on UPF:
  - Rulematch Events
  - L3 Data
  - PFCP Events Tracing
  - EDR
  - SessMGR
  - Subscriber Summary After Call Disconnect
- After SMF GR switchover, the existing sessions of the monitored subscribers aren't impacted on UPF. As monitor nf CLI exists in the config mode, an operator needs to configure the CLI on both the SMF instances.

For UPF reload and switchover scenarios, see the UPF troubleshooting guide for monitor NF.

This section provides information on CLI commands for configuring the UPF monitor subscriber from SMF.

Configuring UPF Monitor Subscriber from SMF

Use the following configuration to enable or disable the UPF Monitor Subscriber protocol from SMF.

- Enabling UPF Monitor Subscriber from SMF
- Disabling UPF Monitor Subscriber from SMF

Enabling UPF Monitor Subscriber from SMF

Use the following configuration to enable UPF Monitor Subscriber from SMF.

```
config
   monitor nf subscriber  [ gpsi gpsi_value |imei imei_id|imsiimsi_value control
 { true | false }  data { true | false } target-nf { sgwu | upf } ]
   end
```

NOTES:

- **monitor nf** —Specify the NF that you want to monitor.
- **gpsi** *gpsi_value*—Specify the subscriber GPSI.
- **imsi** *imsi_value*—Specify the subscriber IMSI. For example: 123456789, *
- **imei** *imei_id*—Specify the subscriber IMEI. For example: 123456789012345, *
- **control { true | false }**—Specify whether to enable or disable the control event tracing.
- **data { true | false }** —Specify whether to enable or disable the data event tracing.
- **target-nf { sgwu | upf }** —Specify the target NF as SGW-U or UPF. **target-nf** is an optional parameter and if an operator doesn't configure this parameter, monitor subscriber is enabled on both the UPF and SGW-U.

Configuration Example

The following is an example configuration.

```
[smf] smf(config)# monitor nf subscriber
   imsi 234150999999999
      control true
      data true
      target-nf upf
exit
```

Disabling UPF Monitor Subscriber from SMF

Use the following configuration to disable UPF Monitor Subscriber from SMF.

```
config
   [ no ]monitor nf subscriber  [ gpsi gpsi_value |imei imei_id | imsiimsi_value
 ]
   end
```

NOTES:

- **monitor nf** —Specify the NF that you want to monitor.

- **gpsi** *gpsi_value*—Specify the subscriber GPSI.
- **imsi** *imsi_value*—Specify the subscriber IMSI. For example: 123456789, *
- **imei** *imei_id*—Specify the subscriber IMEI. For example: 123456789012345, *

Alerts

Feature Description

When the system detects an anomaly, CEE Ops Center generates an alert notification. The system statistics are the cause for these alert notifications. You can set an expression to trigger an alert when the expression becomes true.

How it Works

The Common Execution Environment (CEE) uses the Prometheus Alert Manager for alerting operations. The CEE YANG model - either through CLI or API - allows users to view the active alerts, silenced alerts, and alert history. Also, the applications can call the alert API directly to add or clear alerts. The Prometheus Alert Manager API (v2) is the standard API used.

The Prometheus Alerts Manager includes the following options:

- **Defining Alert Rules**: This option defines the types of alerts that the Alert Manager should trigger. Use the Prometheus Query Language (PromQL) to define the alerts.
- **Defining Alert Routing**: This option defines the action the Alert Manager should take after receiving the alerts. At present, the SNMP Trapper is supported as the outbound alerting. Also, the CEE provides an Alert Logger for storing the generated alerts.

Configuring Alert Rules

Use the following sample configuration to configure the alert rules:

```
config
   alerts rules group alert_group_name
   interval-seconds seconds
   rule rule_name
      expression promql_expression
      duration duration
      severity severity_level
      type alert-type
      annotation annotation_name
      value annotation_value
      exit
   exit
```

NOTES:

- **alerts rules**: Specifies the Prometheus alerting rules.
- **group** *alert_group_name*: Specifies the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The alert-group-name must be a string in the range of 0–64 characters.
- **interval-seconds** *seconds*: Specifies the evaluation interval of the rule group in seconds.
- **rule** *rule_name*: Specifies the alerting rule definition. *rule_name* is the name of the rule.
- **expression** *promql_expression*: Specifies the PromQL alerting rule expression. *promql_expression* is the alert rule query expressed in PromQL syntax.
- **duration** *duration*: Specifies the duration of a true condition before it is considered true. *duration* is the time interval before the alert is triggered.
- **severity** *severity_level*: Specifies the severity of the alert. *severity-level* is the severity level of the alert. The severity levels are critical, major, minor, and warning.
- **type** *alert_type*: Specifies the type of the alert. *alert_type* is the user-defined alert type. For example, Communications Alarm, Environmental Alarm, Equipment Alarm, Indeterminate Integrity Violation Alarm, Operational Violation Alarm, Physical Violation Alarm, Processing Error Alarm, Quality of Service Alarm, Security Service Alarm, Mechanism Violation Alarm, or Time Domain Violation Alarm.
- **annotation** *annotation_name*: Specifies the annotation to attach to the alerts. *annotation_name* is the name of the annotation.
- **value** *annotation_value*: Specifies the annotation value. *annotation_value* is the value of the annotation.

The following example configures an alert, which is triggered when the percentage of Unified Data Management (UDM) responses is less than the specified threshold limit.

Example:

```
 config terminal
  alerts rules group SMFUDMchk_incr
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold‟
  exit
 exit
exit
```

You can view the configured alert using the **show running-config alerts** command.

Example:

The following example displays the alerts configured in the running configuration:

```
 show running-config alerts
  interval-seconds 300
  rule SMFUDMchk_incr
  expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
```

```
 < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of UDM responses is less than threshold‟

  exit
 exit
exit
```

Viewing Alert Logger

The Alert Logger stores all the generated alerts by default. You can view the stored alerts using the following command.

show alert history [filtering]

You can narrow down the result using the following filtering options:

- **annotations**: Specifies the annotations of the alert.
- **endsAt**: Specifies the end time of the alert.
- **labels**: Specifies the additional labels of the alert.
- **severity**: Specifies the severity of the alert.
- **source**: Specifies the source of the alert.
- **startsAt**: Specifies the start time of the alert.
- **type**: Specifies the type of the alert.

The following example history of the alerts configured in the system appears:

Example:

```
show alerts history
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold.” ]
```

You can view the active and silenced alerts with the **show alerts active** command.

The following active alerts example appears. The alerts remain active as long as the evaluated expression is true.

Example:

```
show alerts active
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold.” ]
```

Call Flow Procedure Alerts

This section provides detail of commands that are required to configure alerts related to various call flow procedures.

The alerts, which are specific to SMF, are configured on the Common Execution Environment (CEE). The expressions are developed and new counters are created. Based on the user requirements, the call flow procedure alerts are configured in CEE. These alerts are triggered when the conditions, as specified by users, are met.

4G PDN Modify

Use the following sample configuration to configure alerts related to the 4G PDN Modify procedure:

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNModify
   expression "sum(smf_service_stats{procedure_type=~\"pdn_ho_location_changed|
pdn_ho_rat_type_changed|pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"success\"})/sum(smf_service_stats{procedure_type=~
\"pdn_ho_location_changed|pdn_ho_rat_type_changed |pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"attempted\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Modify is below
threshold"
   exit
exit
```

4G PDN Release Success

Use the following sample configuration to configure alerts related to the 4G PDN Release Success procedure:

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNRelease
   expression "sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Release is below
threshold."
   exit
exit
```

4G PDN Setup Success

Use the following sample configuration to configure alerts related to the 4G PDN Setup Success procedure:

```
alerts rules group SMFPDN
   interval-seconds 300
   rule SMFPDNSetup
   expression "sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"attempted\"} < 0.95 "
```

```
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G PDN Setup is below
threshold."
   exit
exit
```

4G to 5G HO Success

Use the following configuration to configure alerts related to the 4G to 5G HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule 4gTo5gHOSuccess
   expression
"sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\" ,
 status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 4G to 5G HO is below
threshold."
   exit
exit
```

4G To WiFi HO Success

Use the following configuration to configure alerts related to the 4G to WiFi HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule 4GtoWifiHOSuccess
   expression "sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

5G N2 HO Success

Use the following configuration to configure alerts related to the 5G N2 HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule N2HOSuccess
  expression "sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"success\"})
 / sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"attempted\"}) < 0.95 "
   severity major
```

```
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G N2 HO is below threshold."

   exit
exit
```

5G PDU Idle Success

Use the following configuration to configure alerts related to the 5G PDU Idle Success procedure:

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFPDUIdleSuccess
   expression "sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"success\"})
/ sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Idle is below threshold"

   exit
exit
```

5G PDU Modify Success

Use the following configuration to configure alerts related to the 5G PDU Modify Success procedure:

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionModifySuccess
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Modify is below
threshold"
   exit
exit
```

5G PDU Release Success

Use the following configuration to configure alerts related to the 5G PDU Release Success procedure.

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionReleaseFailure
   expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G PDU Setup is below
```

```
threshold"
   exit
exit
```

5G PDU Setup Success

Use the following configuration to configure alerts related to the 5G PDU Setup Success procedure:

```
alerts rules group SMFPDU
   interval-seconds 300
   rule SMFSessionSetupFailure
   expression "sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"attempted\"} < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

5G to 4G HO Success

Use the following configuration to configure alerts related to the 5G to 4G HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule 5gTo4gHOSuccess
   expression "sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|eps_fb_5g_4g_handover_idft
|pdn_5g_4g_handover_idft\" , status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|
eps_fb_5g_4g_handover_idft|pdn_5g_4g_handover_idft\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G to 4G HO is below
threshold."
   exit
exit
```

5G To WiFi HO Success

Use the following sample configuration to configure alerts related to the 5G to WiFi HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule 5GtoWifiHOSuccess
   expression "sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\" ,
 status=\"success\"}) / sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\"
 , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
```

```
   exit
exit
```

5G Xn HO Success

Use the following sample configuration to configure alerts related to the 5G Xn HO Success procedure:

```
alerts rules group Handover
   interval-seconds 300
   rule XnHOSuccess
  expression "sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"success\"})
 / sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"attempted\"}) < 0.95 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage successful 5G Xn HO is below threshold."

   exit
exit
```

PDN Session Create

Use the following sample configuration to configure alerts related to the PDN Session Create procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDNSessCreate
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\"pdn_sess_create\",status=\"success\"}[5m])) /
sum(increase(smf_service_stats{app_name=\"SMF\
/",procedure_type=\"pdn_sess_create\",status=\"  /attempted\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdn_sess_create procedure is
 lesser threshold."
   exit
exit
```

PDU Session Create

Use the following sample configuration to configure alerts related to the PDU Session Create procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessCreate
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\"pdu_sess_create\",status=\"success\"}[5m]))sum
/(increase(smf_service_stats{app_name=\"SMF\",  /procedure_type=\"pdu_sess_create\",status=\
  /"attempted\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of pdu_sess_create procedure is
 lesser threshold."
```

```
   exit
exit
```

PDU Session Modify

Use the following sample configuration to configure alerts related to the PDU Session Modify procedure.

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessModify
   expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".
/*req_pdu_sess_mod\",status=\"success\”}[5m]))sum(increase
/(smf_service_stats{app_name=\"SMF\",procedure_type=~
/\”.*req_pdu_sess_mod\",status=\"attempted\”}[5m]))  / < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of req_pdu_sess_mod procedure
is lesser threshold.”
   exit
exit
```

PDU Session Release

Use the following sample configuration to configure alerts related to the PDU Session Release procedure:

```
alerts rules group SMFProcStatus
   interval-seconds 300
   rule PDUSessRelease
   expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_rel\",status=\
  /"success\”}[5m]))sum(increase(smf_service_stats{app_name=\"SMF
/\",procedure_type=~\”.*req_pdu_sess_rel\",status=\  /"attempted\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the success percentage of req_pdu_sess_rel procedure
is lesser threshold.”
   exit
exit
```

Interface Specific Alerts

This section provides detail of commands that are required to configure alerts related to various interfaces.

GTPC Peer Down

Use the following commands to configure alerts related to the GTPC Peer Down procedure.

```
alerts rules group GTPCPeerDown
   interval-seconds 300
   rule GTPCPeerDown
   expression nodemgr_gtpc_peer_status{gtpc_peer_status=\“gtpc_peer_path_down\”})
   severity major
   type "Communications Alarm"
   annotation summary
```

```
   value "This alert is fired when the GTPC Path failure detected for peer crosses
threshold"
   exit
exit
```

N4 Message Success

Use the following commands to configure alerts related to the N4 Message Success procedure.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN4MessageSuccess
   expression "sum(protocol_udp_res_msg_total{message_direction=\"inbound\",
status=\"accepted\"}) / sum(protocol_udp_res_msg_total{message_direction=\"inbound\",
status=~\"accepted|denied\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

N4 UPF Association Down

Use the following commands to configure alerts related to the N4 UPF Association Down query by N4 address.

```
alerts rules group N4Association
   interval-seconds 300
   rule SMFAssociationRelease
   expression "proto_udp_res_msg_total{procedure_type=\"n4_association_release_res\",
message_direction= \"inbound\", status=\"accepted\"}) "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is released"
   exit
exit
```

N4 UPF Association Up

Use the following commands to configure alerts related to the N4 UPF Association Up query by N4 address.

```
alerts rules group N4Association
   interval-seconds 300
   rule N4AssociationUP
   expression "proto_udp_res_msg_total{procedure_type=\"n4_association_setup_res\",
message_direction= \"inbound\", status=\"accepted\"}"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the N4 Association with UPF is established"
   exit
exit
```

N7 Interface Outbound

Use the following commands to configure alerts related to an outbound N7 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N7 responses received is lesser
threshold."
   exit
exit
```

N7 Interface Inbound

Use the following commands to configure alerts related to an inbound N7 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N7 responses sent is lesser threshold."

   exit
exit
```

N7 Message Timed Out

Use the following commands to configure alerts related to the N7 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN7Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the increase in timeout for N7 messages toward PCF
crosses threshold"
   exit
exit
```

N10 Interface

Use the following commands to configure alerts related to the N10 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N10 responses received is lesser
threshold."
   exit
exit
```

N11 Interface Inbound

Use the following commands to configure alerts related to an inbound N11 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses sent is lesser
threshold."
   exit
exit
```

N11 Interface Outbound

Use the following commands to configure alerts related to an outbound N11 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 60
   rule SMFN11Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N11 responses received is lesser
threshold."
   exit
exit
```

N11 Message Timed Out

Use the following commands to configure alerts related to the N11 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN40Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the increase in timeout for N11 messages toward AMF
crosses threshold"
   exit
exit
```

N40 Interface Inbound

Use the following commands to configure alerts related to an inbound N40 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN40Inbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\", message_direction=\"inbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses sent is lesser
threshold."
   exit
exit
```

N40 Interface Outbound

Use the following commands to configure alerts related to an outbound N40 interface.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN40Outbound
   expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\", message_direction=\"outbound\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N40 responses received is lesser
threshold."
   exit
exit
```

N40 Message Timed Out

Use the following commands to configure alerts related to the N40 Message Timed Out procedure.

```
alerts rules group MessageTimeout
   interval-seconds 300
   rule SMFN11Timeout
   expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired the increase in timeout for N40 messages toward CHF crosses
 threshold"
   exit
exit
```

NRF Discovery

Use the following commands to configure alerts related to the NRF Discovery procedure.

```
alerts rules group NRF
   interval-seconds 300
   rule NRFDiscovery
   expression
"sum(nf_discover_messages_total{result=~\"success|failure\",svc_name=\"nnrf-disc\",
service_name=\"smf-rest-ep\"}) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of N4 responses sent is lesser than 95
 %."
   exit
exit
```

SMF Service Start

Use the following commands to configure alerts related to the SMF Service Start procedure.

```
alerts rules group SMFService
   interval-seconds 300
   rule SMFServiceStart
   expression "irate(outgoing_response_msg_total{msg_type=\"NrfNfmRegistration\"}[5m])"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when SMF-Service starts upon registration with NRF"
   exit
exit
```

IP Pool

This section provides detail of commands that are required to configure alerts related to IP Pool.

IP Pool Used

Use the following commands to configure alerts related to the IP Pool used procedure.

```
alerts rules group IPPool
   interval-seconds 300
   rule IPPool
   expression "sum(IPAM_address_allocations_current) > THRESHOLD"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage IP pool addresses used is above the
threshold"
   exit
exit
```

Message Level Alerts

This section provides detail of commands that are required to configure alerts related to various messages.

N11 SM Create

Use the following commands to configure alerts related to N11 SM Create.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Success
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_create_sm_context responses sent
 is lesser threshold."
   exit
exit
```

N11 SM Update

Use the following commands to configure alerts related to N11 SM Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Update
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
 message_direction=\"inbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_update_sm_context responses sent
 is lesser threshold."
```

```
   exit
exit
```

N11 SM Release

Use the following commands to configure alerts related to N11 SM Release.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11Release
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
 message_direction=\"inbound\", response_status=\"204\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of amf_release_sm_context responses sent
 is lesser threshold.”
   exit
exit
```

N1 N2 Message Transfer

Use the following commands to configure alerts related to N1 N2 Message Transfer.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN1N2Transfer
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
message_direction=\"outbound\", response_status=\"200\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of amf_n1_n2_transfer responses received
 is lesser threshold.”
   exit
exit
```

N11 EBI Assignment

Use the following commands to configure alerts related to N11 EBI Assignment.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11EBI
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\", response_status=\"200\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_assign_ebi responses received is
 lesser threshold.”
```

```
   exit
exit
```

N11 SM Status Notify

Use the following commands to configure alerts related to N11 SM Status Notify.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11StatusNotify
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
message_direction=\"outbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_status_notify responses received
 is lesser threshold.”
   exit
exit
```

N11 SM Context Retrieve

Use the following commands to configure alerts related to N11 SM Context Retrieve.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN11ContextRetrieve
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
 message_direction=\"inbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of amf_retrieve_sm_context responses
sent is lesser threshold.”
   exit
exit
```

N7 SM Policy Create

Use the following commands to configure alerts related to N7 SM Policy Create.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyCreate
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_create responses
```

```
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Update

Use the following commands to configure alerts related to N7 SM Policy Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdate
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_update responses
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Delete

Use the following commands to configure alerts related to N7 SM Policy Delete.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyDelete
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\", response_status=\"204\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_delete responses
 received is lesser threshold."
   exit
exit
```

N7 SM Policy Notify Update

Use the following commands to configure alerts related to N7 SM Policy Notify Update.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyUpdateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update_notify\",
message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
```

```
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of pcf_sm_policy_control_update_notify
 responses sent is lesser threshold."
   exit
exit
```

N7 SM Policy Notify Terminate

Use the following commands to configure alerts related to N7 SM Policy Terminate.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN7PolicyTerminateNotify
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_terminate_notify\",
 message_direction=\"inbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_terminate_notify
 responses sent is lesser threshold."
   exit
exit
```

N10 UE Register

Use the following commands to configure alerts related to N10 UE Register.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10UERegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of register_ue responses received is
lesser threshold."
   exit
exit
```

N10 UE DeRegister

Use the following commands to configure alerts related to N10 UE DeRegister.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10UEDeRegister
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
```

```
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of deregister_ue responses received is
 lesser threshold."
   exit
exit
```

N10 SM Subscription Fetch

Use the following commands to configure alerts related to N10 Subscription Fetch.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionFetch
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of subscription_req responses received
 is lesser threshold."
   exit
exit
```

N10 SM Subscribe for Notification

Use the following commands to configure alerts related to N10 Subscribe for Notification.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10SubscriptionNotification
  expression "sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
 message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when the percentage of sdm_subscription_req responses received
 is lesser threshold."
   exit
exit
```

N10 Charging Data Request

Use the following commands to configure alerts related to N10 Charging Data Request.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingRequest
   expression
"sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
```

```
message_direction=\"outbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of chf_charging_data_request responses
 received is lesser threshold.”
   exit
exit
```

N10 Charging Data Notify

Use the following commands to configure alerts related to N10 Charging Data Notify.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFN10ChargingDataNotify
   expression "sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\", response_status=\"201\”}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\”}[5m])) < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of chf_abort_notify responses sent is
lesser threshold.”
   exit
exit
```

Policy Rule Alerts

This section provides detail of commands that are required to configure alerts related to various policy rules.

Addition of Dynamic PCC Rules

Use the following commands to configure alerts related to addition of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule AddPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"install\”}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"install\”}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful addition of dynamic pcc
rules is lesser threshold.”
   exit
exit
```

Modification of Dynamic PCC Rules

Use the following commands to configure alerts related to modification of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule ModifyPCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"modify\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"modify\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful modification of dynamic
pcc rules is lesser threshold."
   exit
exit
```

Removal of Dynamic PCC Rules

Use the following commands to configure alerts related to removal of dynamic PCC rules.

```
alerts rules group SMFPolicyStatus
   interval-seconds 300
   rule RemovePCCRule
   expression
"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"remove\"}[5m]))
  /
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"remove\"}[5m]))
 < 0.95"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the percentage of successful removal of dynamic pcc
rules is lesser threshold."
   exit
exit
```

SMF Overload/Congestion

This section provides detail of commands that are required to configure alerts related to various SMF Overload/Congestion.

SMF Overload

Use the following commands to configure alerts related to the SMF Overload procedure.

```
alerts rules group SMFSvcStatus
   interval-seconds 300
   rule SMFOverload
   expression "sum by (component) (system_overload_status) == true"
   severity major
   type "Communications Alarm"
   annotation summary
  value "This alert is fired when increase in events not processed due to system overload"

   exit
exit
```

SMF Sessions

This section provides detail of commands that are required to configure alerts related to various SMF sessions.

Session Release Rate

Use the following commands to configure alerts related to the Session Release Rate procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionReleaseRate
  expression "sum(rate(smf_service_stats{procedure_type=~\".*pdu_sess_rel|.*pdn_sess_rel\"
 , status=\"attempted\"}[5m])) >  THRESHOLD "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the session release rate exceeds the threshold"
   exit
exit
```

Session Setup Failure

Use the following commands to configure alerts related to the Session Setup Failure procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionSetupFailure
  expression "sum(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\"
 , status=\"failures\"}) /
sum(smf_service_stats{procedure_type=\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}) >  0.05 "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when failed to setup sessions is more than 5%"
   exit
exit
```

Session Setup Rate

Use the following commands to configure alerts related to the Session Setup Rate procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSessionSetupRate
   expression
"sum(rate(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}[5m]))>  THRESHOLD "
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the session setup rate exceeds the threshold"
   exit
exit
```

Subscriber Limit

Use the following commands to configure alerts related to the Subscriber Limit procedure.

```
alerts rules group SMFSession
   interval-seconds 300
   rule SMFSubscriberLimit
   expression "sum(smf_session_counters{pdu_type=~\"ipv4v6|ipv4|ipv6\"}) > THRESHOLD"
   severity major
   type "Communications Alarm"
   annotation summary
   value "This alert is fired when the max number of subscribers is more
   than the threshold"
   exit
exit
```

Metrics

Feature Description

You can a monitor wide range of application and system statistics, and key performance indicators (KPI) within the SMF infrastructure. KPIs are useful to gain insight into the overall health of the SMF environment. Statistics offer a simplified representation of the SMF configurations and utilization-specific data.

The SMF integrates with Prometheus, a third-party monitoring and alerting solution to capture and preserve the performance data. This data is reported as statistics and can be viewed in the web-based dashboard. Grafana provides a graphical or text-based representation of statistics and counters, which the Prometheus database collects. The Grafana dashboard projects a comprehensive set of quantitative and qualitative data that encourages you to analyze SMF metrics in the reporting tool of your choice and take informed decisions.

By default, the monitoring solution is enabled, which indicates that Prometheus continually monitors your SMF environment and the Prometheus data source is associated with Grafana. You must have the administrative privileges to access Grafana. However, to view a specific dashboard, run the Prometheus queries. The queries are available in the built-in and custom format.

The following snapshot is a sample of the Grafana dashboard.

Figure 278: Grafana Dashboard

How it Works

KPIs constitute of metrics, such as statistics and counters. These metrics represent the performance improvement or degradation. By default, Prometheus is enabled on the system where SMF is deployed, and configured with Grafana. Prometheus dynamically starts monitoring the data sources that are available on the system. For new dashboard panels, execute queries in Prometheus.

For more information about Prometheus, consult the Prometheus documentation at https://prometheus.io/docs/introduction/overview/.

Configuring Metrics Collection

The labels of each SMF metrics are classified into the following three categories:

- Production
- Debug
- Granular

All the SMF application metrics are controlled through the CLI command for performance optimization.

To collect the necessary SMF metrics and labels, use the following sample configuration:

```
config
  infra metrics verbose { service | protocol | load-balancer | application
 } [ level { debug | off | production | trace } | metrics metrics_name [
granular-labels label_name| level { debug | off | production | trace } |
pod pod_name | level { debug | off | production | trace }  ] ]
   end
```

NOTES:

- If the metrics verbosity is not configured, then the default verbosity level for pod type is as follows.
  - LoadBalancer = Production
  - Protocol = Trace
  - Service = Trace
  - Application = Debug
- The order of the level for verbose metrics is in the following priority order:
  - **metrics [[metrics_name] level [production|debug|trace|off]**: [Priority 1]
  - **pod [[pod_Name]] level [production | debug | trace | off]]** [Priority 2]
  - **level [production | debug | trace | off]** [Priority 3]
- **infra metrics verbose { service | protocol | load-balancer | application }**: Enable the metric collection. This configuration helps to collect the required application metrics and labels. By default, this command captures the debug labels of metrics.
- **level { debug | off | production | trace }**: Specify the application metrics category to capture the required application metrics and labels.
  - **debug**: Capture all the labels that are classified as production and debug categories. This option is the default configuration.
  - **off**: Disable the application level metrics collection.

    For example, configuring the **infra metrics verbose application smf_service_stats level off** command disables the smf_service_stats application metrics.
  - **production**: Capture the labels that are classified as production category.
  - **trace**: This option is not supported for SMF application metrics. If this option is configured, the SMF treats this option as **debug**.
- If production and debug classification is empty for a metrics, then all the labels except granular-labels (if configured) are classified as debug.
- **metrics** *metrics_name*: Specify the metrics name to capture only the labels that correspond to the given metrics. The metric-level configuration takes precedence over the application-level configuration. If the metrics level is not configured, the labels are captured at the application level.
- **granular-labels**: Capture only the granular labels. By default, this option is disabled.

  If a granular label is required for KPI, then that label must be configured. For example, to capture dnn labels of smf_service_stats metrics, you must configure the following CLI command:

```
infra metrics verbose application metrics smf_service_stats level debug
 granular-labels [ dnn ]
```

Configuration Example

The following is an example configuration to enable only production level for all the application metrics.

```
infra metrics verbose application level production
```

The following is an example configuration to enable production level for smf_service_stats application metrics and debug level for all other application metrics.

```
infra metrics verbose application smf_service_stats level production
```

The following is an example configuration to enable debug level for smf_service_stats application metrics along with granular labels and production level for all other application metrics.

```
infra metrics verbose application level production smf_service_stats level
 debug granular-labels [ dnn ]
```

The following is an example configuration to enable production level for smf_service_stats application metrics along with granular labels and debug level for all other application metrics.

```
infra metrics verbose application smf_service_stats level production
granular-labels [ dnn ]
```

The following is an example configuration to disable smf_service_stats application metrics and debug level for all other application metrics.

```
infra metrics verbose application smf_service_stats level off
```

The following is an example configuration to configure NSSAI labels of smf_service_stats metrics.

```
infra metrics verbose application metrics smf_service_stats level debug
granular-labels [ snssai ]
```

Note The NSSAI statistics are not pegged without configuring the NSSAI label in the granular-labels configuration.

Configuration Verification

To verify the configuration, use the following show command:

```
show running-config infra metrics verbose application
```

The following are example outputs of the **show running-config infra metrics verbose application** command.

```
[smf] smf# show running-config infra metrics verbose application
infra metrics verbose application
 metrics smf_service_stats
  level production
  granular-labels [ dnn ]
 exit
exit
```

The preceding output indicates that the configuration to capture production labels for smf_service_stats application metrics along with granular labels and debug levels of all other application metrics is enabled.

```
[smf] smf# show running-config infra metrics verbose application
 infra metrics verbose application
  level production
  metrics smf_service_stats
   level debug
   granular-labels [ [dnn] ]
  exit
exit
```

The preceding output indicates that the configuration to capture debug labels for smf_service_stats application metrics along with granular labels and production level of all other application metrics is enabled.

To verify the slice information on procedure and session statistics, use the following show command:

```
show running-config infra metrics verbose application
infra metrics verbose application
 metrics smf_service_stats
  level debug
  granular-labels [ snssai ]
 exit
```

Bulk Statistics and Key Performance Indicators

Feature Description

This section provides details of bulk statistics, and Key Performance Indicators (KPIs) used for performance analysis on SMF.

There are two types of bulk statistics:

- Gauge - A snapshot value that shows the statistic at that reporting moment (for example, the number of current PDP contexts, simultaneous Active EPS Bearers). Gauge statistics can increment or decrement continuously.
- Counter - A historic value that shows the statistic that accumulated over time (for example, the total number of CSR requests received). Counter values can only increment except in two cases:
  - Rollover - where a counter exceeds its maximum value and rolls over to zero.
  - Reset - where a counter is manually reset to zero.

Important For the complete list of supported bulk statistics and KPIs, see the *UCC 5G SMF Metrics Reference* applicable for this release.

Logs

Feature Description

The system logging feature provides a common way to log the log messages across applications. Each log consists of the following components:

- Timestamp—Shows the date and time of the log creation.
- Log message—Shows the message of a specific log.
- Log level—Shows the level of importance of log message.
- Log tag—Shows the details of module name, component name, and interface name. A log tag is pre-created and passes during logging.

SMF provides various types of logging to log the messages. These logging types are application logging, transaction logging, monitor subscriber logging, and trace logging.

The SMF maintains various logs, such as trace logs and event logs. Use the **kubectl get pods -n** *namespace* CLI command to check all the pods and the services that are currently running. Then, use the **kubectl logs** *podname* **-n** *namespace* CLI command to display the log in a pod.

If you encounter any error during the operation of this feature, use the SMF service logs for a particular subscriber session to identify the issues and determine the solution to your problem.

Download OAM and EDR Monitor Pod Files

Feature Description

Files that are generated using the **monitor subscriber** command, **monitor protocol** command, and transaction logs are stored in the OAM pod. The files that are generated in OAM pod are collected and stored in an internal Apache server. You can view and download the files by using a web browser, after user authentication.

Note Use the same credentials as ops-center to authenticate user access to the files present in the oam-pod and edr-monitor pod using a browser.

The files are created in separate folders, as and when their respective commands are executed. You can download the following OAM and EDR pod files:

- **Monitor subscriber files**: These files are generated using the **monitor subscriber** CLI option to trace messages that are related to a specified subscriber. The files that are generated for the **monitor protocol** command are present in the `monsublogs/` directory.
- **Monitor protocol files**: These files are using the **monitor protocol** CLI option to capture packets on a specific interface provided under the CLI command. The files that are generated for the **monitor protocol** command are present in `monprologs/` directory.
- **Transaction logs**: When transaction logging is enabled, the transaction logs are sent to oam-pod and can be downloaded from there. The files generated for transaction logging when enabled and are present in the `transactionlogs/` directory.
- **EDR files**: These files are generated in smf service pod and periodically copied to edr-monitor pod. The files are available in /edr directory.

How it Works

This section describes how to view and download the log files in the oam-pod and edr-monitor pod.

Downloading OAM Pod Files

Open a browser and log on to the Apache server using the *https://oam-files.<ReleaseName>.<Ingress-host-name>.nip.io/* URL. Use the ops-center user credentials. Replace <*ReleaseName*> and <*Ingress-host-name*> with the release name and ingress host name respectively.

The oam-pod directory comprises folders to archive the monitor protocol logs, monitor subscriber logs, and transaction logs.

The directory folders are visible as per the commands executed.

To download the monitor protocol files, use the following URL:

https://oam-files.<ReleaseName>.<Ingress-host-name>.nip.io/ monprologs/

In the preceding URL, replace monprologs with monsublogs for monitor subscriber files and with transactionlogs for the transaction log files.

Downloading EDR Files

To access the EDR files in the persistent volume of EDR monitor pod, log on to the Ops center with required credentials, and use the edr-monitor pod ingress URL.

To determine the ingress URL, use the following command:

kubectl get ingress -n *namespace* **| grep edr**

Example:

cloud-user@svi-cndp-tb41-gr-setup-smf-cluster-2-cndp-server-1:~$ **kubectl get ingress -n smf-smf | grep edr**

Configuring the Logs

This section describes how to configure the logs.

Enabling or Disabling the Transaction Messages

To enable or disable the presence of request response messages in the transaction logs, use the following sample configuration:

```
config
  logging transaction message { disable | enable }
  commit
end
```

NOTES:

- **logging transaction message { disable | enable }**: Specify whether to enable or disable messages in transaction logging.

Viewing Transaction History Logs

To view the transaction history on an OAM pod shell, use the following CLI command in the SMF Ops Center:

```
dump transactionhistory
```

Note The most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

To display the logs in a pod, use the following command on the Kubernetes master node:

kubectl logs -n *<SMF namespace> podname*

Sample Transaction Log

The following is an example of transaction log collected in Monitor Subscriber during SMF PDU session establishment.

```
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
************* TRANSACTION: 00010 *************
TRANSACTION SUCCESS:
    Txn Type             : N10RegistrationRequest(33)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Processing transaction Id: 10
 Type: 33 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.346 [TRACE] [infra.message_log.core] >>>>>>>
IPC message
Name: N10RegistrationRequest
MessageType: N10RegistrationRequest
Key:
--body--
{"regInfo":{"ueId":"imsi-123456789012345","pduSessionId":5},"regReq":{"dnn":"intershat",

"pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123","plmnId":{"mcc":"123","mnc":"456"},


"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2}},


"msgReq":{"Type":2,"ServiceName":4,"Versions":["v1"],"ProfileName":"UP1","FailureProfile":"FH1","SvcMsgType":3,

  "Filter":{"Bitmapfeilds":2,"Dnn":"intershat"}}}
   2020/03/03 05:31:39.346 [DEBUG] [nrfClient.Discovery.nrf] Message send Metadata [Type:UDM
 ServiceName:nudm-uecm
      ..
      ..
Request
Name: UdmRegistrationRequest
Host:
http://209.165.200.229:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Method: PUT
RequestURI:
--- Headers ---
Content-Type: application/json
Body:{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},
"singleNssai":{"sd":"Abf123","sst":2},"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0"}

    2020/03/03 05:31:39.376 [TRACE] [infra.message_log.core] >>>>>>>
Response
Name:
Response Status 201
--- Headers ---
Location:
http://209.165.200.229:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Content-Length: 225
Content-Type: application/json
Body:{"pgwFqdn": "cisco.com.apn.epc.mnc456.mcc123", "plmnId": {"mcc": "123", "mnc": "456"},
 "dnn": "intershat",
  "smfInstanceId": "524f5f8a-b584-47b8-86f5-a5292eabcdef", "pduSessionId": 5, "singleNssai":
 {"sd": "Abf123", "sst": 2}}
    ..
    ..
    ..
--body--
{"regRes":{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},
  ..
  ..
```

```
*********************************************
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
************* TRANSACTION: 00011 *************
TRANSACTION SUCCESS:
    Txn Type             : N10SubscriptionFetchReq(36)
    Priority             : 1
    Session State        : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Processing transaction Id: 11
 Type: 36 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.384 [TRACE] [infra.message_log.core] >>>>>>>
IPC message
Name: N10SubscriptionFetchReq
MessageType: N10SubscriptionFetchReq
Key:
--body--
  ..
  ..
Request
Name: UdmSubscriptionRequest
Host:
http://209.165.200.229:9020/nudm-sdm/v1/imsi-123456789012345/sm-data?dnn=intershat&plmn-id=%7B%22mcc%22%3A%22123%22%2C%22mnc%22%3A%2

   2456%22%7D&single-nssai=%7B%22sd%22%3A%22Abf123%22%2C%22sst%22%3A2%7D&supported-features=0
Method: GET
RequestURI:
--- Headers ---
IPC message
Name: N10SubscriptionFetchSuccess
MessageType: N10SubscriptionFetchSuccess
Key:
  ..
  ..
--body--
  ..
  ..
```

Configuring the Logging Levels

This section describes how to configure the logging level parameters.

Use the following sample configuration to configure the logging level:

```
config
  logging level { application | monitor-subscriber | tracing |transaction
 }
  end
```

NOTES:

- **logging level { application | monitor-subscriber | tracing | transaction }**– Enter the transaction log configuration mode.
  - **application** – Configures the option application logging level.
  - **monitor-subscriber** – Configures the option monitor subscriber logging level.
  - **tracing** – Configures the option logging level tracing
  - **transaction** – Configures the option transaction logging level.

Configuring Persistent Transaction Logs

This section describes how to configure the persistent transaction log parameters.

The transaction logs are saved in the transaction log file that resides in the transaction logs directory of OAM pod.

Use the following sample configuration to configure the persistent transaction logs:

```
config
  logging transaction persist enable { max-file-size | max-rotation }
  end
```

NOTES:

- **logging transaction**– Enter the transaction log configuration mode.
- **persist enable { max-file-size | max-rotation }** – Configure the option to enable writing of transaction logs to the transaction log file.
  - **max-file-size** *max_filesize*– Specify the maximum size (in MB) of the transaction logs that must be preserved in the file. The default size is 50 MB. The accepted range is 1-10000 MB.
  - **max-rotation** *max_rotation*– Specify the maximum number of files that must be stored in the folder. After reaching the specified number, the file rotation begins. With this rotation, the oldest file is deleted and the latest log file is added to the folder. For example, if the folder has files a1.txt–a.10.txt and when the a.11.txt is added, then a1.txt is deleted. The default number is 10. The accepted range is 2 -1000.
- **persist enable** – Disables writing of transaction logs to the transaction log file.

Viewing Persistent Transaction Logs

This section describes how to view the transaction logs that are stored on the OAM pod.

To view the persistent transaction logs, use the following configuration through the SMF Ops Center:

transaction file dump filename *file_path*

You can use the **transaction log list** command to view the list of log files and their paths.

The following is a sample output of the transaction logs:

```
RELEASE_NAMESPACE: 'example-data'
Dumping file 'transactionlogs/transaction.log.20200907033433.4.gz'
InstanceInfo: example.example-rest-ep.cluster1.example-data.1
TimeStamp: 2020-09-09 00:25:18.379439773 +0000 UTC
************* TRANSACTION: 01371 *************
TRANSACTION SUCCESS:
    Txn Type             : MessageTypeExampleCreate(1)
    Priority             : 1
    Session Namespace    : none(0)
LOG MESSAGES:
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Message Example_Create decod
ed
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process init
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] Config from GetConfig is Ve
rsion: 783da2fc038c6bc961a95e2bf3dd6d93f282e36b30e0362698a1de369a2fd15c Services
: [Name: restServer Type: Rest Endpoint: sbi Name: tcpServer Type: Tcp Endpoint:
 tcp-protocol Name: udpServer Type: Udp Endpoint: udp-protocol]
    2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process continue
```

```
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] DerivedConfig from GetConfi
g is DerivedNameToBeTested_cb3383b95927a434d42cd9d5687ccf1b13e2de4b2faf4543287a3
4afb32518fe
    2020/09/09 00:25:18.339 [DEBUG] [rest_ep.udp.n5] Sending message Example_Cre
ate to example-service
    2020/09/09 00:25:18.342 [INFO] [infra.transaction.core] Calling RPC example-
service_ipc_stream on host example-service_1 proc-name example-service_ipc_strea
```

Dispatcher

Feature Description

Dispatcher is an ingress throttling configuration of rate of admission with number of queues and size of queue configuration at GTP and PFCP.

Configuration Limit for Dispatcher on S11 Interface

When impacted, an IMS bearer results in voice call failures due to S11 interface and GTPv2 message drops at the ingress protocol dispatcher.

The S11 protocol dispatcher configuration at cnSGW is static and requires tuning based on the production requirements. If the configuration isn't appropriate for the MME pool that is being served, then in the case of high call events per seconds (CEPS), the GTPv2 message drops.

Any GTPv2 -S11 is discarded or dropped due to dispatcher queue limits at the ingress, which includes request or response messages, such as Release Access Bearer (RAB), Modify Bearer Request (MBR), and DDN Acknowledgment. For example, a drop in MBR from MME with an existing voice bearer results in a call drop. A drop of MBR from MME with a voice bearer transfer as part of EPS Fallback (EPSFB) results in an EPSFB call setup failure (Voice Access Failure Rate (AFR)).

Configuring Dispatcher for S11 Interface

To configure a dispatcher for S11 interface, use the following sample configuration:

```
config
  interface interface_name
    sla response response_time_value
    dispatcher
      count count_value
      capacity capacity_value
      outbound [ true | false ]
      cache [ true | false ]
      threshold threshold_value
      expiry expiry_time_value
      nonresponsive nonresponsive_time_value
   exit
```

NOTES:

- **interface** *interface_name*: Specify the interface name as S11.
- **sla response** *response_time_value*: Specify the SLA response time. *response_time_value* must be an integer.

- **count** *count_value*: Specify the count of dispatcher queues.
- **capacity** *capacity_value*: Specify the capacity of each dispatcher queue.
- **outbound [true | false]**: Specify this value to enable or disable the queue support for the outbound messages.
- **cache [true | false]**: Specify this value to enable or disable the retransmission of cache.
- **threshold** *threshold_value*: Specify the threshold value for the outstanding requests per queue cache.
- **expiry** *expiry_time_value*: Specify the responded cache entry expiry duration in milliseconds.
- **nonresponsive** *nonresponsive_time_value*: Specify this value for the non-responsive cache entry expiry duration in milliseconds.

Configuration Example

The following is an example configuration of dispatcher for S11 interface.

```
interface s11
   sla response 5500
   dispatcher
    count         10
    capacity      100000
    outbound      true
    threshold     160000
    expiry        7000
    nonresponsive 6000
   exit
```

OAM Support

This section details the metrics supported for the dispatcher.

Metrics

Following new metrics is introduced to capture the specific event when the dispatcher queue is configured:

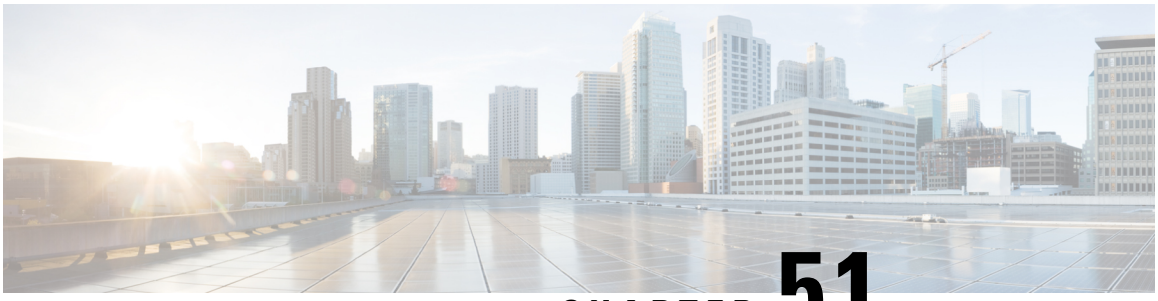
Metric Name: outgoing_drop_queued_total

Description: The metric captures the specific event when the dispatcher queue configured at the UDP client is full and is loaded with too many messages beyond the configured queue capacity

Following labels are added in this metric:

- **local_address:** Local UDP address where the UDP endpoint is started.
- **interface:** Name of the UDP interface configured in the endpoint configuration.
- **protocol:** Name of the protocol configured in the endpoint configuration. For example, UDP
- **queue_id:** Queue index number based on the source IP address.
- **peer_address:** IP address of the peer endpoint.
- **cause:** The reason for the drop of message from the queue. For example, one of the reasons is dispatcher queue being full.

- **queue_type:** Type of queue configured in the dispatcher configuration.



CHAPTER 51

Sample SMF Configuration

- Sample Configuration, on page 1631

Sample Configuration

The following is only a sample configuration file provided solely for your reference. You must create and modify your own configuration file according to the specific needs of your deployment.

```
profile compliance comp1
 service nsmf-pdusession
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service namf-comm
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service n1
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service n2
  version uri v1
  version full 1.0.0
  version spec 15.4.0
 exit
 service nudm-sdm
  version uri v2
  version full 2.0.1
  version spec 15.4.0
 exit
 service nudm-uecm
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service nnrf-disc
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service nnrf-nfm
```

```
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service npcf-smpolicycontrol
  version uri v1
  version full 1.0.2
  version spec 15.4.0
 exit
 service nchf-convergedcharging
  version uri v2
  version full 2.0.1
  version spec 15.3.0
 exit
exit
profile network-element amf amf1
 nf-client-profile        AP1
 failure-handling-profile FH3
 query-params [ dnn target-nf-instance-id ]
exit
profile network-element udm udm1
 nf-client-profile        UP1
 failure-handling-profile FH1
 query-params [ target-plmn target-nf-instance-id ]
 query-target-plmn        primary
exit
profile network-element pcf pcf1
 nf-client-profile        PP1
 failure-handling-profile FH1
 query-params [ dnn target-plmn target-nf-instance-id requester-snssais ]
 rulebase-prefix          cbn#
 predefined-rule-prefix   crn#
 use-amf-provided-pcf     true
exit
profile network-element chf chf1
 nf-client-profile                CP1
 failure-handling-profile         FH2
 query-params [ dnn target-plmn chf-supported-plmn ]
 query-target-plmn                primary
 nf-client-profile-offline        CP2
 failure-handling-profile-offline FH2
exit
profile network-element chf chgser1
exit
profile network-element sepp sepp1
 nf-client-profile hsepp
exit
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.231
 n4-peer-port      8805
 upf-group-profile upfGroup1
 dnn-list          [ cisco intershat starent ]
 capacity          65535
 priority          1
exit
profile network-element upf upf2
 n4-peer-address ipv4 209.165.200.232
 n4-peer-port 8805
 dnn-list     [ cisco intershat starent ]
 capacity     65535
 priority     2
exit
profile network-element upf upf3
 node-id      toolsUPF
```

```
 n4-peer-address ipv4 209.165.200.233
 n4-peer-port 8805
 dnn-list     [ cisco intershat starent ]
 capacity     32768
 priority     10
exit
profile upf-group upfGroup1
 heartbeat
  interval               63
  retransmission-timeout 3
  max-retransmissions    5
 exit
 supported-features [ secondary-pdr ]
exit
profile wps wps1
 arp              1-15
 dscp n3 0x14
 dscp sxa 0x22
 dscp s5e 0x24
 dscp s11 0x26
 message-priority [ pfcp gtpc ]
exit
profile wps wps_F5972
 arp              1-4,14
 dscp n3 0x0F
 message-priority [ pfcp gtpc ]
exit
profile pcscf pcscf1
 v4-list
  precedence 3
   primary 209.165.201.1
   secondary 209.165.201.2
  exit
 exit
 v6-list
  precedence 3
   primary 33:33::1
   secondary 33:33::2
  exit
 exit
 v4v6-list
  precedence 3
   primary ipv4 209.165.200.225
   primary ipv6 fd01:976a:c305:9::5
   secondary ipv4 209.165.200.26
   secondary ipv6 46:46:33::2
  exit
 exit
exit
profile icmpv6 icmpprf1
 options virtual-mac b6:6d:57:45:45:45
exit
profile charging chgprf1
 method                  [ offline ]
 limit volume 10000000
 limit duration 7200
 accounting limit volume downlink 100000 total 100000 uplink 100000
 accounting triggers [ qos-change rat-change serv-node-change ambr-change ue-time-change
plmn-change user-loc-change ]
 tight-interworking-mode true
 quota request always
 quota suppress triggers [ qht ]
 reporting-level online rating-group
 reporting-level offline service-id
```

```
exit
profile charging chgprf2
 method                  [ offline ]
 accounting limit volume downlink 100000 total 100000 uplink 100000
 accounting triggers [ qos-change rat-change serv-node-change ambr-change ue-time-change
plmn-change user-loc-change ]
 tight-interworking-mode true
 quota request always
 quota suppress triggers [ qht ]
 reporting-level online rating-group
 reporting-level offline service-id
exit
profile charging chgprf3_roaming
 method [ offline ]
exit
profile charging-characteristics 1
 charging-profile     chgprf2
 charging-qbc-profile qbc_general
exit
profile charging-qbc qbc_general
 limit volume 20500
 limit duration 70
 max-charging-condition 1
 max-deferred-urr       2
 triggers               [ ambr-change qos-change user-loc-change ]
exit
profile charging-qbc qbc_hsmf1
 limit volume 40500
 limit duration 140
 triggers [ ambr-change qos-change serv-node-change user-loc-change ]
exit
profile failure-handling FH1
 interface pfcp
  message N4SessionEstablishmentReq
   cause-code pfcp-entity-in-congestion action retry-terminate max-retry 2
   cause-code system-failure action terminate
   cause-code service-not-supported action terminate
   cause-code no-resource-available action retry-terminate max-retry 3
   cause-code no-response-received action retry-terminate max-retry 1
   cause-code reject action terminate
  exit
  message N4SessionModificationReq
   cause-code mandatory-ie-incorrect action terminate
   cause-code session-ctx-not-found action terminate
   cause-code reject action terminate
  exit
 exit
 interface sxa
  message SessionEstablishmentReq
   cause-code 2-255 action retry-terminate max-retry 4
  exit
 exit
exit
profile failure-handling gtp1
 interface gtpc message S5S8CreateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
 interface gtpc message S5S8UpdateBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
```

```
 interface gtpc message S5S8DeleteBearerReq
  cause-code temp-fail
   action retry timeout 1000 max-retry 2
  exit
 exit
exit
profile access access1
 n26 idft enable timeout 15
 n2 idft enable timeout 15
 gtpc gtpc-failure-profile gtp1
 erir delay 1
 eps-fallback cbr delay 3000 max-retry 1 timeout 1
exit
profile access idft
 n1 t3591-pdu-mod-cmd timeout 2 max-retry 1
 n1 t3592-pdu-rel-cmd timeout 2 max-retry 1
 n26 idft enable timeout 15
 n2 idft enable timeout 15
 erir delay 2000
exit
profile tai-group TA1
 mcc 123 mnc 456
  tac list [ 00092a 2346 2356 ]
 exit
 mcc 310 mnc 260
  tac list [ 00092a 2346 2356 ]
  tac range start 1234 end 7890
  exit
 exit
 mcc 310 mnc 310
  tac list [ 2346 2356 2378 ]
  tac range start 5676 end 5767
  exit
 exit
exit
profile tai-group TA2
 mcc 310 mnc 260
  tac list [ 2346 5676 ]
 exit
exit
profile tai-group tgp2
 mcc 091 mnc 05
 exit
exit
profile ecgi-group ECGI1
 mcc 122 mnc 234
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 123 mnc 456
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 310 mnc 260
  ecgi range start 1234567 end 1234577
  exit
 exit
 mcc 310 mnc 310
 exit
exit
profile ecgi-group ECGI2
exit
profile ncgi-group NCGI1
 mcc 123 mnc 456
```

```
  ncgi range start 123456788 end 133456789
  exit
 exit
 mcc 310 mnc 260
  ncgi list [ 123456789 ]
  ncgi range start 123456788 end 234567891
  exit
 exit
 mcc 310 mnc 310
  ncgi list [ 123456789 133456789 ]
  ncgi range start 234567891 end 244567891
  exit
 exit
exit
profile ncgi-group NCGI2
 mcc 123 mnc 456
  ncgi range start 123456789 end 133456789
  exit
  ncgi range start 234567891 end 244567891
  exit
 exit
 mcc 310 mnc 260
  ncgi range start 123456789 end 133456789
  exit
 exit
exit
profile location-area-group loc1
 tai-group  TA1
 ecgi-group ECGI1
 ncgi-group NCGI1
exit
profile location-area-group loc2
 tai-group  TA2
 ncgi-group NCGI1
exit
profile radius
 deadtime           2
 detect-dead-server response-timeout 2
 max-retry          2
 timeout            2
 enable-packet-dump
 server 209.165.200.248 1812
  type     auth
  secret   $8$j1Tgf1IvRvdywBgDZsP7q7FPzo87+/c1QV99bLxz6AY=
  priority 1
 exit
 server 209.165.200.248 1813
  type     acct
  secret   $8$bANgMCn/x7CspByC/q5Jm1sMo5d9TZMKdTbEq7543wc=
  priority 10
 exit
 attribute
  nas-identifier CISCO-SMF
 exit
 accounting
  algorithm first-server
  max-retry 3
  timeout   1
  attribute
   nas-identifier CISCO-ACCT-SMF
  exit
 exit
 server-group sg1
  server auth 209.165.200.248 1812
```

```
  exit
  server acct 209.165.200.248 1813
  exit
  attribute
   nas-ip 209.165.200.226
  exit
  accounting
   attribute
    nas-ip 209.165.200.226
   exit
  exit
 exit
exit
profile radius-dynamic-author
 client 209.165.200.248
  secret $8$G7fLQoqcBFPFpZNstAQUT/VtoxHqGqwPdLNB1PliHOI=
 exit
exit
profile dnn cisco
 dns primary ipv4 209.165.200.239
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 network-element-profiles sepp sepp1
 dnn cisco network-function-list [ upf upf2 ]
 dnn rmgr cisco
 timeout absolute 360000 up-idle 900 cp-idle 1500
 charging-profile           chgprf1
 charging-qbc-profile       qbc_hsmf1
 virtual-mac                b6:6d:47:47:47:47
 pcscf-profile              pcscf1
 wps-profile                wps1
 ssc-mode 1 allowed [ 3 ]
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn cisco
 qos-profile                qos_nonStdQci
 authentication secondary radius group sg1
 authentication algorithm pap 1 password-use-pco chap 2 convert-to-mschap mschap 3
 always-on                  false
 userplane-inactivity-timer 300
 only-nr-capable-ue         true
exit
profile dnn intershat
 dns primary ipv4 209.165.200.239
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 network-element-profiles sepp sepp1
 timeout absolute 360000 up-idle 900 cp-idle 1500
 charging-profile           chgprf1
 charging-qbc-profile       qbc_hsmf1
 virtual-mac                b6:6d:47:47:47:47
 nexthop-forwarding-address ipv4 209.165.200.254
 nexthop-forwarding-address ipv6 8454:8454::8454
 pcscf-profile              pcscf1
 wps-profile                wps1
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
```

```
 qos-profile                qos_nonStdQci
 authentication secondary radius group sg1
 authentication algorithm pap 1 password-use-pco chap 2 convert-to-mschap mschap 3
 always-on                  false
 dcnr                       true
 userplane-inactivity-timer 1800
 only-nr-capable-ue         true
 emergency                  false
exit
profile dnn sos
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 virtual-mac b6:6d:47:47:47:47
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 authorization local
 emergency   true
exit
profile dnn starent
 dns primary ipv4 209.165.200.226
 dns primary ipv6 2001:4870:e00b:1a::3
 dns secondary ipv6 2001:4870:e00b:1a::5
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
 network-element-profiles udm udm1
 dnn cisco network-function-list [ upf upf2 ]
 timeout absolute 360000 up-idle 60 cp-idle 600
 charging-profile           chgprf1
 virtual-mac                b6:6d:47:47:47:47
 pcscf-profile              pcscf1
 wps-profile                wps2
 ssc-mode 1
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 qos-profile                qos_F5972
 always-on                  false
 userplane-inactivity-timer 300
 only-nr-capable-ue         true
 emergency                  false
exit
profile sgw-qos-profile sgw-non-standardqci
 dscp-map operator-defined-qci 128 non-gbr arp-priority-level 5 uplink user-datagram
dscp-marking 0x1e
 dscp-map operator-defined-qci 128 non-gbr arp-priority-level 5 downlink user-datagram
dscp-marking 0x22 encaps-header copy-inner
exit
profile qos 5qi-to-dscp-mapping-table
 dscp-map qi5 1 uplink user-datagram dscp-marking 0x2D
 dscp-map qi5 1 downlink encsp-header dscp-marking 0x2F
 dscp-map qi5 3 uplink user-datagram dscp-marking 0x0c
 dscp-map qi5 3 downlink encsp-header dscp-marking 0x0c
 dscp-map qi5 5 uplink user-datagram dscp-marking 0x3D
 dscp-map qi5 5 downlink encsp-header dscp-marking 0x3F
 dscp-map qi5 6 uplink user-datagram dscp-marking 0x0c
 dscp-map qi5 6 downlink encsp-header dscp-marking 0x0c
 dscp-map qi5 7 uplink user-datagram dscp-marking 0x0e
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x0e
 dscp-map qi5 8 uplink user-datagram dscp-marking 0x0e
 dscp-map qi5 8 downlink encsp-header dscp-marking 0x0e
 dscp-map qi5 9 uplink user-datagram dscp-marking 0x0a
 dscp-map qi5 9 downlink encsp-header dscp-marking 0x0a
```

```
 dscp-map qi5 43 uplink user-datagram dscp-marking 0x1D
 dscp-map qi5 43 downlink encsp-header dscp-marking 0x1F
exit
profile qos abc
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
 qi5      7
 arp priority-level 14
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 priority 120
 max data-burst 2000
 dscp-map qi5 1 arp-priority-level 12 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 1 arp-priority-level 12 downlink user-datagram dscp-marking 0x12 encsp-header
 copy-inner
 dscp-map qi5 1 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 1 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 2 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 2 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 3 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 3 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 4 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 4 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 5 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 5 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 6 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 6 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 7 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 7 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 8 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 8 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 9 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 9 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 65 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 65 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 66 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 66 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 69 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 69 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 70 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 70 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 80 uplink user-datagram dscp-marking 0x2e
 dscp-map qi5 80 downlink user-datagram dscp-marking 0x12 encsp-header copy-inner
 dscp-map qi5 82 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 82 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
 dscp-map qi5 83 uplink user-datagram dscp-marking 0x3f
 dscp-map qi5 83 downlink user-datagram dscp-marking 0x2a encsp-header dscp-marking 0x0a
exit
profile qos qos1
 qi5      128
 arp priority-level 8
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln NOT_PREEMPTABLE
 priority 9
 max data-burst 2048
exit
profile qos qos_F5972
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
exit
profile qos qos_nonStdQci
 ambr ul "250 Kbps"
 ambr dl "500 Kbps"
```

```
 qi5 128
 arp priority-level 12
 arp preempt-cap NOT_PREEMPT
 arp preempt-vuln PREEMPTABLE
 dscp-map qi5 1 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 1 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 2 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 2 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 3 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 3 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 6 downlink encsp-header copy-inner
 dscp-map qi5 7 downlink encsp-header dscp-marking 0x01
 dscp-map qi5 15 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 15 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 65 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 65 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 70 arp-priority-level 12 uplink user-datagram dscp-marking 0x2f
 dscp-map qi5 70 arp-priority-level 12 downlink user-datagram dscp-marking 0x14 encsp-header
 copy-inner
 dscp-map qi5 80 downlink encsp-header copy-inner
 dscp-map qi5 81 downlink encsp-header copy-inner
 dscp-map qi5 83 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 83 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 85 downlink encsp-header dscp-marking 0x01
 dscp-map qi5 128 arp-priority-level 5 uplink user-datagram dscp-marking 0x1e
 dscp-map qi5 128 arp-priority-level 5 downlink user-datagram dscp-marking 0x22 encsp-header
 copy-inner
 dscp-map qi5 230 arp-priority-level 6 uplink user-datagram dscp-marking 0x3e
 dscp-map qi5 230 arp-priority-level 6 downlink user-datagram dscp-marking 0x23 encsp-header
 copy-inner
 dscp-map qi5 254 downlink encsp-header dscp-marking 0x01
exit
profile ppd ppd1
 fqi 1,10-15,43,65
 dscp 0 ppi 3
 dscp 1 ppi 2
 dscp 43 ppi 3
exit
profile nf-client nf-type udm
 udm-profile UP1
  locality LOC1
   priority 30
   service name type nudm-sdm
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9001
     exit
    exit
   exit
   service name type nudm-uecm
    endpoint-profile EP1
```

```
      capacity   30
      uri-scheme http
      endpoint-name EP1
       primary ip-address ipv4 209.165.200.248
       primary ip-address port 9001
      exit
     exit
    exit
    service name type nudm-ee
     endpoint-profile EP1
      capacity       30
      api-uri-prefix PREFIX
      api-root       ROOT
      uri-scheme     http
      endpoint-name EP1
       priority 56
       primary ip-address ipv4 209.165.200.248
       primary ip-address port 9001
      exit
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type pcf
 pcf-profile PP1
  locality LOC1
   priority 30
   service name type npcf-smpolicycontrol
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 100
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9003
     exit
     endpoint-name realPCF
      priority 50
      primary ip-address ipv4 209.165.200.226
      primary ip-address port 9082
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type amf
 amf-profile AP1
  locality LOC1
   priority 30
   service name type namf-comm
    endpoint-profile EP2
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9002
     exit
     endpoint-name realAMF
      priority 100
      primary ip-address ipv4 209.165.202.138
      primary ip-address port 8090
```

```
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type chf
 chf-profile CP1
  locality LOC1
   priority 30
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 100
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9004
     exit
    exit
   exit
  exit
 exit
 chf-profile CP2
  locality LOC1
   priority 31
   service name type nchf-convergedcharging
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     version
      uri-version v2
      exit
     exit
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.248
      primary ip-address port 9005
     exit
    exit
   exit
  exit
 exit
exit
profile nf-client nf-type sepp
 sepp-profile hsepp
  locality LOC1
   priority 30
   service name type nsmf-pdusession
    endpoint-profile EP1
     capacity   30
     uri-scheme http
     endpoint-name EP1
      priority 56
      primary ip-address ipv4 209.165.200.250
      primary ip-address port 8090
     exit
     endpoint-name lfs-hsepp
      priority 10
      primary ip-address ipv4 209.165.200.248
```

```
      primary ip-address port 8888
      secondary ip-address ipv4 209.165.200.249
      secondary ip-address port 8889
     exit
    exit
   exit
  exit
 exit
exit
profile nf-pair nf-type UDM
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true timeout 20000
exit
profile nf-pair nf-type AMF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type PCF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type SEPP
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type UPF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
exit
profile nf-pair nf-type CHF
 nrf-discovery-group DISC1
 locality client  LOC1
 locality preferred-server LOC1
 locality geo-server GEO
 cache invalidation true timeout 20000
exit
profile nf-client-failure nf-type udm
 profile failure-handling FH1
  service name type nudm-sdm
   message type UdmSdmGetUESMSubscriptionData
    status-code httpv2 504
     retry  1
     action continue
    exit
   exit
   message type UdmSdmSubscribeToNotification
    status-code httpv2 504
     retry  1
     action continue
    exit
   exit
   message type UdmSubscriptionReq
    status-code httpv2 504
```

```
      retry  1
      action continue
     exit
    exit
   exit
   service name type nudm-uecm
    message type UdmUecmRegisterSMF
     status-code httpv2 504
      retry  1
      action continue
     exit
    exit
    message type UdmUecmUnregisterSMF
     status-code httpv2 504
      action continue
     exit
    exit
    message type UdmRegistrationReq
     status-code httpv2 504
      action continue
     exit
    exit
   exit
  exit
 exit
profile nf-client-failure nf-type pcf
 profile failure-handling FH1
  service name type npcf-smpolicycontrol
   responsetimeout 4000
   message type PcfSmpolicycontrolCreate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400,504
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
     action retry-and-continue
    exit
   exit
   message type PcfSmpolicycontrolUpdate
    status-code httpv2 0,403
     action retry-and-ignore
    exit
    status-code httpv2 400,504
     action continue
    exit
    status-code httpv2 404
     action terminate
    exit
    status-code httpv2 500
     retry  2
     action retry-and-ignore
    exit
    status-code httpv2 503
     retry  2
```

```
      action retry-and-continue
     exit
    exit
    message type PcfSmpolicycontrolDelete
     status-code httpv2 0,403
      action retry-and-ignore
     exit
     status-code httpv2 400
      action continue
     exit
     status-code httpv2 404
      action terminate
     exit
     status-code httpv2 500
      retry  2
      action retry-and-ignore
     exit
     status-code httpv2 503
      retry  2
      action retry-and-continue
     exit
    exit
   exit
  exit
 exit
profile nf-client-failure nf-type chf
 profile failure-handling FH2
  service name type nchf-convergedcharging
   message type ChfConvergedchargingCreate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type ChfConvergedchargingUpdate
    status-code httpv2 0,500,504
     action continue
    exit
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
   message type ChfConvergedchargingDelete
    status-code httpv2 0,500,504
     action continue
    exit
```

```
    status-code httpv2 400,404
     retry  3
     action retry-and-terminate
    exit
    status-code httpv2 403
     retry  3
     action retry-and-ignore
    exit
    status-code httpv2 503
     action terminate
    exit
   exit
  exit
 exit
exit
profile nf-client-failure nf-type sepp
 profile failure-handling sepp
  service name type nsmf-pdusession
   responsetimeout 4000
   message type VsmfPduSessionCreate
    status-code httpv2 0
     retry  5
     action retry-and-terminate
    exit
    status-code httpv2 504
     retry  3
     action retry-and-terminate
    exit
   exit
   message type VsmfPduSessionUpdate
    status-code httpv2 0,401,404,503-504
     action retry-and-continue
    exit
    status-code httpv2 400
     action terminate
    exit
   exit
   message type VsmfPduSessionRelease
    status-code httpv2 0,504
     action retry-and-terminate
    exit
   exit
  exit
 exit
exit
profile smf smf1
 locality      LOC1
 instances 1 allowed-nssai [ slice1 slice2 ]
 load-profile  gtp-load1
 instances 1 fqdn   5gc.mnc456.mcc123.3gppnetwork.org
 instances 1 inter-plmn-fqdn 5gc.mnc210.mcc310.3gppnetwork.org
 instances 1 supported-features [ vsmf ]
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 310 mnc 310
 exit
 service name nsmf-pdu
  type               pdu-session
  schema             http
  service-id         1
  version            1.Rn.0.0
  http-endpoint base-url http://smf-service
  icmpv6-profile     icmpprf1
  compliance-profile comp1
```

```
  access-profile     access1
  subscriber-policy  polSub
 exit
exit
profile sgw sgw1
 locality          LOC1
 fqdn              cisco.com.apn.epc.mnc456.mcc123
 subscriber-policy polSub
 ddn failure-action-drop-timer 60
 ddn no-user-connect-retry-timer 60
 qci-qos-profile   sgw-non-standardqci
 wps-profile       wps1
 plmn-list mcc 123 mnc 456
 exit
 plmn-list mcc 310 mnc 260
 exit
exit
profile sgw-charging-threshold thre1
 cc profile value 1
  volume total 100000
  buckets  2
  duration 180
 exit
 cc profile value 2
  volume uplink 100000
  volume downlink 100000
  buckets  4
  duration 120
 exit
 cc profile value 4
  volume total 10000000
  buckets  4
  duration 300
 exit
 cc profile value 8
  volume total 100000
  buckets  2
  duration 3000
 exit
exit
profile overload gtp-overload1
 overload-exclude-profile self-protection gtp-overloadExclude1
 node-level
  tolerance minimum 15
  tolerance maximum 35
  reduction-metric minimum 20
  reduction-metric maximum 90
  advertise
   interval        300
   change-factor   15
   validity-period 60
  exit
  interface gtpc
   overloaded-action [ advertise ]
  exit
 exit
exit
profile overload-exclude gtp-overloadExclude1
 dnn-list       [ sos ]
 arp-list       [ 1 2 3 ]
 procedure-list [ session-delete ]
 message-priority s5
  upto 0
 exit
```

```
exit
profile load gtp-load1
 load-calc-frequency  30
 load-fetch-frequency 15
 advertise
  interval      30
  change-factor 5
 exit
 interface gtpc
  action advertise
 exit
exit
profile gtpp-profile pf1 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile gtpp-profile pf2 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile gtpp-profile pf4 gtpp
 local-storage
  file
   rotation
    volume        5
    cdr-count     1000
    time-interval 60
   exit
   name
    prefix               hSMF-cnsgw1
    format               .%Y-%m-%d%H-%M-%S.%4Q
    max-file-seq-num     9
```

```
    start-file-seq-num   1
    recover-file-seq-num true
   exit
   format custom1
  exit
 exit
 dictionary custom24
exit
profile dns-proxy
 timeout             6000
 round-robin-answers
 servers serv1
  ip       209.165.202.143
  port     53
  protocol tcp
 exit
 servers serv2
  ip       209.165.200.225
  port     53
  protocol tcp
 exit
exit
profile converged-core cc1
 max-upf-index 150
exit
nf-tls certificates cert1
 cert-data abc
 private_key k1
exit
active-charging service acs1
 bandwidth-policy BWP
  flow limit-for-bandwidth id 1 group-id 2
  flow limit-for-bandwidth id 2 group-id 3
  flow limit-for-bandwidth id 3 group-id 4
  group-id 2 direction uplink peak-data-rate 64000 peak-burst-size 8000 violate-action
discard
  group-id 2 direction downlink peak-data-rate 64000 peak-burst-size 8000 violate-action
discard
  group-id 3 direction uplink peak-data-rate 128000 peak-burst-size 12000 violate-action
discard
  group-id 3 direction downlink peak-data-rate 128000 peak-burst-size 12000 violate-action
 discard
  group-id 4 direction uplink peak-data-rate 3000000000 peak-burst-size 100 violate-action
 discard
  group-id 4 direction downlink peak-data-rate 3000000000 peak-burst-size 100 violate-action
 discard
 exit
 packet-filter pkt1
  ip local-port range 2 to 23
  ip protocol = 23
  ip remote-address = 209.165.201.0/27
  ip remote-port range 12 to 34
  ip tos-traffic-class = 23 mask = 23
  priority 23
 exit
 charging-action ca1
  billing-action egcdr
  content-id         51
  flow action redirect-url http://www.google.com
  flow limit-for-bandwidth id 1
  service-identifier 6000
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
```

```
 exit
 charging-action caStaticOfflineOnline
  billing-action egcdr
  cca charging credit
  content-id         30
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000000 peak-burst-size 100
violate-action discard committedDataRate 1000000000 committed-burst-size 100 exceed-action
 discard
  flow limit-for-bandwidth direction downlink peak-data-rate 1000000000 peak-burst-size 100
 violate-action discard committedDataRate 1000000000 committed-burst-size 100 exceed-action
 discard
  service-identifier 60
  tft-notify-ue
  tos af11
  tft packet-filter pkt1
 exit
 rulebase cisco
  billing-records egcdr
  edr transaction-complete http charging-edr http-edr
  dynamic-rule order first-if-tied
  egcdr threshold interval 1000
  action priority 1 ruledef ip-any-rule charging-action cisco
  route priority 1000 ruledef http-port-route analyzer http
 exit
 rulebase rba1
  action priority 1 dynamic-only ruledef rda1 charging-action ca1 description myrule1
  action priority 10 ruledef rda1 charging-action ca1
 exit
 urr-list urr_smf
  rating-group 10 urr-id 1
  rating-group 10 service-identifier 20 urr-id 2
  rating-group 10 service-identifier 21 urr-id 50
  rating-group 11 urr-id 3
  rating-group 11 service-identifier 21 urr-id 4
  rating-group 11 service-identifier 201 urr-id 11
  rating-group 12 urr-id 5
  rating-group 12 service-identifier 22 urr-id 6
  rating-group 13 urr-id 7
  rating-group 13 service-identifier 23 urr-id 8
  rating-group 30 urr-id 17
  rating-group 30 service-identifier 60 urr-id 18
  rating-group 30 service-identifier 61 urr-id 19
  rating-group 31 urr-id 20
  rating-group 31 service-identifier 61 urr-id 21
  rating-group 31 service-identifier 62 urr-id 22
  rating-group 32 urr-id 23
  rating-group 40 urr-id 24
  rating-group 51 service-identifier 6000 urr-id 32
  rating-group 100 urr-id 9
  rating-group 100 service-identifier 200 urr-id 10
  rating-group 100 service-identifier 201 urr-id 51
  rating-group 101 urr-id 11
  rating-group 101 service-identifier 201 urr-id 12
  rating-group 102 urr-id 13
  rating-group 102 service-identifier 202 urr-id 14
  rating-group 103 urr-id 15
  rating-group 103 service-identifier 203 urr-id 16
  rating-group 110 urr-id 25
  rating-group 199 urr-id 199
 exit
 ruledef adc_Youtube
  multi-line-or all-lines
 exit
 credit-control group onlineoffline
```

```
  diameter ignore-service-id true
 exit
 group-of-ruledefs adc_specific
  add-ruledef priority 1 ruledef adc_google
  add-ruledef priority 2 ruledef adc_facebook_https
  add-ruledef priority 3 ruledef adc_sni
 exit
gtpp group group1
 gtpp egcdr service-data-flow threshold interval 60
 gtpp egcdr service-data-flow threshold volume downlink 100000 uplink 100000 total 200000
exit
apn cisco
 gtpp group group1
 active-charging rulebase rba1
exit
apn intershat
 gtpp group group1
 active-charging rulebase rba1
exit
policy subscriber polSub
 precedence 1
  sst              22
  sdt              Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range 100000000000001
  supi-stop-range  299999999999999
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  operator-policy  opPol1
 exit
 precedence 511
  operator-policy defOprPol1
 exit
exit
policy upf-selection up-policy1
 precedence 1
   [ dnn slice ]
 exit
 precedence 2
   [ dnn location ]
 exit
 precedence 3
   [ dnn pdn-type-session ]
 exit
 precedence 4
   [ dnn ]
 exit
exit
policy operator defOprPol1
 policy dnn         defPolDnn
 policy network-capability nc1
exit
policy operator opPol1
 policy dnn         polDnn
 policy network-capability nc1
exit
policy operator opPol2
 policy dnn         polDnn
 policy network-capability nc1
exit
policy dnn defPolDnn
 profile default-profile
 dnn cisco profile cisco
```

```
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 dnn sos profile sos
 dnn starent profile abc.com
exit
policy dnn dnnPol1
 profile default
 dnn starent profile abc.com
exit
policy dnn polDnn
 profile default-profile
 dnn cisco profile cisco
 dnn dnn2 profile profile2
 dnn intershat profile intershat
 exit
policy network-capability nc1
 nw-support-local-address-tft true
exit
nssai name slice1
 sst 1
 dnn [ cisco intershat sos starent ]
exit
nssai name slice2
 sst 2
 sdt abf123
 dnn [ cisco intershat sos starent ]
exit
system-diagnostics session-consistency action monitor
ipam
 instance 1
  source local
  address-pool v4pool1
   vrf-name ISP
   tags
    dnn intershat
   exit
   ipv4
    split-size
     per-cache 65536
     per-dp    65536
    exit
    address-range 209.165.201.1 209.165.201.30
   exit
  exit
 exit
exit
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
group nrf discovery DISC1
 nrf-type PLMN
 service type nrf nnrf-disc
  endpoint-profile
   name       EP1
   uri-scheme http
   version
    uri-version v1
     full-version 209.165.200.224/27
    exit
   exit
   endpoint-name sauNRF
    priority 80
    capacity 56
```

```
    primary ip-address ipv4 209.165.201.4
    primary ip-address port 8095
   exit
  exit
 exit
exit
cdl system-id          2
cdl enable-geo-replication true
cdl zookeeper replica 1
cdl remote-site 1
 db-endpoint host 209.165.202.154
 db-endpoint port 8882
 kafka-server 209.165.200.226 10092
 exit
exit
cdl label-config session
 endpoint key smi.cisco.com/node-type
 endpoint value smf-cdl
 slot map 1
  key   smi.cisco.com/node-type
  value smf-cdl
 exit
 slot map 2
  key   smi.cisco.com/node-type
  value smf-cdl-1
 exit
 index map 1
  key   smi.cisco.com/node-type
  value smf-cdl-1
 exit
exit
cdl logging default-log-level error
cdl logging logger datastore.ep.session
 level debug
exit
cdl logging logger datastore.index.session
 level debug
exit
cdl logging logger datastore.slot.session
 level debug
exit
cdl datastore session
 label-config    session
 geo-remote-site [ 1 ]
 slice-names     [ 1 2 ]
 endpoint replica 1
 endpoint external-ip 209.165.202.158
 endpoint external-port 8882
 index replica 1
 index map    1
 index write-factor 1
 slot replica 1
 slot map     2
 slot write-factor 1
exit
cdl kafka replica 1
cdl kafka ssl-settings enable-ssl false
cdl kafka label-config key smi.cisco.com/pod-type
cdl kafka label-config value cdl-kafka-1
cdl kafka external-ip 209.165.202.158 10092
exit
etcd replicas 1
edr reporting disable
edr all subscribers
```

```
edr file transaction
 reporting enable
exit
edr file transaction-collision
 reporting enable
exit
instance instance-id 1
 endpoint li
  replicas 1
  nodes    1
  vip-ip 209.165.200.226
 exit
 endpoint nodemgr
  replicas 1
  nodes    2
 exit
 endpoint gtp
  replicas                1
  nodes                   2
  internal-vip            209.165.200.226
  mbr-optimization
   enable            true
   teid-cache-expiry 120000
   mbr-cache-expiry  50
  exit
  enable-gtpc-bypass      true
  retransmission timeout 5 max-retry 4
  enable-cpu-optimization true
  enable-go-encdec        true
  sla response 5000
  sla procedure 5000
  vip-ip 209.165.200.226
  interface s5
   sla procedure 5000
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
   retransmission timeout 5 max-retry 4
   enable-go-encdec true
  exit
  interface s5e
   sla response 5000
   sla procedure 5000
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
   path-failure detection-policy pol_egtp_path_failure
   retransmission timeout 5 max-retry 4
   enable-go-encdec true
  exit
  interface s2b
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
  exit
  interface gtpu
  exit
  interface s11
   sla response 5500
   echo interval          60
   echo retransmission-timeout 5
   echo max-retransmissions 4
   path-failure detection-policy pol_egtp_path_failure
   retransmission timeout 5 max-retry 4
```

```
  enable-go-encdec true
  dscp             0x20
  vip-ip 209.165.200.226
 exit
exit
endpoint pfcp
 replicas               1
 nodes                  2
 internal-vip           209.165.200.226
 retransmission timeout 3 max-retry 2
 enable-cpu-optimization true
 vip-ip 209.165.200.226
 interface sxa
  sla response 4000
  heartbeat
   interval               60
   retransmission-timeout 9
   max-retransmissions    10
  exit
  retransmission timeout 5 max-retry 4
  vip-ip 209.165.200.226
  dispatcher
   count         25
   capacity      250
   outbound      true
   cache         true
   threshold     500
   expiry        60000
   nonresponsive 30500
  exit
 exit
 interface n4
  heartbeat
   interval               0
   retransmission-timeout 3
   max-retransmissions    5
  exit
  retransmission timeout 3 max-retry 2
  vip-ip 209.165.200.226
  dispatcher
   count         5
   capacity      1000
   outbound      true
   threshold     5000
   expiry        60000
   nonresponsive 30500
  exit
 exit
exit
endpoint service
 replicas 1
 nodes    1
exit
endpoint protocol
 replicas     1
 nodes        2
 internal-vip 209.165.200.226
 vip-ip 209.165.200.226
exit
endpoint radius
 replicas 1
 nodes    1
 vip-ip 209.165.200.226
 interface coa-nas
```

```
   vip-ip 209.165.200.226 vip-port 3799
  exit
 exit
 endpoint sgw-service
  replicas 1
  nodes    1
 exit
 endpoint dns-proxy
  replicas 1
 exit
 endpoint sbi
  replicas 1
  nodes    1
  vip-ip 209.165.200.226
  interface nrf
   vip-ip 209.165.200.226
  exit
 exit
exit
logging transaction message enable
logging transaction duplicate enable
logging level application trace
logging level transaction trace
logging level tracing debug
logging name infra.application.core level application warn
logging name infra.application.core level tracing warn
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.config.core level tracing off
logging name infra.dispatcher.core level application warn
logging name infra.dispatcher.core level transaction warn
logging name infra.dispatcher.core level tracing warn
logging name infra.heap_dump.core level application warn
logging name infra.ipcstream.core level application error
logging name infra.ipcstream.core level transaction warn
logging name infra.ipcstream.core level tracing warn
logging name infra.memory_cache.core level application error
logging name infra.memory_cache.core level transaction error
logging name infra.message_log.core level transaction trace
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
logging name infra.rest_server.core level application error
logging name infra.rest_server.core level tracing off
logging name infra.topology.core level application off
logging name infra.topology.core level transaction off
logging name infra.topology.core level tracing off
deployment
 app-name               cnsgw-smf-1
 cluster-name           Local
 dc-name                DC
 model                  small
 logical-nf-instance-id 1
exit
k8 label protocol-layer key smi.cisco.com/vm-type value smf-proto-1
exit
k8 label service-layer key smi.cisco.com/vm-type value smf-svc-1
exit
k8 label cdl-layer key smi.cisco.com/node-type value smf-cdl-1
exit
k8 label oam-layer key smi.cisco.com/node-type value oam
exit
instances instance 1
 system-id  smf
 cluster-id smf
```

```
 slice-name 1
exit
local-instance instance 1
system mode running
helm default-repository roaming-ph2
helm repository cnsgw-1
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/master/
exit
helm repository roaming-cx
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw
 url
https://engci-maven-master.cisco.com/artifactory/mobile-cnat-charts-release/releng-builds/2021.03.m0.d4.0/ccg/2021.03.m0.d4.0.i77/ccg.2021.03.m0.d4.0.i77/
exit
helm repository roaming-ph2
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw
 url
https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnat-cn/cn-products/dev-smf-amigos/
exit
k8s name          cnsgw-smf-1
k8s namespace     cnsgw-1
k8s nf-name       smf
k8s registry      dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node   true
k8s use-volume-claims false
k8s ingress-host-name 209.165.200.238.nip.io
aaa authentication users user admin
 uid        117
 gid        117
 password   $1$bQRuPxWc$ESF/KLDQBkmdQNtrReTJN1
 ssh_keydir /tmp/admin/.ssh
 homedir    /tmp/admin
exit
aaa authentication users user liadmin
 uid        201
 gid        2011
 password   $1$LugH/seF$hi4y0QnpOZoEiJDqGLd0L.
 ssh_keydir /tmp/liadmin/.ssh
 homedir    /tmp/liadmin
exit
aaa authentication users user liadmin2
 uid        202
 gid        2021
 password   $1$HBRlXp0W$pmaMFhDV9QIayXTxEZtxc0
 ssh_keydir /tmp/liadmin2/.ssh
 homedir    /tmp/liadmin2
exit
aaa authentication users user liadmin3
 uid        203
 gid        2031
 password   $1$kE6v4ZBD$sv97OlhMCmTtjm7Q35Esq1
 ssh_keydir /tmp/liadmin3/.ssh
 homedir    /tmp/liadmin3
exit
aaa ios level 0
 prompt "\h> "
exit
aaa ios level 15
 prompt "\h# "
exit
```

```
aaa ios privilege exec
 level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
  command exit
  exit
  command help
  exit
  command startup
  exit
 exit
 level 15
  command configure
  exit
 exit
exit
nacm write-default deny
nacm groups group LI
 user-name [ liadmin ]
exit
nacm groups group LI2
 user-name [ liadmin2 ]
exit
nacm groups group LI3
 user-name [ liadmin3 ]
exit
nacm groups group admin
 user-name [ admin ]
exit
nacm rule-list admin
 group [ admin ]
 rule li-deny-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            deny
 exit
 rule li-deny-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            deny
 exit
 rule any-access
  action permit
 exit
exit
nacm rule-list confd-api-manager
 group [ confd-api-manager ]
 rule any-access
  action permit
 exit
exit
nacm rule-list ops-center-security
 group [ * ]
 rule change-self-password
  module-name       ops-center-security
  path              /smiuser/change-self-password
  access-operations exec
  action            permit
```

```
 exit
 rule smiuser
  module-name       ops-center-security
  path              /smiuser
  access-operations exec
  action            deny
 exit
exit
nacm rule-list lawful-intercept
 group [ LI LI2 LI3 ]
 rule li-accept-tap
  module-name       lawful-intercept
  path              /lawful-intercept
  access-operations *
  action            permit
 exit
 rule li-accept-clear
  module-name       tailf-mobile-smf
  path              /clear/lawful-intercept
  access-operations *
  action            permit
 exit
exit
```