Release Change Reference, StarOS Release 21.11/Ultra Services Platform Release 6.5

First Published: 2018-11-29

Last Modified: 2020-10-07

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

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.

CHAPTER 1

Release 21.11/6.5 Features and Changes Quick Reference

Release 21.11/6.5 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5G NSA for SAEGW, on page 13	SAEGW	21.11
Automatic Password Generator (APG) Application, on page 41	UGP	6.5
Automatic Scale-out Support, on page 43	UGP	6.5
Backward Compatibility Restoration by QoS-Information AVP, on page 45	GGSN	21.11.2
CLI Support for P-GW to include AVPs in CCR-U Messages, on page 47	P-GW	21.11.3
Controlled ORBS Service Initialization, on page 51	All	21.11
Collision Handling for Path Update during Bearer Creation, on page 53	MME	21.11.13
Debug Console Swap, on page 55	All	21.12
Deprecation of Manual Scaling, on page 57	UAS	6.0
ERAB Setup Retry Handling, on page 59	MME	21.11.13
Handling NPLI Requests, on page 67	P-GW	21.11.3
GB Manager Queue Handling	SGSN	21.11.9
Handling of APN Configuration in ISDR from HSS	MME	21.11.9

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
MME Manager Status Traps, on page 83	MME	21.11.3
MME Support for Service Impacting KPI Bulk Statistics, on page 101	MME	21.11.3
Monitor Process Listing, on page 69	All	21.11
NAS Signaling Security, on page 71	MME	21.11.3
New Attribute in P-GW CDR for Custom GTPP Dictionary, on page 81	P-GW	21.11.3
NAS Notification for SRVCC Cancellation due to TAU Request, on page 79	MME	21.11.16
Paging eDRX H-SFN Changed to 10 Bits Counter, on page 87	MME	21.11.3
SBc Message Size, on page 89	MME	21.11
Secure File Transfer, on page 91	USP	6.5
Service Impacting SGSN KPI Bulk Statistics, on page 109	SGSN	21.11.3
SGs SCTP Association Counters, on page 105	MME	21.11
Short Message Service, on page 111	MME	21.11
SRVCC Delete Bearer Request Handling, on page 97	MME	21.11.4
SRVCC HO Timer Configuration for ESM Notification, on page 99	MME	21.11.9
Support for OSP 13 with RHEL 7.5, on page 143	P-GW S-GW UGP	21.11 6.5
TCP Proxy-Enabled Flows, on page 145	P-GW	21.11.7
User Session Management for UAS and UEM VMs, on page 147	UGP	6.5

CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

The following table indicates what features are enabled or disabled by default.

Feature	Default
5G NSA for SAEGW	Disabled - Configuration Required
Automatic Password Generator (APG) Application	Enabled - Always-on
Automatic Scale-out Support	Disabled - Configuration required
Backward Compatibility Restoration by QoS-Information AVP	Enabled - Always-on
CLI Support for P-GW to include AVPs in CCR-U Messages	Disabled – Configuration Required
Controlled ORBS Service Initialization	Disabled – Configuration Required
Collision Handling for Path Update during Bearer Creation	Enabled - Always-on
Debug Console Swap	Enabled - Always on
Deprecation of Manual Scaling	Disabled - Configuration Required
ERAB Setup Retry Handling	Disabled - Configuration Required
GM Manager Queue Handling	Disabled – Configuration Required
Handling NPLI Requests	Disabled - Configuration Required
Handling of APN Configuration in ISDR from HSS	Enabled – Always-on
NAS Notification for SRVCC Cancellation due to TAU Request	Enabled- Always On
Monitor Process Listing	Enabled - Always-on
NAS Signaling Security	Disabled - Configuration Required

Feature	Default
New Attribute in P-GW CDR for Custom GTPP Dictionary	Enabled - Always-on (for a customer-specific GTPP dictionary)
Paging eDRX H-SFN changed to 10 bits counter	This feature is enabled/disabled, when the eDRX feature is enabled/disabled.
SBc Message Size	Disabled – Configuration Required
Secure File Transfer	Disabled – Configuration Required
SGs SCTP Association Counters	Enabled - Always-on
Short Message Service	Disabled - Configuration Required
SRVCC Delete Bearer Request Handling	Disabled - Configuration Required
SRVCC HO Timer Configuration for ESM Notification	Enabled – Configuration Required
Support for OSP 13 with RHEL 7.5	Disabled – Configuration Required
TCP Proxy-enabled Flows	Enabled - Always-on
User Session Management for UAS and UEM VMs	Enabled - Always-on

CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.11 software release.

Important For more information regarding bulk statistics identified in this section, see the latest version of the *BulkstatStatistics_document.xls* spreadsheet supplied with the release.

Bulk statistics changes for 21.11 include:

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.11.

None in this release.

Modified Bulk Statistics

This section identifies bulk statistics that have been modified in release 21.11.

None in this release.

Deprecated Bulk Statistics

This section identifies bulk statistics that are no longer supported in release 21.11.

None in this release.

CHAPTER 4

SNMP MIB Changes in StarOS 21.11 and USP 6.5

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.11 and Ultra Services Platform (USP) 6.5 software releases.

SNMP MIB Object Changes for 21.11

This section provides information on SNMP MIB alarm changes in release 21.11.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.11.

The following alarms are new in this release:

- starCBCBufSizeExceeded

Modified SNMP MIB Object

This section identifies SNMP MIB alarms modified in release 21.11.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Object

This section identifies SNMP MIB alarms that are no longer supported in release 21.11.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Alarm Changes for 21.11

This section provides information on SNMP MIB alarm changes in release 21.11.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 21.11.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 21.11.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 21.11.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Conformance Changes for 21.11

This section provides information on SNMP MIB alarm changes in release 21.11.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Conformance

This section identifies new SNMP MIB alarms available in release 21.11.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Conformance

This section identifies SNMP MIB alarms modified in release 21.11.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Conformance

This section identifies SNMP MIB alarms that are no longer supported in release 21.11.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Object Changes for 6.5

This section provides information on SNMP MIB object changes in the Ultra M MIB corresponding to release 6.5.

Important For more information regarding SNMP MIB objects in this section, see the *Ultra M Solutions Guide* for this release.

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 6.5.

The following objects are new in this release:

- None in this release.

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 6.5.

The following objects have been modified in this release:

- None in this release.

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 6.5.

The following objects have been deprecated in this release:

- None in this release.

SNMP MIB Alarm Changes for 6.5

This section provides information on SNMP MIB alarm changes in the Ultra M MIB corresponding to release 6.5.

Important For more information regarding SNMP MIB alarms in this section, see the *Ultra M Solutions Guide* for this release.

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 6.5.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 6.5.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 6.5.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Conformance Changes for 6.5

This section provides information on SNMP MIB conformance statement changes in the Ultra M MIB corresponding to release 6.5.

Important For more information regarding SNMP MIB conformance statements in this section, see the *Ultra M Solutions Guide* for this release.

New SNMP MIB Conformance Statements

This section identifies new SNMP MIB conformance statements available in release 6.5.

The following conformance statements are new in this release:

- None in this release.

Modified SNMP MIB Conformance Statements

This section identifies SNMP MIB conformance statements that are modified in release 6.5.

The following conformance statements have been modified in this release:

- None in this release.

Deprecated SNMP MIB Conformance Statements

This section identifies SNMP MIB conformance statements that are no longer supported in release 6.5.

The following conformance statements have been deprecated in this release:

- None in this release.

CHAPTER 5

5G NSA for SAEGW

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable

Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

The 5G NSA solution for SAEGW supports dcca-custom1, dcca-custom7 and dcca-custom8 dictionaries additionally.	21.11
The 5G NSA solution for SAEGW supports the following functionality in this release: • P-GW Custom Dictionaries support over Gz for extended bitrate • S-GW Custom Dictionaries support over Gz for extended bitrate • P-GW Custom Dictionaries support over Gy and Rf for extended bitrate • S-GW support of Secondary RAT Data Usage Report in Gz CDRs	21.10
The 5G NSA solution for SAEGW supports the following functionality in this release: • P-GW support of Secondary RAT Data Usage Report in Gz CDRs • P-GW support of Secondary RAT Data Usage Report in Rf CDRs • S-GW and P-GW support of statistics for DCNR PDNs	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
The 5G NSA solution for SAEGW supports the following functionality in this release: • Feature License • Dedicated Bearers • Gy interface • URLLC QCI	21.8
First introduced.	21.6

Feature Description

Cisco 5G Non Standalone (NSA) solution leverages the existing LTE radio access and core network (EPC) as an anchor for mobility management and coverage. This solution enables operators using the Cisco EPC Packet Core to launch 5G services in shorter time and leverage existing infrastructure. Thus, NSA provides a seamless option to deploy 5G services with very less disruption in the network.

Overview

5G is the next generation of 3GPP technology, after 4G/LTE, defined for wireless mobile data communication. The 5G standards are introduced in 3GPP Release 15 to cater to the needs of 5G networks.

The two solutions defined by 3GPP for 5G networks are:

- 5G Non Standalone (NSA): The existing LTE radio access and core network (EPC) is leveraged to anchor the 5G NR using the Dual Connectivity feature. This solution enables operators to provide 5G services with shorter time and lesser cost.

  Note The 5G NSA solution is supported in this release.

- 5G Standalone (SA): An all new 5G Packet Core will be introduced with several new capabilities built inherently into it. The SA architecture comprises of 5G New Radio (5G NR) and 5G Core Network (5GC).

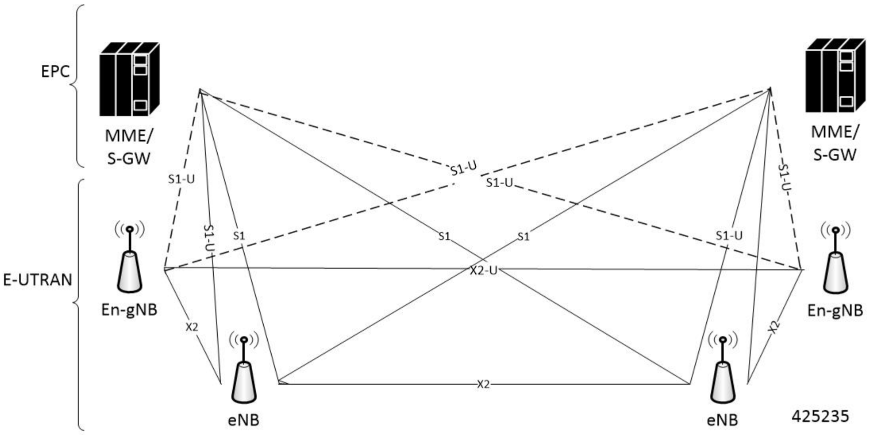
  Network Slicing, CUPS, Visualization, Multi-Gbps support, Ultra low latency, and other such aspects will be natively built into the 5G SA Packet Core architecture.

Dual Connectivity

The E-UTRA-NR Dual Connectivity (EN-DC) feature supports 5G New Radio (NR) with EPC. A UE connected to an eNodeB acts as a Master Node (MN) and an en-gNB acts as a Secondary Node (SN). The eNodeB is connected to the EPC through the S1 interface and to the en-gNB through the X2 interface. The en-gNB can be connected to the EPC through the S1-U interface and other en-gNBs through the X2-U interface.

The following figure illustrates the E-UTRA-NR Dual Connectivity architecture.

Figure 1: EN-DC Architecture



If the UE supports dual connectivity with NR, then the UE must set the DCNR bit to "dual connectivity with NR supported" in the UE network capability IE of the Attach Request/Tracking Area Update Request message.

If the UE indicates support for dual connectivity with NR in the Attach Request/Tracking Area Update Request message, and the MME decides to restrict the use of dual connectivity with NR for the UE, then the MME sets the RestrictDCNR bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message.

If the RestrictDCNR bit is set to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message, the UE provides the indication that dual connectivity with NR is restricted to the upper layers.

If the UE supports DCNR and DCNR is configured on MME, and if HSS sends ULA/IDR with "Access-Restriction" carrying "NR as Secondary RAT Not Allowed", MME sends the "NR Restriction" bit set in "Handover Restriction List" IE during Attach/TAU/Handover procedures. Similarly, MME sets the RestrictDCNR bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept/Tracking Area Update Accept message. Accordingly, UE provides the indication that dual connectivity with NR is restricted to the upper layers.

The "Handover Restriction List" IE is present in the "Initial Context Setup Request" message for Attach and TAU procedure with data forwarding procedure, in the "Handover Required" message for S1 handover procedure, in the "Downlink NAS Transport" message for TAU without active flag procedure.

Important 5G NSA feature is license controlled from release 21.8 onwards. Contact your Cisco account representative for detailed information on specific licensing requirements.

The 5G NSA solution for SAEGW supports the following functionalists:

- **High Throughput**

  5G NR offers downlink data throughput up to 20 Gbps and uplink data throughput up to 10 Gbps. Some interfaces in EPC have the support to handle (encode/decode) 5G throughput. For example, NAS supports up to 65.2 Gbps (APN-AMBR) and S5/S8/S10/S3 (GTP-v2 interfaces) support up to 4.2 Tbps. The diameter interfaces S6a and Gx support only up to 4.2Gbps throughput, S1-AP supports only up to 10

Gbps and NAS supports up to 10 Gbps (MBR, GBR). New AVP/IE have been introduced in S6a, Gx , S1-AP, and NAS interfaces to support 5G throughput. See the *How It Works* section for more information.

- **DCNR Support on P-GW:**

  Supports configuration of DCNR feature at the P-GW-service, by configuring “Extended-BW-NR” feature in IMSA service. Advertises the DCNR feature support by sending “Extended-BW-NR” feature bit in “Feature-List-ID-2” towards PCRF. Forwards AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in CCR messages when it receives APN-AMBR values greater than 4.2Gbps from MME/S-GW. Decodes the extended AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" when it is received from PCRF.

- Sends AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when it receives MBR and GBR values greater than 4.2Gbps from MME/S-GW. Decodes the AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when received from PCRF. Supports dedicated bearer establishment with extended QoS. Sends AVP Extended-Max-Requested-BW-UL and "Extended-Max-Requested-BW-DL" in Gy records.

- **Ultra Low Latency Support**:

  Supports 5G requirements of Ultra-Reliable and Low Latency Communications (URLLC). 3GPP introduced URLCC QCI 80 (Non-GBR resource type), QCI 82 and 83 (GBR resource type). P-GW establishes default bearers with URLLC QCI 80, which is typically used by low latency eMBB applications. P-GW establishes dedicated bearers with URLLC QCI 82 and 83 (also with QCI 80 if dedicated bearers of Non-GBR type to be established), which is typically used by discrete automation services (industrial automation).

- **ICSR Support**

  With release 21.10 onwards ICSR for 5G NSA on SAEGW is supported.

- **Dynamic S-GW and P-GW selection by MME for DCNR capable UE**

  When DCNR capable UE attempts to register in MME and when all DCNR validations are successful (for example DCNR feature configuration on MME, HSS not sending access-restriction for NR, and son on), the MME sets “UP Function Selection Indication Flags” IE with DCNR flag set to 1 in “Create Session Request” message. This feature is relevant for CUPS architecture to help SGW-C and PGW-C to select SGW-U and PGW-U which supports dual connectivity with NR. When S-GW receives this IE over S11, it sends this IE over S5 to P-GW. S-GW ignores IE if it receives it in Non-CUPS deployment.

- **P-GW Secondary RAT Usage Data Report Handling:**

  P-GW supports custom24 and custom44 for Gz and aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries for Rf to support Secondary RAT Data Usage Report in CDRs.

- **Statictics support for DCNR PDNs:**

  S-GW and P-GW statistics support for DCNR PDNs

- **S-GW Secondary RAT Usage Data Report Handling:**

  S-GW supports custom24 and custom6 dictionaries to support Secondary RAT Data Usage Report in CDRs over Gz.

- **P-GW Custom Dictionaries Support over Gz:**

  P-GW supports Custom44 and Custom24 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Multiple Presence Reporting Area Support:**

  S-GW supports Multiple-PRA action and Multiple-PRA Information over S11/S4 and S5/S8 interfaces. P-GW supports Multiple-PRA Action and Multiple-PRA Information over S5/S8 and Gx interfaces.

- **S-GW Custom Dictionaries Support over Gz :**

  S-GW supports custom24 and custom6 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gx:**

  P-GW supports dpca-custom15, dpca-custom11, dpca-custom23, dpca-custom19 and dpca-custom17, dictionarie to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gy:**

  P-GW supports dcca-custom1, dcca-custom7, dcca-custom8 and dcca-custom13 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL

  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Rf:**

  P-GW supports aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

Multiple Presence Reporting Area

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

Note This feature is introduced in release 21.9.1. For more information, refer to the *Presence Reporting Area* chapter in the *P-GW Administration Guide*.

How It Works

Architecture

This section describes the architecture for Gx (PCRF), Gy (OCS), Gz (P-GW), and Rf (P-GW) interfaces with respect to 5G NSA for SEAEGW feature.

Gx (PCRF)

The Gx interface supports new AVPs to handle 5G throughput for default bearers and dedicated bearers. Gx interface introduced new "AVP Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in grouped "AVP QoS-Information" and "Conditional-APN-Aggregate-Max-Bitrate" to handle 5G throughput for default bearers. New AVPs "Extended-GBR-UL", "Extended-GBR-DL", "Extended-Max-Requested-BW-UL" and "Extended-Max-Requested-BW-DL" are added in grouped AVP "QoS-Information" for dedicated bearers.

When the maximum bandwidth value set for UL or DL traffic is higher than 4294967295 bits per second, the "Max-Requested-Bandwidth-UL" or DL, AVP must be present, and set to its upper limit 4294967295 along with the "Extended-Max-Requested-BW-UL" or DL must be present, and set to the requested bandwidth value in kilobits per second. The same principal applies for "Extended-GBR-UL/DL" and "Extended-APN-AMBR-UL/DL".

The following new AVPs are introduced in the grouped AVP QoS-Information:

- Extended-Max-Requested-BW-UL
- Extended-Max-Requested-BW-DL
- Extended-GBR-UL
- Extended-GBR-DL
- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

the following new AVPs are introduced in the grouped AVP Conditional-APN-Aggregate-Max-Bitrate.

- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

Gy (OCS)

New AVPs "Extended-Max-Request-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL", "Extended-GBR-DL", "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in grouped AVP “QoS-Information” are introduced Gy interface to handle 5G throughput for dedicated bearers.

When the maximum bandwidth value set for UL/DL traffic is higher than 4294967295 bits per second, P-GW sets the "Max-Requested-Bandwidth-UL/DL" AVP to its upper limit 4294967295 and sets the "Extended-Max-Requested-BW-UL/DL" to the required bandwidth value in kilobits per second in CCR-I/CCR-U messages. The same principal applies for "Extended-GBR-UL/DL" and "Extended-APN-AMBR-UL/DL".

5G NSA feature supports Gy dcca-custom1, dcca-custom7, dcca-custom8 and standard dcca-custom13 dictionaries.

Gz (P-GW)

New sequence of container in PGWRecord for PGW-CDR to support RAN secondary RAT usage data report is introduced in Gz interface. AVPs "listOfRANSecondaryRATUsageReports" and "RANSecondaryRATUsageReport" are introduced.

New AVPs "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL", "Extended-GBR-DL", "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" are introduced over Gz interface as part of existing "EPCQoSInformation" AVP to handle 5G throughput for default and dedicated bearers.

Rf (P-GW)

New AVPs "RAN-Secondary-RAT-Usage-Report" which is grouped type to support secondary RAT usage data report values is introduced in Rf interface. This contains the volume count as reported by the RAN for the secondary RAT(separated for uplink and downlink) including the time of the report.

AVPs "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL", "Extended-GBR-DL", "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" are introduced over Rf interface to handle 5G throughput for default and dedicated bearers.

Gz(S-GW)

New sequence of container in SGWRecord for SGW-CDR to support RAN secondary RAT usage data report is introduced in Gz interface. AVPs "listOfRANSecondaryRATUsageReports" and "RANSecondaryRATUsageReport" are introduced.

New AVPs "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL", "Extended-GBR-DL", "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" are introduced over Gz interface as part of existing "EPCQoSInformation" AVP to handle 5G throughput for default and dedicated bearers.

Limitations

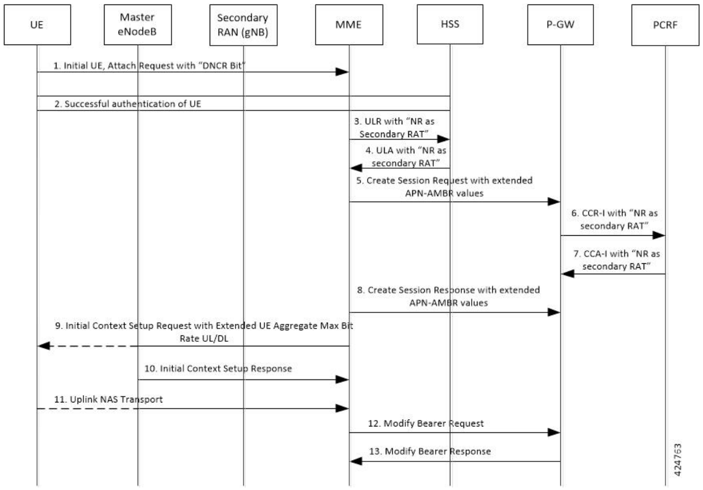
This section describes the known limitations for 5G NSA feature

- 5G NSA supports Gx standard dictionary (r8-gx-standard), dpca-custom11, dpca-custom15, dpca-custom17, dpca-custom19, and dpca-custom23.
- 5G NSA has been implemented for Gy dictionaries dcca-custom1, dcca-custom7, dcca-custom8 and standard dcca-custom13. In order to support NSA for other Gx and Gy dictionaries, dynamic dictionary must be built. Contact your Cisco Account representative for more details.
- Secondary RAT usage data report will not carry start or end time values prior to “00:00:00 UTC, Thursday, 1 January 1970".

Flows

This section describes the following call flows related to the DCNR feature.

Initial Registration by DCNR Capable UE


UE
Master eNodeB
Secondary RAN (gNB)
MME
HSS
P-GW
PCRF
1. Initial UE, Attach Request with "DNCR Bit"
2. Successful authentication of UE
3. ULR with "NR as Secondary RAT"
4. ULA with "NR as secondary RAT"
5. Create Session Request with extended APN-AMBR values
6. CCR-I with "NR as secondary RAT"
7. CCA-I with "NR as secondary RAT"
8. Create Session Response with extended APN-AMBR values
9. Initial Context Setup Request with Extended UE Aggregate Max Bit Rate UL/DL
10. Initial Context Setup Response
11. Uplink NAS Transport
12. Modify Bearer Request
13. Modify Bearer Response
424763

Step	Description
1	The DCNR capable UE sets the "DCNR bit" in the NAS message "Attach Request" of "UE Network Capability" IE.
2	MME successfully authenticates the UE.
3	As part of the authorization process, while sending ULR to HSS, MME advertises the DCNR support by sending “NR as Secondary RAT" feature bit in “Feature-List-ID-2".
4	HSS sends ULA by advertising the DCNR by sending "NR as Secondary RAT" feature bit in “Feature-List-ID-2" and sends Max-Requested-Bandwidth-UL as 4294967295 bps, Max-Requested-Bandwidth-DL as 4294967295 bps and the extended bandwidth values in new AVPs "Extended-Max-Requested-BW-UL" and "Extended-Max-Requested-BW-DL". If HSS determines that the UE is not authorized for DCNR services, HSS sends Subscription-Data with “Access-Restriction" carrying “NR as Secondary RAT Not Allowed".
5	MME sends Create Session Request with the extended APN-AMBR values in existing AMBR IE. As the APN-AMBR values in GTP-v2 interface are encoded in kbps, the existing AMBR IE handles the 5G NSA bit rates.
6	P-W sends CCR-I to PCRF advertising the DCNR by sending “Extended-BW-NR" feature bit in “Feature-List-ID-2". P-GW also sends "APN-Aggregate-Max-Bitrate-UL" as 4294967295 bps, "APN-Aggregate-Max-Bitrate-DL" as 4294967295 bps and the extended bandwidth values in new AVPs "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL".
7	PCRF sends CCA-I advertising the DCNR by sending the “Extended-BW-NR" feature bit in “Feature-List-ID-2". PCRF also sends "APN-Aggregate-Max-Bitrate-UL" as 4294967295 bps and "APN-Aggregate-Max-Bitrate-DL" as 4294967295 bps and the extended bandwidth values in new "AVPs Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL". PCRF offers the same extended APN-AMBR values requested by PCEF or modify the extended APN-AMBR values. P-GW enforces the APN-AMBR values accordingly.
8	P-GW honors the APN-AMBR values as offered by PCRF and sends the extended APN-AMBR values in existing IE APN-AMBR in the Create Session Response message.

Step	Description
9	MME computes the UE-AMBR values and sends the extended UE-AMBR values in new IEs “Extended UE Aggregate Maximum Bit Rate Downlink" and “Extended UE Aggregate Maximum Bit Rate Uplink" by setting the legacy “UE AMBR Uplink" and “UE AMBR Downlink" values to the maximum allowed value 10000000000 bps(10 Gbps) in Initial Context Setup Request. MME sends the APN-AMBR values up to 65.2 Gbps in existing IE APN-AMBR in NAS Activate Default EPS Bearer Context Request – Attach Accept. If the APN-AMBR values are beyond 65.2 Gbps, MME sends the extended APN-AMBR values in new IE “Extended APN aggregate maximum bit rate. If ULA is received with “Access-Restriction" carrying “NR as Secondary RAT Not Allowed", MME sends the “Initial Context Setup Request" with “NR Restriction" bit set in “Handover Restriction List" IE. Also MME sets the "RestrictDCNR" bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept message. Accordingly, UE provides the indication that DCNR is restricted to the upper layers. If DCNR is not configured at MME service or call control profile level, MME sets the RestrictDCNR bit to "Use of dual connectivity with NR is restricted" in the EPS network feature support IE of the Attach Accept message. Accordingly, UE provides the indication that DCNR is restricted to the upper layers.
10	eNodeB sends the Initial Context Setup Response message. If master eNodeB determines to establish the bearer on secondary eNodeB, F-TEID of secondary eNodeB may be sent in this step (Transport layer address and TEID of secondary eNodeB). It is transparent to MME if the bearer is established on master eNodeB or secondary eNodeB.
11	eNodeB sends Uplink NAS Transport with NAS message Attach Complete - Activate Default EPS Bearer Context Accept.
12	MME sends Modify Bearer Request to S-GW with S1-U FTEID details as received in the Initial Context Setup Response message.
13	MME receives the Modify Bearer Response message from S-GW.

Supported Standards

Cisco's implementation of the 5G NSA complies with the following standards:

- 3GPP 23.401 Release 15.2.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 29.212 Release 15.2.0 - Policy and Charging Control (PCC)
- 3GPP 29.274 Release 15.2.0 - 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP 32.299 Release 15.2.0 - Charging Management; Diameter Charging Applications
- 3GPP 32.298 Release 15.2.0 - Charging Management; Charging Data Record (CDR) parameter description

Configuring 5G NSA for SAEGW

This section describes how to configure 5G NSA to support SAEGW.

Configuring 5G NSA on SAEGW involves:

- Enabling DCNR in P-GW Service, on page 24
- Configuring Bearer Duration Statistics for URLLC QCI, on page 24
- Configuring EGTPC QCI Statistics for URLLC QCI, on page 25
- Configuring Extended Bandwidth with New Radio, on page 25
- Configuring Network-Initiated Setup/Teardown Events for URLLC QCI, on page 26
- Configuring URLLC QCI in APN Configuration, on page 26
- Configuring URLCC QCI In Charging Action, on page 27
- Configuring URLCC QCI in QCI QOS Mapping Table , on page 27

Enabling DCNR in P-GW Service

Use the following configuration to enable Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

```
configure
   context context_name
      pgw-service service_name
         [ no ] dcnr
         end
```

NOTES:

- **pgw-service** *service_name*: Creates an P-GW service or configures a existing P-GW service. *service_name* must be an alphanumeric string of 1 to 63 characters.
- **no**: Disables the DCNR configuration.
- The **dcnr** CLI command is disabled by default.

Configuring Bearer Duration Statistics for URLLC QCI

Use the following configuration to configure QCI based duration statistics for URLLC QCI.

```
configure
   context context_name
      apn apn_name
          [ no ] bearer-duration-stats qci qci_val
          end
```

NOTES:

- **apn** *apn_name*: Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context. *apn_name* specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive.
- **bearer-duration-stats**: Enables or disables per QCI call duration statistics for dedicated bearers.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 80, 82, and 83.
- **no**: Disables per QCI call duration statistics.

Configuring EGTPC QCI Statistics for URLLC QCI

Use the following configuration to configure QCI based EGTPC QCI statistics for URLLC QCI.

```
configure
   context context_name
      apn apn_name
          [ no ] egtpc-qci-stats { qci80 | qci82 | qci83 }
          default egtpc-qci-stats
          end
```

Notes:

- **apn** *apn_name*: Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context. *apn_name* specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive.
- **egtpc-qci-stats**: Enables/Disables an APN candidate list for the **apn-expansion** bulkstats schema.
- **qci80**: Configure apn-qci-egtpc statistics for QCI 80.
- **qci82**: Configure apn-qci-egtpc statistics for QCI 82.
- **qci83**: Configure apn-qci-egtpc statistics for QCI 83.
- **no**: Disables APN candidate list(s) for the apn-expansion bulkstats schema.
- **default**: Disables an APN candidate list for the apn-expansion bulkstats schema.

Configuring Extended Bandwidth with New Radio

Use the following configuration to configure extended bandwidth with new radio in IMS authorization service mode.

```
configure
   context context_name
      ims-auth-service ims_auth_service_name
         policy-control
            diameter encode-supported-features extended-bw-newradio
            [ no ] diameter encode-supported-features
            end
```

NOTES:

- **ims-auth-service** *ims_auth_service_name*: Creates an IMS authentication service. *ims_auth_service_name* must be an alphanumeric string of 1 through 63 characters.
- **policy-control**: Configures Diameter authorization and policy control parameter for IMS authorization.
- **extended-bw-newradio**: Enables extended bandwidth with New-Radio feature.
- **diameter encode-supported-features**: Enables/Disables encoding and sending of Supported-Features AVP.
- **no**: Removes the configuration of extended bandwidth with new-radio in IMS authorization service mode.

Configuring Network-Initiated Setup/Teardown Events for URLLC QCI

Use the following configuration to configure network initiated setup or teardown events KPI for URLCC QCI.

```
configure
   transaction-rate nw-initiated-setup-teardown-events qci qci_val
   [ default | no ] transaction-rate nw-initiated-setup-teardown-events
qci
   end
```

NOTES:

- **transaction-rate nw-initiated-setup-teardown-events**: Enables operators to set the Quality of Class Identifier (QCI) value for use in tracking Network Initiated Setup/Tear down Events per Second key performance indicator (KPI) information.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 65, 66, 69, 70, 80, 82, 83, and 128 to 254.
- **no**: Disables the collection of network-initiated setup/teardown events for the specified QCI value.
- **default**: Returns the setting to its default value. The default is for network-initiated setup/teardown events to be tracked for all supported QCI values.

Configuring URLLC QCI in APN Configuration

Use the following configuration to configure URLCC QCI in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         qos rate-limit direction { downlink | uplink } qci qci_val
         no qos rate-limit direction { downlink | uplink }
         end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.

- **qos rate-limit**: Configures the action on a subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic shaping and policing functionality.
- **direction { downlink | uplink }**: Specifies the direction of traffic on which this QoS configuration needs to be applied.
  - **downlink**: Apply the specified limits and actions to the downlink.
  - **uplink**: Apply the specified limits and actions to the uplink.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 80, 82, and 83.
- **no**: Disables the QoS data rate limit configuration for the APN.

Configuring URLCC QCI In Charging Action

Use the following configuration to configure URLCC QCI in the Charging Action Configuration mode.

```
configure
   active-charging service service_name
      charging-action charging_action_name
          qos-class-identifier qos_class_identifier
          no qos-class-identifier
          end
```

NOTES:

- **active-charging service** *service_name*: Specifies name of the active charging service. *service_name* must be an alphanumeric string of 1 through 15 characters.
- **charging-action** *charging_action_name* : Creates a charging action. *qos_class_identifier* must be an alphanumeric string of 1 through 63 characters.
- **qos-class-identifier** *qos_class_identifier*: Specifies the QoS Class Identifier. *qos_class_identifier* must be an integer between 1 to 9, 65, 66, 69, 70, 80, 82, and 83.
- **no**: Disables the QoS Class Identifier.

Configuring URLCC QCI in QCI QOS Mapping Table

Use the following configuration to configure URLCC QCI in the QCI QOS Mapping Table.

```
configure
   qci-qos-mapping name
       [ no ] qci qci_value
       end
```

NOTES:

- **qci-qos-mapping** *name*: Specifies the map name. *name* must be an alphanumeric string of 1 through 63 characters.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 65, 66, 69, 70, 80, 82, and 83.

- **no**: Disables the QCI value.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the 5G NSA feature.

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the DCNR feature.

show pgw-service name

The output of this command includes the "DCNR" field to indicate if the DCNR feature is enabled or disabled at P-GW service.

show ims-authorization service name

The output of this command includes the following fields:

Diameter Policy Control:

Supported Features:

- extended-bw-nr

show gtpu statistics

The output of this command includes the following fields:

- Uplink Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink packets.
- Uplink Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink bytes.
- Downlink Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink packets.
- Downlink Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink bytes.
- Packets Discarded — Displays the total number of discarded QCI 80, QCI 82, and QCI 83 packets.
- Bytes Discarded — Displays the total number of discarded QCI 80, QCI 82, and QCI 83 bytes.

show apn statistics all

The output of this command includes the following fields:

4G Bearers Released By Reasons:

Admin disconnect — Displays dedicated bearers released due to administration clear from P-GW for QCI 80, QCI 82, and QCI 83.

- Bearer Active — Displays the total number for QCI 80, QCI 82, and QCI 83 active bearers.
- Bearer setup — Displays the total number for QCI 80, QCI 82, and QCI 83 bearers setup.

- Bearer Released — Displays the total number for QCI 80, QCI 82, and QCI 83 released bearers.
- Bearer Rejected —
- Uplink Bytes Forwarded — Displays the total number for QCI 80, QCI 82, and QCI 83 uplink packets forwarded.
- Uplink pkts forwarded — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink packets forwarded.
- Uplink Bytes dropped — Displays the total number for QCI 80, QCI 82, and QCI 83 uplink bytes forwarded.
- Downlink Bytes forwarded — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink bytes forwarded.
- Uplink pkts dropped — Displays the total number for QCI 80, QCI 82, and QCI 83 uplink packets dropped.
- Downlink Bytes dropped — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink bytes dropped.
- Uplink Bytes dropped(MBR Excd) — Displays the total number for QCI 80, QCI 82, and QCI 83 uplink bytes dropped due to MBR being exceeded.
- Uplink pkts dropped(MBR Excd) — Displays the total number for QCI 80, QCI 82, and QCI 83 uplink packets dropped due to MBR being exceeded.
- Downlink pkts forwarded — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink packets forwarded.
- Downlink pkts dropped — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink packets dropped.
- Downlink Bytes dropped(MBR Excd) — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink bytes dropped due to MBR being exceeded.
- Downlink pkts dropped(MBR Excd) — Displays the total number for QCI 80, QCI 82, and QCI 83 downlink packets dropped due to MBR being exceeded.

show pgw-service statistics all verbose

The output of this command includes the following fields:

Bearers By QoS characteristics:

- Active — Displays the total number of active bearers for QCI 80, QCI 82, and QCI 83.
- Released — Displays the total number of bearers released for QCI 80, QCI 82, and QCI 83.
- Setup — Displays the total number of bearers setup for QCI 80, QCI 82, and QCI 83.

Data Statistics Per PDN-Type:

Uplink:

- Packets — Displays the total number of uplink packets forwarded for QCI 80, QCI 82, and QCI 83.
- Bytes — Displays the total number of uplink bytes forwarded for QCI 80, QCI 82, and QCI 83.

- Dropped Packets — Displays the total number of uplink packets dropped for QCI 80, QCI 82, and QCI 83.
- Dropped Bytes — Displays the total number of uplink bytes dropped for QCI 80, QCI 82, and QCI 83.

Downlink:

- Packets — Displays the total number of downlink packets forwarded for QCI 80, QCI 82, and QCI 83.
- Bytes — Displays the total number of downlink bytes forwarded for QCI 80, QCI 82, and QCI 83.
- Dropped Packets — Displays the total number of downlink packets dropped for QCI 80, QCI 82, and QCI 83.
- Dropped Bytes — Displays the total number of downlink bytes dropped for QCI 80, QCI 82, and QCI 83.

DCNR PDN Statistics:

- Active — The total number of current active P-GW DCNR PDNs.
- Setup — The total number of P-GW PDNs that are setup as a DCNR PDN.
- Released — The total number of P-GW DCNR PDNs released.

show sgw-service statistics all verbose

The output of this command includes the following fields:

Bearers By QoS characteristics:

- Active — Displays the total active EPS Bearers for QCI 80, QCI 82, and QCI 83.
- Released — Displays the total number of EPS Bearers released for QCI 80, QCI 82, and QCI 83.
- Setup — Displays the total number of EPS bearers setup for QCI 80, QCI 82, and QCI 83.
- Modified — Displays the total number of EPS bearers modified for QCI 80, QCI 82, and QCI 83.

Dedicated Bearers Released By Reason:

- P-GW Initiated — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason P-GW initiated on the S-GW.
- S1 Error Indication — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S1 error indication on the S-GW.
- S5 Error Indication — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S5 error indication on the S-GW.
- S4 Error Indication — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S4 error indication on the S-GW.
- S12 Error Indication — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S12 error indication on the S-GW.
- Local — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason local error indication on the S-GW.

- PDN Down — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released due to PDN cleanup on the S-GW.
- Path Failure S1-U — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S1-U path failure on the S-GW.
- Path Failure S5-U — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S5-U path failure on the S-GW.
- Path Failure S5 — Displays the total number of dedicated EPS bearers for QCI 80, QCI 82, and QCI 83 released with the reason S5 path failure on the S-GW.
- Path Failure S11 — Displays the total number of dedicated bearers for QCI 80, QCI 82, and QCI 83 released due to path failure on the S11 interface.
- Path Failure S4-U — Displays the total number of dedicated bearers for QCI 80, QCI 82, and QCI 83 released due to path failure on S4-U interface.
- Path Failure S12 — Displays the total number of dedicated bearers for QCI 80, QCI 82, and QCI 83 released due to path failure on S12 interface.
- Inactivity Timeout — Displays the total number of dedicated bearers for QCI 80, QCI 82, and QCI 83 released due to the inactivity timeout.
- Other — Displays the total number of dedicated bearers for QCI 80, QCI 82, and QCI 83 released due to other reasons.

Data Statistics Per Interface:

S1-U/S11-U/S4-U/S12/S5-U/S8-U Total Data Statistics:

Uplink:

- Packets — Displays the total number of uplink data packets received by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.
- Bytes — Displays the total number of uplink data bytes received by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.
- Dropped Packets — Displays the total number of uplink data packets dropped by the S-GW for a bearer with a QCI 80, QCI 82, and QCI 83.
- Dropped Bytes — Displays the total number of uplink data bytes dropped by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.

Downlink:

- Packets — Displays the total number of downlink data packets received by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.
- Bytes — Displays the total number of downlink data bytes received by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.
- Dropped Packets — Displays the total number of downlink data packets dropped by the S-GW for bearer with QCI 80, QCI 82, and QCI 83.
- Dropped Bytes — Displays the total number of downlink data bytes dropped by the S-GW for a bearer with QCI 80, QCI 82, and QCI 83.

DCNR PDN Statistics:

- Active — The total number of current active S-GW DCNR PDNs.
- Setup — The total number of S-GW PDNs that are setup as a DCNR PDN.
- Released — The total number of S-GW DCNR PDNs released.

show saegw-service statistics all verbose

The output of this command includes the following fields:

Bearers By QoS characteristics:

- Active — Displays the total number of QCI 80, QCI 82, and QCI 83 active bearers.
- Released — Displays the total number of QCI 80, QCI 82, and QCI 83 released bearers.
- Setup — Displays the total number of QCI 80, QCI 82, and QCI 83 bearers setup.

Data Statistics Per PDN-Type:

Uplink:

- Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink packets forwarded.
- Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink bytes forwarded.
- Dropped Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink packets dropped.
- Dropped Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 uplink bytes dropped.

Downlink:

- Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink packets forwarded.
- Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink bytes forwarded.
- Dropped Packets — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink packets dropped.
- Dropped Bytes — Displays the total number of QCI 80, QCI 82, and QCI 83 downlink bytes dropped.

DCNR PDNs:

Colocated PDNs:

- Active — The total number of currently active SAEGW collapsed DCNR PDNs.
- Setup — The total number of SAEGW collapsed PDNs that are setup as a DCNR PDN.
- Released — The total number of SAEGW collapsed DCNR PDNs released.

PGW-Anchor PDNs:

- Active — The total number of currently active P-GW anchored DCNR PDNs.
- Setup — The total number of P-GW anchored PDNs that are setup as a DCNR PDN.
- Released — The total number of P-GW anchored DCNR PDNs that are released.

SGW-Anchor PDNs:

- Active — The total number of current active S-GW anchored DCNR PDNs.
- Setup — The total number of S-GW anchored PDNs that are setup as a DCNR PDN.
- Released — The total number of S-GW anchored DCNR PDNs that are released.

Bulk Statistics

The following statistics are added in support of the 5G NSA feature.

APN Schema

The following 5G NSA feature related bulk statistics are available in the APN schema.

Bulk Statistics	Description
qci80-actbear	The total number of QCI80 active bearers.
qci82-actbear	The total number of QCI82 active bearers.
qci83-actbear	The total number of QCI83 active bearers.
qci80-setupbear	The total number of QCI80 bearers setup.
qci82-setupbear	The total number of QCI82 bearers setup.
qci83-setupbear	The total number of QCI83 bearers setup.
qci80-relbear	The total number of QCI80 released bearers.
qci82-relbear	The total number of QCI82 released bearers.
qci83-relbear	The total number of QCI83 released bearers.
qci80-uplinkpkt-fwd	The total number of QCI80 uplink packets forwarded.
qci82-uplinkpkt-fwd	The total number of QCI82 uplink packets forwarded.
qci83-uplinkpkt-fwd	The total number of QCI83 uplink packets forwarded.
qci80-dwlinkpkt-fwd	The total number of QCI80 downlink packets forwarded.
qci82-dwlinkpkt-fwd	The total number of QCI82 downlink packets forwarded.
qci83-dwlinkpkt-fwd	The total number of QCI83 downlink packets forwarded.
qci80-uplinkbyte-fwd	The total number of QCI80 uplink bytes forwarded.
qci82-uplinkbyte-fwd	The total number of QCI82 uplink bytes forwarded.
qci83-uplinkbyte-fwd	The total number of QCI83 uplink bytes forwarded.

Bulk Statistics	Description
qci80-dwlinkbyte-fwd	The total number of QCI80 downlink bytes forwarded.
qci82-dwlinkbyte-fwd	The total number of QCI82 downlink bytes forwarded.
qci83-dwlinkbyte-fwd	The total number of QCI83 downlink bytes forwarded.
qci80-uplinkpkt-drop	The total number of QCI80 uplink packets dropped.
qci82-uplinkpkt-drop	The total number of QCI82 uplink packets dropped.
qci83-uplinkpkt-drop	The total number of QCI83 uplink packets dropped.
qci80-dwlinkpkt-drop	The total number of QCI80 downlink packets dropped.
qci82-dwlinkpkt-drop	The total number of QCI82 downlink packets dropped.
qci83-dwlinkpkt-drop	The total number of QCI83 downlink packets dropped.
qci80-uplinkbyte-drop	The total number of QCI80 uplink bytes dropped.
qci82-uplinkbyte-drop	The total number of QCI82 uplink bytes dropped.
qci83-uplinkbyte-drop	The total number of QCI83 uplink bytes dropped.
qci80-dwlinkbyte-drop	The total number of QCI80 downlink bytes dropped.
qci82-dwlinkbyte-drop	The total number of QCI82 downlink bytes dropped.
qci83-dwlinkbyte-drop	The total number of QCI83 downlink bytes dropped.
qci80-uplinkpkt-drop-mbrexcd	The total number of QCI80 uplink packets dropped due to MBR being exceeded.
qci82-uplinkpkt-drop-mbrexcd	The total number of QCI82 uplink packets dropped due to MBR being exceeded.
qci83-uplinkpkt-drop-mbrexcd	The total number of QCI83 uplink packets dropped due to MBR being exceeded.
qci80-dwlinkpkt-drop-mbrexcd	The total number of QCI80 downlink packets dropped due to MBR being exceeded.
qci82-dwlinkpkt-drop-mbrexcd	The total number of QCI82 downlink packets dropped due to MBR being exceeded.
qci83-dwlinkpkt-drop-mbrexcd	The total number of QCI83 downlink packets dropped due to MBR being exceeded.
qci80-uplinkbyte-drop-mbrexcd	The total number of QCI80 uplink bytes dropped due to MBR being exceeded.
qci82-uplinkbyte-drop-mbrexcd	The total number of QCI82 uplink bytes dropped due to MBR being exceeded.

Bulk Statistics	Description
qci83-uplinkbyte-drop-mbrexcd	The total number of QCI83 uplink bytes dropped due to MBR being exceeded.
qci80-dwlinkbyte-drop-mbrexcd	The total number of QCI80 uplink bytes dropped due to MBR being exceeded.
qci82-dwlinkbyte-drop-mbrexcd	The total number of QCI82 uplink bytes dropped due to MBR being exceeded.
qci83-dwlinkbyte-drop-mbrexcd	The total number of QCI83 uplink bytes dropped due to MBR being exceeded.
qci80-rejbearer	The total number of QCI80 rejected bearers.
qci82-rejbearer	The total number of QCI82 rejected bearers.
qci83-rejbearer	The total number of QCI83 rejected bearers.
sessstat-bearrel-ded-admin-clear-qci80	The total number dedicated bearers released due to admin clear from P-GW for QCI80.
sessstat-bearrel-ded-admin-clear-qci82	The total number dedicated bearers released due to admin clear from P-GW for QCI82.
sessstat-bearrel-ded-admin-clear-qci83	The total number dedicated bearers released due to admin clear from P-GW for QCI83.

P-GW Schema

The following 5G NSA feature related bulk statistics available in the P-GW schema.

Bulk Statistics	Description
pgw-anchor-pdns-dcnr-current-active	The total number of currently active P-GW anchored DCNR PDNs.
pgw-anchor-pdns-dcnr-cumulative-activated	The total number of P-GW anchored PDNs that are setup as DCNR PDN.
pgw-anchor-pdns-dcnr-cumulative-deactivated	The total number of P-GW anchored PDNs that were either released or degrades to a non-DNCR PDN.
sessstat-pdn-dcnr-current-active	Session Statistics - DCNR PDN-Type Statistics - Current Active.
sessstat-pdn-dcnr-cumulative-activated	Session Statistics - DCNR PDN-Type Statistics - Cumulative PDNs Activated.
sessstat-pdn-dcnr-cumulative-deactivated	Session Statistics - DCNR PDN-Type Statistics - Cumulative PDNs Deactivated.

SAEGW Schema

The following 5G NSA feature related bulk statistics available in the SAEGW schema.

Bulk Statistics	Description
saegw-collocated-pdns-dcnr-current-active	The total number of currently active SAEGW collapsed DCNR PDNs.
saegw-collocated-pdns-dcnr-cumulative-activated	The total number of SAEGW collapsed PDNs that are setup as a DCNR PDN.
saegw-collocated-pdns-dcnr-cumulative-deactivated	The total number of SAEGW collapsed DCNR PDNs released.

S-GW Schema

The following 5G NSA feature related bulk statistics available in the S-GW schema.

Bulk Statistics	Description
sessstat-pdn-dcnr-current-active	The total number of currently active S-GW DCNR PDNs.
sessstat-pdn-dcnr-cumulative-activated	The total number of S-GW PDNs that are setup as a DCNR PDN.
sessstat-pdn-dcnr-cumulative-deactivated	The total number of S-GW DCNR PDNs released.
sgw-anchor-pdns-dcnr-current-active	The total number of currently active S-GW anchored DCNR PDNs.
sgw-anchor-pdns-dcnr-cumulative-activated	The total number of S-GW anchored PDNs that are setup as a DCNR PDN.
sgw-anchor-pdns-dcnr-cumulative-deactivated	The total number of S-GW anchored DCNR PDNs that are released.

System Schema

The following 5G NSA feature related bulk statistics are available in the System schema.

Bulk Statistics	Description
sess-bearerdur-5sec-qci80	The current number of bearer sessions with a duration of 5 seconds and having a QCI of 80.
sess-bearerdur-5sec-qci82	The current number of bearer sessions with a duration of 5 seconds and having a QCI of 82.
sess-bearerdur-5sec-qci83	The current number of bearer sessions with a duration of 5 seconds and having a QCI of 83.

Bulk Statistics	Description
sess-bearerdur-10sec-qci80	The current number of bearer sessions with a duration of 10 seconds and having a QCI of 80.
sess-bearerdur-10sec-qci82	The current number of bearer sessions with a duration of 10 seconds and having a QCI of 82.
sess-bearerdur-10sec-qci83	The current number of bearer sessions with a duration of 10 seconds and having a QCI of 83.
sess-bearerdur-30sec-qci80	The current number of bearer sessions with a duration of 30 seconds and having a QCI of 80.
sess-bearerdur-30sec-qci82	The current number of bearer sessions with a duration of 30 seconds and having a QCI of 82.
sess-bearerdur-30sec-qci83	The current number of bearer sessions with a duration of 30 seconds and having a QCI of 83.
sess-bearerdur-1min-qci80	The current number of bearer sessions with a duration of 1 minute and having a QCI of 80.
sess-bearerdur-1min-qci82	The current number of bearer sessions with a duration of 1 minute and having a QCI of 82.
sess-bearerdur-1min-qci83	The current number of bearer sessions with a duration of 1 minute and having a QCI of 83.
sess-bearerdur-2min-qci80	The current number of bearer sessions with a duration of 2 minutes and having a QCI of 80.
sess-bearerdur-2min-qci82	The current number of bearer sessions with a duration of 2 minutes and having a QCI of 82.
sess-bearerdur-2min-qci83	The current number of bearer sessions with a duration of 2 minutes and having a QCI of 83.
sess-bearerdur-5min-qci80	The current number of bearer sessions with a duration of 5 minutes and having a QCI of 80.
sess-bearerdur-5min-qci82	The current number of bearer sessions with a duration of 5 minutes and having a QCI of 82.
sess-bearerdur-5min-qci83	The current number of bearer sessions with a duration of 5 minutes and having a QCI of 83.
sess-bearerdur-15min-qci80	The current number of bearer sessions with a duration of 15 minutes and having a QCI of 80.
sess-bearerdur-15min-qci82	The current number of bearer sessions with a duration of 15 minutes and having a QCI of 82.
sess-bearerdur-15min-qci83	The current number of bearer sessions with a duration of 15 minutes and having a QCI of 83.

Bulk Statistics	Description
sess-bearerdur-30min-qci80	The current number of bearer sessions with a duration of 30 minutes and having a QCI of 80.
sess-bearerdur-30min-qci82	The current number of bearer sessions with a duration of 30 minutes and having a QCI of 82.
sess-bearerdur-30min-qci83	The current number of bearer sessions with a duration of 30 minutes and having a QCI of 83.
sess-bearerdur-1hr-qci80	The current number of bearer sessions with a duration of 1 hour and having a QCI of 80.
sess-bearerdur-1hr-qci82	The current number of bearer sessions with a duration of 1 hour and having a QCI of 82.
sess-bearerdur-1hr-qci83	The current number of bearer sessions with a duration of 1 hour and having a QCI of 83.
sess-bearerdur-4hr-qci80	The current number of bearer sessions with a duration of 4 hours and having a QCI of 80.
sess-bearerdur-4hr-qci82	The current number of bearer sessions with a duration of 4 hours and having a QCI of 82.
sess-bearerdur-4hr-qci83	The current number of bearer sessions with a duration of 4 hours and having a QCI of 83.
sess-bearerdur-12hr-qci80	The current number of bearer sessions with a duration of 12 hours and having a QCI of 80.
sess-bearerdur-12hr-qci82	The current number of bearer sessions with a duration of 12 hours and having a QCI of 82.
sess-bearerdur-12hr-qci83	The current number of bearer sessions with a duration of 12 hours and having a QCI of 83.
sess-bearerdur-24hr-qci80	The current number of bearer sessions with a duration of 24 hours and having a QCI of 80.
sess-bearerdur-24hr-qci82	The current number of bearer sessions with a duration of 24 hours and having a QCI of 82.
sess-bearerdur-24hr-qci83	The current number of bearer sessions with a duration of 24 hours and having a QCI of 83.
sess-bearerdur-over24hr-qci80	The current number of bearer sessions with a duration of over 24 hours and having a QCI of 80.
sess-bearerdur-over24hr-qci82	The current number of bearer sessions with a duration of over 24 hours and having a QCI of 82.
sess-bearerdur-over24hr-qci83	The current number of bearer sessions with a duration of over 24 hours and having a QCI of 83.

Bulk Statistics	Description
sess-bearerdur-2day-qci80	The current number of bearer sessions with a duration of 2 days and having a QCI of 80.
sess-bearerdur-2day-qci82	The current number of bearer sessions with a duration of 2 days and having a QCI of 82.
sess-bearerdur-2day-qci83	The current number of bearer sessions with a duration of 2 days and having a QCI of 83.
sess-bearerdur-4day-qci80	The current number of bearer sessions with a duration of 4 days and having a QCI of 80.
sess-bearerdur-4day-qci82	The current number of bearer sessions with a duration of 4 days and having a QCI of 82.
sess-bearerdur-4day-qci83	The current number of bearer sessions with a duration of 4 days and having a QCI of 83.
sess-bearerdur-5day-qci80	The current number of bearer sessions with a duration of 5 days and having a QCI of 80.
sess-bearerdur-5day-qci82	The current number of bearer sessions with a duration of 5 days and having a QCI of 82.
sess-bearerdur-5day-qci83	The current number of bearer sessions with a duration of 5 days and having a QCI of 83.

CHAPTER 6

Automatic Password Generator (APG) Application

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	UGP
Feature Default	Enabled - Always On
Related Features in this Release	Not Applicable
Related Documentation	- *Ultra Services Platform Deployment Automation Guide* - *UEM-based VNF Deployment Guide*

Revision History

Revision Details	Release
First introduced.	6.5

Feature Description

UAS and UEM use a new password generation tool i.e. APG application to generate random and strong passwords for the user accounts in Ubuntu server.

Use the following commands on UAS or UEM component console to generate password according to the predefined constraints:

```
# apg -a 0 -M SNCL -t -E !
```

or

```
# apg -a 1 -M SNCL -t -E !
```

For more information on the password requirements, see the *Cisco Ultra Services Platform Deployment Automation Guide*.

CHAPTER 7

Automatic Scale-out Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required
Related Features in this Release	Not Applicable
Related Documentation	- *UEM-based VNF Deployment Guide* - *Ultra M Solutions Guide* - *Ultra Services Platform Deployment Automation Guide*

Revision History

Revision Details	**Release**
First introduced.	6.5

Feature Description

Important This feature is not fully qualified and is made available only for testing purposes. For more information, contact your Cisco Accounts representative.

UEM already supports manual scale-out (addition) of the SF VMs within your VNF deployment. For detailed information on manual scaling feature, see the *Cisco Ultra Services Platform Deployment Automation Guide*.

For automatic scale-out, UEM triggers the function based on certain predefined constraints. Currently, auto scale-out is supported based on average CPU / average memory of the active SF cards. One of these two constraints must be configured as part of auto-scaling configuration.

Important Auto-scaling is an optional feature and is triggered only when **auto-scaling-policy** element is configured in *vnfd.xml*.

Along with the day-0 configuration in UEM, auto-scaling policy configuration must be included in *vnfd.xml* for enabling Auto-scaling feature. The scaling related configuration data is present for each VNFD in the specified format in the *vnfd.xml* file.

For detailed information on the Automatic Scale-out feature, see the *UEM-based VNF Deployment Guide*.

CHAPTER 8

Backward Compatibility Restoration by QoS-Information AVP

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	GGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

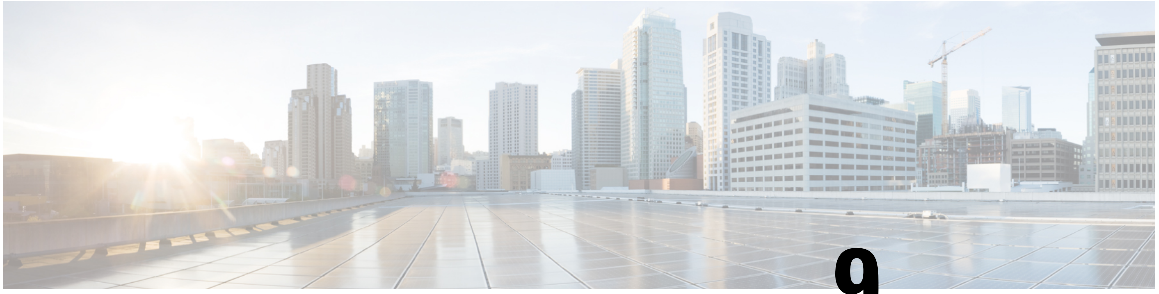
Revision Details	Release
With this release, backward compatibility is restored by sending the QoS-Information AVP only when the Extended-BW for APN-AMBR, MBR, or GBR parameter is available for dcca-custom1, dcca-custom7, and dcca-custom8 Diameter dictionaries.	21.11.2
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: In earlier releases, OCS failed to decode the QoS-Information AVP, which was included in Gy records, for dcca-custom1, dcca-custom7, and dcca-custom8 Diameter dictionaries.

New Behavior: In 21.11.2 and later releases, QoS-Information AVP is included only if Extended-BW is available for MBR, GBR, or AMBR parameter in Gy records for the dcca-custom1, dcca-custom7, and dcca-custom8 Diameter dictionaries.

Customer Impact: None



CHAPTER 9

CLI Support for P-GW to include AVPs in CCR-U Messages

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
This Behavior Change was introduced in 21.4.14. With this release, CLI support for P-GW to include AVPs in CCR-U messages is also applicable to 21.11.3	21.11.3

Revision Details	Release
This Behavior Change was introduced in 21.4.14. With this release, CLI support for P-GW to include AVPs in CCR-U messages is also applicable to 21.8.10	21.8.10
For Wi-Fi calls, when P-GW receives the AVPs - UDP-SOURCE-PORT and UE-Local-IP-Address, in the CB Rsp or UB Rsp or DB Rsp message, it sends these AVPs in the CCR-U messages towards the PCRF even if there are no changes in the AVP values.	21.4 .14
First introduced.	Pre 21.2

Feature Changes

For Wi-Fi calls, when P-GW receives the AVPs - UDP-SOURCE-PORT and UE-Local-IP-Address, in the CB Rsp or UB Rsp or DB Rsp message, it sends these AVPs in the CCR-U messages towards the PCRF even if there are no changes in the AVP values.

To support the above functionality, a new keyword - **ue-ip-udp-port**, is added to the **diameter encode-supported-features command** in the *Policy Control Configuration Mode*. By default, this keyword is disabled.

Previous Behavior: For Wi-Fi calls, if P-GW receives the AVPs - UDP-SOURCE-PORT and/or UE-Local-IP-Address in the CB Rsp, UB Rsp or DB Rsp, it checks for a change in the AVP values with the value received earlier. If there are no changes in the AVP values, then the P-GW does not send these AVPs in the CCR-U message towards PCRF. Otherwise, the P-GW only sends the UE-Local-IP-Address IE in the CCR-U message towards PCRF.

New Behavior: For Wi-Fi calls, when the CLI is configured with the keyword **ue-ip-udp-port** enabled, the P-GW sends the AVPs - UDP-SOURCE-PORT and UE-Local-IP-Address in the CCR-U message towards PCRF.

Note If P-GW does not receive the above mentioned AVPs in the CB Rsp, UB Rsp or DB Rsp message, it does not send the AVPs in the CCR-U message towards PCRF.

Command Changes

diameter encode-supported-features

In the *Policy Control Configuration* mode, the **diameter encode-supported-features** command's **netloc-untrusted-wlan** is supported with the **ue-ip-udp-port** keyword which facilitates the P-GW to include the UDP-SOURCE-PORT and UE-Local-IP-Address AVPs in the CCR-U message sent towards PCRF.

To enable this functionality, use the following configuration:

```
configure
   context context_name
```

```
     ims-auth-service service_name
        policy-control
           diameter encode-supported-features netloc-untrusted-wlan
ue-ip-udp-port
           no diameter encode-supported-features
           end
```

NOTES:

- The **ue-ip-udp-port** keyword is displayed only if **netloc-untrusted-wlan** is configured.
- **ue-ip-udp-port**: Sends the UDP-SOURCE-PORT and UE-Local-IP-Address AVPs in CCR-U messages for Wi-Fi calls even though the AVP values remain unchanged.
- **no**: Disables this functionality at an IMS-Auth service level.

Performance Indicator Changes

show ims-authorization service all verbose

The output of this command includes the following fields in support of this functionality:

- Supported Features
    - netloc-untrusted-wlan ue-ip-udp-port

CHAPTER 10

Controlled ORBS Service Initialization

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• Command Line Interface Reference • Statistics and Counters Reference

Revision History

Revision Details	Release
With this release, ORBS services initialize only when configured in the configuration file.	21.11
First introduced.	Pre 21.2

Feature Changes

In certain deployment scenarios, Object Request Broker Server (ORBS) services were initializing automatically even when the services were not configured. This release provides a solution to the issue by disabling nonessential services and closing unused ports, thereby enhancing product security.

Previous Behavior: In releases earlier to 21.11, ORBS services initialized without prior configuration.

New Behavior: Now, ORBS services initialize only when configured.

Customer Impact: If the Object Request Broker Element Management (ORBEM) is configured in the configuration file, ORBS services initialize as expected.

If ORBEM is not configured in the configuration file, ORBS services do not initialize.

CHAPTER 11

Collision Handling for Path Update during Bearer Creation

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled - Always on
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	**Release**
Collision Handling for Path-Update during Bearer Creation support added.	21.5.28
Collision Handling for Path-Update during Bearer Creation support added.	21.5.26
Collision Handling for Path-Update during Bearer Creation support added.	21.11.13
Collision Handling for Path-Update during Bearer Creation support added.	12.12.15
First introduced.	21.14

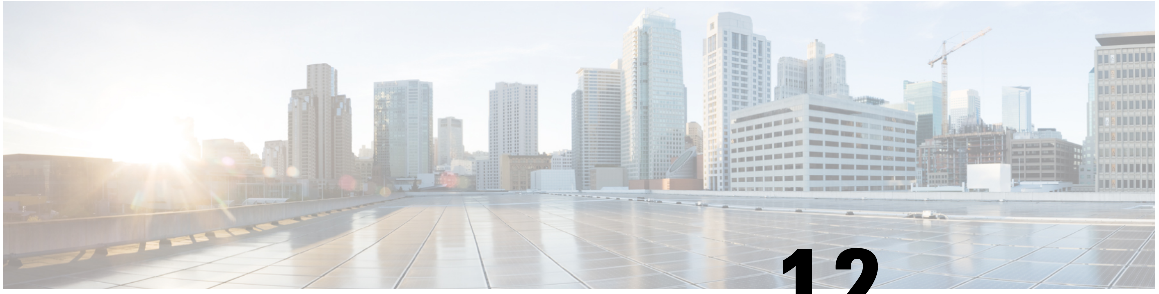
Feature Description

MME supports processing of NSA path-update procedure under the following collision scenarios:

- Collision between path-update and one or more dedicated-bearer creation initiated by network.
- Collision between path-update and IM-EXIT procedure is in progress.

As part of the above collision handling, MME handles the ERAB-Setup response received from eNB as follows:

- MME processes the ERAB-SETUP response received with cause "Interaction-With-Other-Procedures" from eNB and retries the ERAB-Setup again towards eNB.
- MME processes the ERAB-SETUP response received when Create-Bearer procedure is in suspended state due to path-update in progress.
- MME retries the ERAB-SETUP towards eNB after the successful completion of path-update procedure.



CHAPTER 12

Debug Console Swap

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• VPC-DI • VPC-SI
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Command Line Interface Reference

Revision History

Revision Details	Release
With this release, the debug event logs are configured to be sent from serial1 console to serial0.	21.11.3
First introduced.	Pre 21.2

Feature Changes

In the current deployment of StarOS, debug event logs are currently sent to the first serial port (serial1) on the console. On Red Hat OpenStack (OSP), this console is configured by default, therefore, post-deployment scripts are executed to configure debug event log collection. The execution of post-deployment of scripts becomes more complicated on Cisco Virtualized Infrastructure Manager (CVIM) and on OSP 13 where OSP functionality is containerized. To address this, a new keyword **first-console** is added to the existing **logging** CLI command, which enables or disables debug event logs to be sent from serial1 console to serial0.

Note This CLI does not enable or disable system logs such as crash logs, system printed logs, and so on, which are always enabled.

Previous Behavior: In releases earlier to 21.12, debug event logs were sent to serial1 console.

New Behavior: Now, on the first serial port (serial0) a debug console is seen for event logs. This console captures the critical log and all the logs that were configured using the **logging runtime** CLI command.

Note that on a VPC-DI that has a CF and SF card, the CF card on the first serial port is configured as the debug console. The second serial port is configured as the CLI console.

Note The CF card on the VPC-DI and VPC-SI can be configured as the VGA, which also provides the CLI console.

On the SF card, the first serial port is configured as the debug console. The second serial port cannot be configured as the CLI console because there is no support for this console on the SF card.

Customer Impact:

For existing deployments: For VPC-DI systems, the console swap occurs when the build with the fix is loaded. For VPC-SI systems, the console swap occurs after loading the build with the fix and then configured with a new boot priority.

For new deployments: The console swap occurs when the image with the fix is deployed.

Command Changes

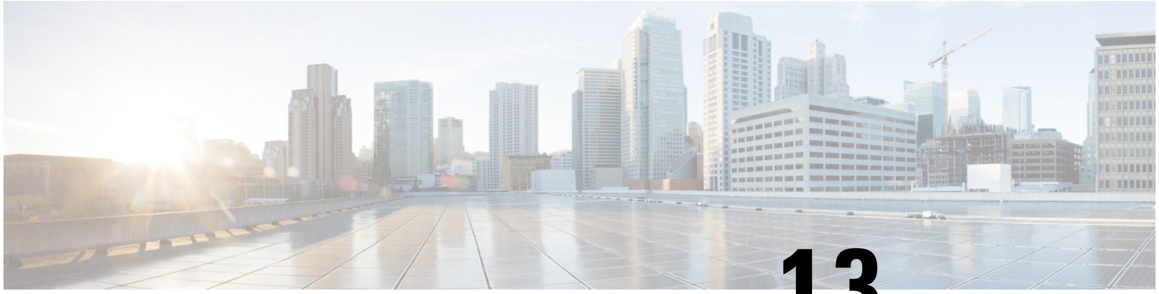
logging

The above CLI command is enhanced to include the **first-console** keyword, which is used to enable or disable the first serial port as the debug console for event log collection. This command is configured in the Context Configuration Mode.

```
configure
   [ no ] logging first-console
   end
```

NOTES:

- **no**: Disables the first serial port as the debug console for event log collection.
- Note that this CLI does not enable or disable system logs such as crash logs, system printed logs, and so on, which are always enabled.
- By default, this CLI is enabled.



CHAPTER 13

Deprecation of Manual Scaling

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UAS
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide*

Revision History

Revision Details	**Release**
The support for manual scale-in and scale-out functionality has been deprecated in this release.	6.0 through 6.14
First introduced	6.0

Feature Changes

Previous Behavior: In previous releases, the Service Function (SF) scaling (including the manual scale-in and scale-out) feature was supported.

New Behavior: In this release, the manual scale-out and scale-in functionalities have been deprecated. For more information, contact your Cisco account representative.

CHAPTER 14

ERAB Setup Retry Handling

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**
Retry ERAB Setup Request Support added	21.5.26
Retry ERAB Setup Request Support added.	21.11.13

Revision Details	Release
Retry ERAB Setup Request Support added.	12.12.15
Retry ERAB Setup Request Support added.	21.15
Retry ERAB Setup Request Support added.	21.14.3
First introduced.	21.14

Feature Changes

MME delays re-sending the "ERAB Setup Request" message if failure response is received with cause "Interaction with other procedure."

Previous Behavior: The MME re-transmits the "E-RAB Setup Request" immediately on the reception of "E-RAB Setup Response" with cause "interaction with other procedure."

New Behavior: MME will start Timer (Tm) after the reception of "E-RAB Setup Response" with cause "Interaction with other procedure." Once the timer expires, MME re-transmits the "E-RAB Setup Request." MME supports the maximum retry count. This behavior is CLI controlled.

Command Changes

erab-setup-rsp-fail retry-timer

Use the following configuration to configure the ERAB Setup retry handling:

```
configure
   context context_name
      mme-service service_name
         policy erab-setup-rsp-fail retry-timer retry_timer  max-retries
max_retries
         { default | no } policy erab-setup-rsp-fail retry-timer
         end
```

NOTES:

- **no** Disables the retry timer mechanism.
- **default** Restores the default value to existing behavior by disabling the retry timer mechanism.
- **policy** Specifies the user-defined policies like idle mode detach behavior and so on.
- **erab-setup-rsp-fail** Sets the handling for ERAB-SETUP-RESPONSE failure message.
- **retry-timer** *retry_timer* Configures the retry timer for ERAB Setup Procedure. *retry_timer* must be an integer value in the range of 1-15.
- **max-retries** *max_retries* Configures the maximum retry limit for ERAB Setup Procedure. *max_retries* must be an integer value in the range of 1-10.

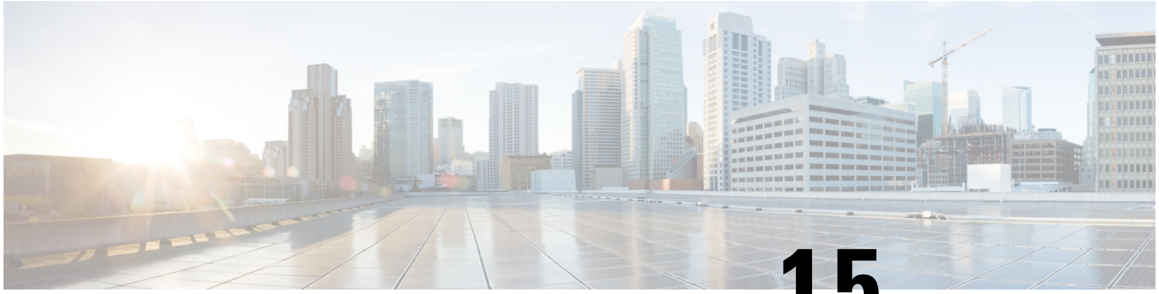
Performance Indicator Changes

show mme-service name <mme_svc_name>

The output of this command includes the following fields:

- Policy ERAB Setup Procedure
  - ERAB Setup retry timer - Retry timer for ERAB Setup Procedure
  - ERAB Setup maximum retry limit - Maximum retry limit for ERAB Setup Procedure

Important ERAB Setup Retry Handling is applicable only for Dedicated Bearer Creation.



CHAPTER 15

GB Manager Queue Handling

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision Details	**Release**
Introduced to 21.12 release.	21.12.13
Introduced to 21.11 release.	21.11.9
First introduced.	21.6.b23

Feature Description

Important This feature is customer-specific.

After handling the messages in the queue, GB manager exits the loop to handle the heartbeat.

Previous Behavior: GB manager handles all packets in the queue, it will not handle other events until the queue is empty.

New Behavior: GB manager handles configured number of packets in the queue and it handles other events if they exist.

Important For configuration related information of this feature, contact your Cisco Account representative.

CHAPTER 16

Handling of APN Configuration in ISDR from HSS

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled – Always-on
Related Changes in This Release	Not applicable
Related Documentation	*MME Administration Guide*

Revision History

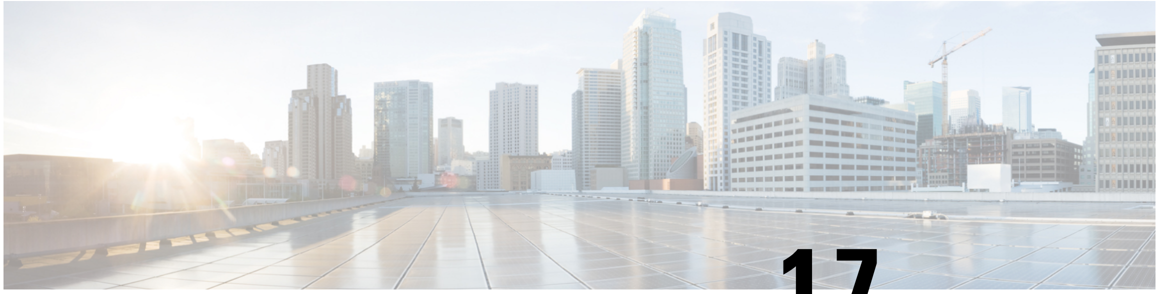
Revision Details	**Release**
Handling of APN Configuration in ISDR from HSS support added.	12.12.15
Handling of APN Configuration in ISDR from HSS support added.	21.11.9
First introduced.	21.5.19

Feature Changes

APN configuration handling received in HSS ISDR message is modified in compliance with 3GPP TS 29.272.

Previous Behavior: If All APN configurations included indicator value is set to "MODIFIED/ADDED_APN_CONFIGURATIONS_INCLUDED" then the APN configuration data is merged in the MME DB record.

New Behavior: If all APN configurations include indicator value is set to "MODIFIED/ADDED_APN_CONFIGURATIONS_INCLUDED" then the APN configuration data is replaced in the MME DB record.



CHAPTER 17

Handling NPLI Requests

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
This Behavior Change was introduced in 21.4.15. With this release, Handling NPLI Requests is also applicable in 21.11.3	21.11.3
This Behavior Change was introduced in 21.4.15. With this release, Handling NPLI Requests is also applicable in 21.8.10	21.8.10
The Update Bearer procedure on default bearer is generated with PCRF requesting for the NPLI Information even if the CLI **no policy-control update-default-bearer** is configured.	21.4 .15

Revision Details	Release
First introduced.	Pre 21.2

Feature Changes

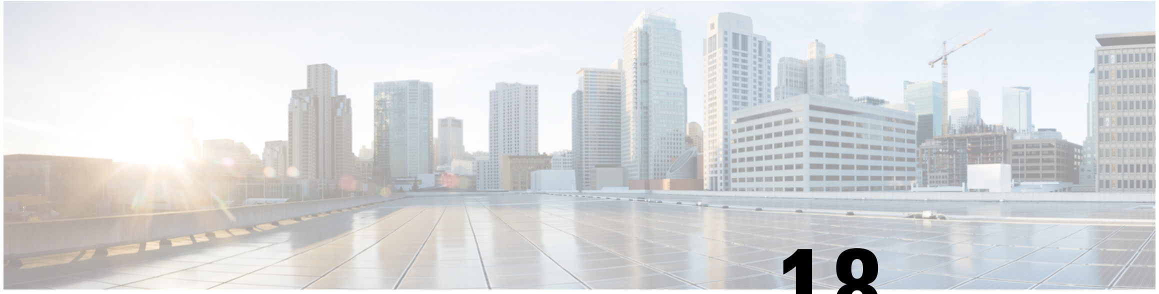
The Update Bearer procedure on default bearer is generated with PCRF requesting for the NPLI Information even if the CLI **no policy-control update-default-bearer** is configured.

Previous Behavior: The Update Bearer procedure on default bearer was not generated to retrieve the UE location information for Bearer Independent NPLI procedures when NPLI requests were received on the PCEF from the PCRF.

With reference to 3GPP 23.842 Section 6.4.4 “Bearer Independent NPLI fetch by P-CSCF,” the P-GW must generate Update Bearer Request to retrieve the current location of a User. This feature was not achievable when the CLI **no policy-control update-default-bearer** was configured.

New Behavior: A functionality has been added to handle NPLI requests received on PCEF (P-GW) from the PCRF. The Update Bearer procedure on default bearer is now generated even if the CLI **no policy-control update-default-bearer**is configured.

Note The functionality is restricted to CCA-U and RAR messages. It is not included for CCR-I messages because the functionality is considered only for a default bearer setup and not a mid-call User location fetch from PCRF. Calls coming from a 3G network to a 4G network, CCA-U for RAT_TYPE acknowledgment NPLI request will not be considered.



CHAPTER 18

Monitor Process Listing

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
First introduced.	21.11

Feature Description

The Monitor Process Listing feature supports the following functionalities:

- Viewing the running processes to check and detect intrusion.
- Checking the software to detect if it is tamper-proof.
- Enabling security decisions.

The newly introduced CLI command, **show process status**, supports this feature.

Monitoring and Troubleshooting

This section provides information regarding the CLI command available in support of monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

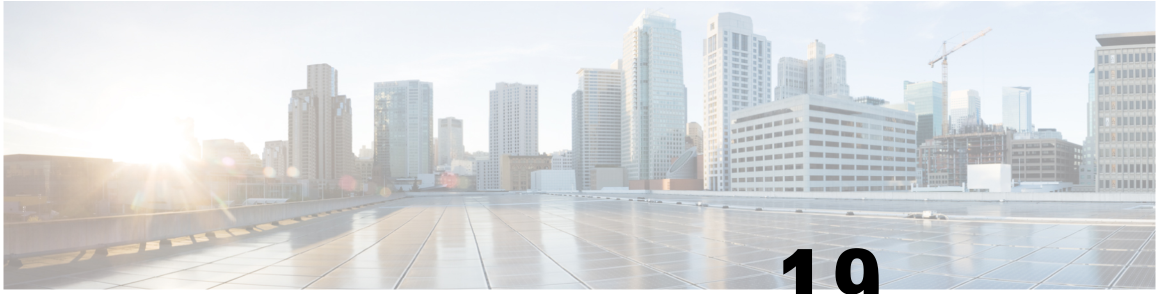
This section provides information regarding the show command and/or its output in support of this feature.

show process status

The output of this CLI command now includes the following fields in support of this feature:

- card - cpu
  - USER
  - PID
  - PPID
  - STARTED
  - %CPU
  - %MEM
  - COMMAND

Note Only the Security Administrator can run this command.



CHAPTER 19

NAS Signaling Security

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
The support for EEA3 and EIA3 NAS encryption/integrity algorithms is added.	21.11.3
First introduced.	Pre 21.2

Feature Description

The Non-Access Stratum (NAS) Signaling Security feature provides integrity protection and encryption of NAS signaling. The MME works as the termination point in the network for ciphering/integrity protection of NAS signaling and handles the security key management.

The NAS security association is between the UE and the MME. The MME uses the NAS Security Mode Command procedure to securely deliver NAS signaling messages between the UE and MME.

The following two standardized algorithms are supported for the radio interface in the LTE network:

- EEA: EPS Encryption Algorithm
- EIA: EPS Integrity Algorithm

The first set of encryption and integrity algorithm, 128-EEA1 and 128-EIA1, is based on the stream cipher SNOW 3G, and inherited from the UMTS network. The second set, 128-EEA2 and 128-EIA2, is based on the block cipher AES (Advanced Encryption Standard). The third set, 128-EEA3 and 128-EIA3, is based on a core stream cipher algorithm named ZUC.

Configuring NAS Signaling Security

This section describes how to configure the NAS Signaling Security feature.

Configuring LTE Encryption Algorithm in Call Control Profile

Use the following configuration to configure the precedence for LTE encryption algorithms to use for security procedures in the call control profile.

```
configure
  call-control-profile profile_name
    encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2
 | 128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 }
] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4
 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
    remove encryption-algorithm-lte
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **priority1**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 1.

- **priority2**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 2.
- **priority3**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 3.
- **priority4**: Specifies the preference of encryption algorithm for security procedures on this call control profile as priority 4.
- **128-eea0**: Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea3**: Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.
- **remove**: Deletes the priorities definition from the call control profile configuration.
- All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Configuring LTE Encryption Algorithm in MME Service

Use the following configuration to configure the precedence for LTE encryption algorithms to use for security procedures in the MME service.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

```
configure
  context context_name
    mme-service service_name
     encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2
 | 128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 }
] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4
 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
      default encryption-algorithm-lte
      end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.

- **priority1**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 1.
- **priority2**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 2.
- **priority3**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 3.
- **priority4**: Specifies the preference of encryption algorithm for security procedures on this MME service as priority 4.
- **128-eea0**: Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
- **128-eea3**: Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.
- **default**: Sets the default LTE encryption algorithm for security procedures with configured priority value. The lowest value has the highest preference.

  The default configuration of LTE encryption algorithm is:

  - priority1 with 128-eea0 encryption algorithm
  - priority2 with 128-eea1 encryption algorithm
  - priority3 with 128-eea2 encryption algorithm

Configuring LTE Integrity Algorithm in Call Control Profile

Use the following configuration to configure the precedence of LTE integrity algorithms to use for security procedures in the call control profile.

```
configure
  call-control-profile profile_name
    integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2
| 128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
 [ priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4
 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
    remove integrity-algorithm-lte
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **priority1**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

- **priority2**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.
- **priority3**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.
- **priority4**: Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.
- **128-eia0**: Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia3**: Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.
- **remove**: Deletes the priorities definition from the call control profile configuration.
- All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Configuring LTE Integrity Algorithm in MME Service

Use the following configuration to configure the precedence of LTE integrity algorithms to use for security procedures in the MME service.

By default, the integrity algorithm is enabled on MME service and cannot be disabled.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

```
configure
   context context_name
      mme-service service_name
        integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2
 | 128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 }
] [ priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4
 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
         default integrity-algorithm-lte
         end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.
- **priority1**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.
- **priority2**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.
- **priority3**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.
- **priority4**: Specifies the preference of integrity algorithm for security procedures on this MME service as priority 4.
- **128-eia0**: Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia1**: Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia2**: Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.
- **128-eia3**: Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.
- **default**: Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. The default configuration of LTE integrity algorithm is:

  The default configuration of LTE integrity algorithm is:

  - priority1 with 128-eia0 integrity algorithm
  - priority2 with 128-eia1 integrity algorithm
  - priority3 with 128-eia2 integrity algorithm

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the NAS Signaling Security feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the NAS Signaling Security feature.

show call-control-profile full all

The output of this command includes the following fields:

- Order of Preference for Integrity Algorithm is — The integrity algorithm that receives the first priority.

- Order of Preference for Encryption Algorithm is — The encryption algorithm that receives the first priority.
- Order of Preference for Gprs Ciphering Algorithm is — The GPRS ciphering algorithm that receives the first priority.
- Order of Preference for LTE(MME) Encryption Algorithm is — Displays the configured priorities and the LTE encryption algorithm applied for security procedures.
- Order of Preference for LTE(MME) Integrity Algorithm is — Displays the configured priorities and the LTE integrity algorithm applied for security procedures.

show mme-service all

The output of this command includes the following fields:

- Encryption Algorithms — Displays the priority and the encryption algorithm applied for security procedures through the MME service.
  - **Priority**: The priority set for the applied encryption algorithm. The least value has the highest preference.

    In releases prior to 21.11.3: Possible priority values are between 1 to 3.

    In 21.11.3 and later releases: Possible priority values are between 1 to 4.
  - **Algorithm**: The applied encryption algorithm. Possible algorithms are:
    - **128-eea0**: Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures. This is the default encryption algorithm applicable for security procedures.
    - **128-eea1**: SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures.
    - **128-eea2**: Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.
    - **128-eea3**: ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.
- Integrity Algorithms — Displays the priority and the integrity algorithm applied for security procedures through the MME service.
  - **Priority**: The priority set for the applied integrity algorithm. The least value has the highest preference.

    In releases prior to 21.11.3: Possible priority values are between 1 to 3.

    In 21.11.3 and later releases: Possible priority values are between 1 to 4.
  - **Algorithm**: The applied encryption algorithm. Possible algorithms are:
    - **128-eia0**: Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.
    - **128-eia1**: SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures.

- **128-eia2**: Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE encryption as the integrity algorithm for security procedures. This is the default encryption algorithm applicable for security procedures.
- **128-eia3**: ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.

CHAPTER 20

NAS Notification for SRVCC Cancellation due to TAU Request

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled –Always on
Related Changes in This Release	Not applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	**Release**
In this release, MME supports NAS notification to reestablish IMS for SRVCC Cancellation.	21.11.16
In this release, MME supports NAS notification to reestablish IMS for SRVCC Cancellation.	21.5.26

Feature Changes

Previous Behavior: MME does not send NAS Notification to reestablish IP Multimedia Subsystem (IMS) for SRVCC Cancellation due to TAU request even after MSC sends PS_TO_CS_CANCELLATION_ACK with STI flag set.

New Behavior: MME sends NAS notification to reestablish IMS for SRVCC Cancellation due to TAU request. This notification is sent irrespective of receiving PS_TO_CS_CANCELLATION_ACK with STI flag set, which is received from MSC.

CHAPTER 21

New Attribute in P-GW CDR for Custom GTPP Dictionary

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on (for customer-specific GTPP dictionary)
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	**Release**
In this release, new 5G NSA attributes are included in customer-specific P-GW GTPP dictionary.	21.11.3
First introduced.	Pre 21.2

Feature Changes

To support 5G NSA NR usage reporting functionality, Cisco has introduced additional containers for secondary RAT usage reports in P-GW CDR for a customer-specific GTPP dictionary.

Important This feature is customer-specific, requiring a custom GTPP dictionary. For more information, contact your Cisco Account representative.

The following fields are now included in P-GW CDR for a custom GTPP dictionary.

Field	Tag Number	Category	Description	Format	Size (in bytes)	ASN1 Code
List of RAN Secondary RAT Usage Reports	73	OC	This field includes one or more containers reported from the RAN for a secondary RAT.	Sequence of RAN Secondary RAT Usage Report	Variable	0xbf49
RAN Secondary RAT Usage Report	73-0	M	This field includes one or more containers reported from the RAN for a secondary RAT.	Sequence	Variable	0x30
Data Volume Uplink	73-0-1	M	This field includes the number of octets transmitted during the use of the packet data services in the uplink direction reported from RAN. The counting and reporting from RAN of uplink data volumes is optional.	Unsigned Integer	9	0x81
Data Volume Downlink	73-0-2	M	This field includes the number of octets transmitted during the use of the packet data services in the downlink direction reported from RAN. The counting and reporting from RAN of downlink data volumes is optional.	Unsigned Integer	9	0x82
RAN Start Time	73-0-3	M	This field is a time stamp, which defines the moment when the volume container is opened by the RAN.	Timestamp	9	0x83
RAN End Time	73-0-4	M	This field is a time stamp, which defines the moment when the volume container is closed by the RAN.	Timestamp	9	0x84

CHAPTER 22

MME Manager Status Traps

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	Release
Introduced to 21.12 release.	21.12.12
First introduced.	21.11.3

Feature Description

The MME manager generates traps based on the below two conditions:

- When the MME manager CPU utilization is above the configured congestion threshold value, the MME manager state becomes busy and it sends a "MMEManagerBusy" trap informing its instance and status.
- When the MME manager CPU utilization reduces below the configured congestion threshold value, the MME Manager state becomes Normal and it sends a "MMEManagerNormal" trap informing its instance and status.

Important If MME manager restarts, it will not come back in the same state, so it will not send any trap.

Configuring MME Manager Status Traps

Use the following configuration to enable MME Manager Status Traps.

Enable MME manager busy trap

```
config
   snmp trap enable MMEManagerBusy
   end
```

Enable MME manager normal trap

```
config
   snmp trap enable MMEManagerNormal
   end
```

Disable MME manager busy trap

```
config
   snmp trap suppress MMEManagerBusy
   end
```

Disable MME manager normal trap

```
config
   snmp trap suppress MMEManagerNormal
   end
```

NOTES:

- **enable**: Enables specific traps.
- **suppress**: Suppresses (disables) specific traps.
- **MMEManagerBusy**: Trap Number 1405.
- **MMEManagerNormal**: Trap Number 1406.

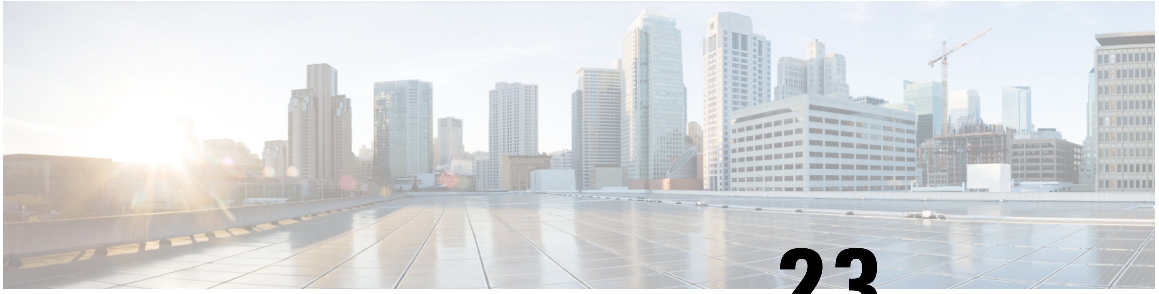
Monitoring and Troubleshooting

This section provides information regarding SNMP Traps available to monitor and troubleshoot the MME Manager Status Traps feature.

SNMP Traps

The following traps are available to track status and conditions related to the MME Manager Status Traps feature.

Trap Name	Description
starMMEManagerBusy	When the MME manager CPU utilization is above the configured congestion threshold value, the MME manager state becomes busy and it sends a "MMEManagerBusy" trap informing its instance and status.
starMMEManagerNormal	When the MME manager CPU utilization reduces below the configured congestion threshold value, the MME Manager state becomes Normal and it sends a "MMEManagerNormal" trap informing its instance and status.



CHAPTER 23

Paging eDRX H-SFN Changed to 10 Bits Counter

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	This feature is enabled/disabled, when the eDRX feature is enabled/disabled.
Related Changes in This Release	Not applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	**Release**
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.13.	21.13.11
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.11.	21.11.3
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.12.	21.12.5
First introduced.	21.0

Feature Changes

Previous Behavior: Paging eDRX H-SFN is 32 bits counter.

New Behavior: Paging eDRX H-SFN changed to 10 bits counter to allow values between 0 to 1023 as per 3GPP TS 36.331 V13.13.0.

Customer Impact: Customer can see the change in the paging timings.

CHAPTER 24

SBc Message Size

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	*MME Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
New SNMP trap "CBCBufSizeExceeded" is introduced and peer-id added to the existing log.	21.11
The CBC can handle bigger SBc messages up to 50K bytes.	21.9

Revision Details	Release
First introduced.	Pre 21.2

Feature Changes

The MME uses the SBc interface, between the MME and the Cell Broadcast Center (CBC), for warning message delivery and control functions. In this release, the SBc message size is increased to handle large messages.

Previous Behavior: When CBC sends the warning messages, MME dropped the SBc messages with size greater than 10K bytes.

New Behavior: When CBC sends the warning messages, the MME can handle SBc messages up to 50K bytes. If the MME receives the WRITE-REPLACE WARNING REQUEST over 50K bytes, the message cannot be processed and a warning syslog is generated.

When the size of the received SBc message is greater than 50 KB, a log with peer-id is displayed. The system also generates a SNMP trap “CBCBufSizeExceeded”.

Customer Impact: With this enhancement, the CBC can send bigger SBc messages with more cell/tac information. Customer can troubleshoot easily with the new trap.

Performance Indicator Changes

show snmp trap statistics

The output of this command includes "CBCBufSizeExceeded" field to indicate number of times the trap is hit.

SNMP Traps

A new trap "starCBCBufSizeExceeded" is introduced to indicate CBC message exceeded the buffer size limit.

CHAPTER 25

Secure File Transfer

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required
Related Features in this Release	Not Applicable
Related Documentation	• *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide* • *Cisco Ultra Services Platform NETCONF API Guide* • *UEM-based VNF Deployment Guide*

Revision History

Revision Details	Release
First introduced.	6.5

Feature Description

UAS provides **upload-file** RPC in ConfD to transfer a file or an image to the VNFC components under given NSD and VNFD levels in a deployed setup.

This command can be invoked from ConfD CLI of AutoDeploy and AutoVNF.

Important Though the **upload-file** command can be invoked from AutoDeploy and AutoVNF, it is highly important that the **nsd-id** must be specified as AutoVNF name only.

Limitations

The file transfer cannot be initiated to the components with following vnf-types — UEM, USP-UAS, ESC. That is, if **esc** is specified as **vnfd** in the **upload-file** command, then the file cannot be transferred to ESC.

How it Works

Perform the following procedure to transfer a file or an image to the VNFs.

1. Log on to AutoDeploy VM or AutoVNF VM as the default user, *ubuntu*.

2. Switch to the *root* user.

   ```
   sudo su
   ```

3. Enter the ConfD CLI.

   ```
   confd_cli -C -u admin
   ```

4. Enter the *admin* user password when prompted.

5. Initiate the file transfer to the VNFs using the following command:

   For AutoDeploy:

   ```
   nsd:upload-file nsd-id <nsd id> vnfd <vnfd name> source <path of the file>
   destination < path >
   ```

   For AutoVNF:

   ```
   upload-file nsd-id <nsd id> vnfd <vnfd name> source <path of the file>
   destination < path >
   ```

   Notes:

   - The **nsd-id** must always be specified as AutoVNF name.
   - **vnfd** is an optional parameter in this configuration. This parameter must be alpha and/or numeric characters, and it accepts more than one value as an input. For example: [vpc1], [vpc1 vpc2 vpc3].

- If **vnfd** is specified in the **upload-file** command and it is a valid VNFD, the file or image is transferred successfully. For the list of invalid or unsupportedVNFDs, see the Limitations, on page 92.
- If **vnfd** is not specified in the **upload-file** command, then the file or image is transferred only to the valid VNFDs in the given NSD deployment.
- If the command includes a single invalid VNFD, the file transfer will not be executed and an error indicating invalid argument in AutoDeploy is displayed. For the list of invalid or unsupportedVNFDs, see the Limitations, on page 92.

Command example:

```
nsd:upload-file nsd-id abc-autovnf vnfd [ vpc ] source
/home/ubuntu/x.cfg destination /sftp
```

6. Monitor the progress of the file transfer operation.

```
show transaction <transaction-id>
```

transaction_id is the ID displayed as a result of the **upload-file** command executed in the previous step.

Example command output:

```
show transaction 15407
TX ID     TX TYPE  DEPLOYMENT ID     TIMESTAMP                 STATUS  STATUS DETAIL
15407 upload-file  vnf-autovnf 2018-10-29T05:43:47.666386-00:00  error    -
```

Also, view the logs associated with a specific transaction.

```
show log <transaction-id>
```

Monitoring File Transfer Operations

AutoDeploy and AutoVNF maintain logs for all transactions in persistent storage. The status/progress of file transfer can be viewed in AutoDeploy/AutoVNF logs archived under */var/log/upstart/* based on where it is invoked.

If invoked from AutoDeploy, then RPC internally connects with AutoVNF and performs the file transfer. The respective progress can be viewed through the AutoVNF logs.

To view the logs associated with a specific transaction:

```
show log <transaction-id>
```

Sample AutoDeploy Logs:

```
2018-10-26 16:12:30,156 - allowed-address-pair: 90.90.90.0/24 on eth0
2018-10-26 16:12:30,163 - Adding pre-created network: suneduvv-orch into catalog
2018-10-26 16:12:30,169 - Adding uplink action check-liveness-using-ping to eth1
2018-10-26 16:12:30,178 - Found VNFD 'suneduvv-autovnf' of type UAS
/usr/lib/python2.7/dist-packages/Crypto/Cipher/blockalgo.py:141: FutureWarning: CTR mode
needs counter parameter, not IV
  self._cipher = factory.new(key, *args, **kwargs)
2018-10-26 16:12:30,634 - Connected to AutoVNF[10.225.202.246]
2018-10-26 16:12:30,641 - dst file name x.cfg
2018-10-26 16:12:30,645 - abs_dest_file /var/cisco/isos/x.cfg
2018-10-26 16:12:30,650 - Skipping copy, file '/var/cisco/isos/x.cfg' already exists
2018-10-26 16:12:30,676 - Updated path to URL in handle_file_transfer
'http://90.90.90.23:5000/isos/x.cfg'
2018-10-26 16:12:31,145 - <?xml version="1.0" encoding="UTF-8"?>
```

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:d9ad94ed-8c42-4059-829c-96182b384b27"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><transaction-id
xmlns='http://www.cisco.com/usp/nfv/usp-nsds'>1540570351-451419</transaction-id>
</rpc-reply>
2018-10-26 16:12:31,150 - Waiting for deployment notifications for tx-id '1540570351-451419'
2018-10-26 16:12:31,155 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:31.472658+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'requested')]
2018-10-26 16:12:31,160 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:requested
2018-10-26 16:12:31,164 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:31.764652+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'instantiated')]
2018-10-26 16:12:31,169 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:instantiated
2018-10-26 16:12:31,173 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:31.790449+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'in-progress')]
2018-10-26 16:12:31,178 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:in-progress
2018-10-26 16:12:31,183 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:31.842616+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'in-progress')]
2018-10-26 16:12:31,188 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:in-progress
2018-10-26 16:12:31,257 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:31.925373+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'in-progress')]
```

```
90.90.90.25 - - [26/Oct/2018 16:12:31] "GET /isos/x.cfg HTTP/1.0" 200 -
2018-10-26 16:12:31,262 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:in-progress
2018-10-26 16:12:32,833 - [('{urn:ietf:params:xml:ns:netconf:notification:1.0}notification',
 None), ('{urn:ietf:params:xml:ns:netconf:notification:1.0}eventTime',
'2018-10-26T16:12:33.493671+00:00'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}upload-file-event', '\n  '),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}instance-id',
'suneduvv-autovnf-instance'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}descriptor-id', 'suneduvv-autovnf'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}transaction-id', '1540570351-451419'),
 ('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}operation-type', 'upload-file'),
('{http://www.cisco.com/usp/nfv/usp-uas-common-oper}status', 'error')]
2018-10-26 16:12:32,838 - Received upload-file-event for suneduvv-autovnf:1540570351-451419
 with status:error
2018-10-26 16:12:32,843 - RPC NS[suneduvv-autovnf:suneduvv-autovnf-instance] failed
2018-10-26 16:12:32,849 - Failed to transfer a file
2018-10-26 16:12:32,854 - Deployment upload-file: suneduvv-autovnf failed
2018-10-26 16:12:32,871 - Send Deployment notification for: suneduvv-autovnf-instance
No handlers could be found for logger "AutoVNF-Traces"
2018-10-26 16:12:32,954 - One or more tasks failed, break the pipeline
2018-10-26 16:12:32,961 - Deployment upload-file: suneduvv-autovnf failed
2018-10-26 16:12:32,982 - Send Deployment notification for: suneduvv-autovnf-instance
```

Sample AutoVNF Logs:

```
2018-10-26 16:14:10,009 - Waiting for all workers to finish the transactions
2018-10-26 16:14:10,037 - Send Deployment notification for: suneduvv-autovnf-instance
2018-10-26 16:14:10,044 - Deployment upload-file: suneduvv-autovnf started
2018-10-26 16:14:10,050 - DOWNLOADING FILE TO STAGING FOLDER FROM
/home/ubuntu/em-6_3_0_4765.qcow2 ========== /var/cisco/isos/em-6_3_0_4765.qcow2
2018-10-26 16:14:10,057 - URL IS NONE []
2018-10-26 16:14:10,063 - Skipping copy, file '/var/cisco/isos/em-6_3_0_4765.qcow2' already
 exists
2018-10-26 16:14:10,070 - I AM HERE56565656   ['vpc']
2018-10-26 16:14:10,087 - vnfrs for the given nsd is suneduvv-autovnf-esc suneduvv-autovnf-vpc
2018-10-26 16:14:10,100 - vnfr_vnfc is [{'vnfr': 'suneduvv-autovnf-esc', 'vnfc': 'esc',
'ip-addr': '90.90.90.32', 'floating-ip': None}, {'vnfr': 'suneduvv-autovnf-vpc', 'vnfc':
'cf', 'ip-addr': '90.90.90.47', 'floating-ip': None}, {'vnfr': 'suneduvv-autovnf-vpc',
'vnfc': 'em', 'ip-addr': '90.90.90.38', 'floating-ip': None}]
2018-10-26 16:14:10,106 - vnfr_vnfd is [{'vnfr': 'suneduvv-autovnf-esc', 'vnfd': 'esc'},
{'vnfr': 'suneduvv-autovnf-vpc', 'vnfd': 'vpc'}]
2018-10-26 16:14:10,112 - vnfdid_list is [{'vnfcid': 'cf', 'fl-ip': None, 'vnfdid': 'vpc',
 'vnfr': 'suneduvv-autovnf-vpc', 'ips': [], 'ha-vip': '90.90.90.47'}, {'vnfcid': 'em',
'fl-ip': None, 'vnfdid': 'vpc', 'vnfr': 'suneduvv-autovnf-vpc', 'ips': [], 'ha-vip':
'90.90.90.38'}]
/usr/lib/python2.7/dist-packages/Crypto/Cipher/blockalgo.py:141: FutureWarning: CTR mode
needs counter parameter, not IV
  self._cipher = factory.new(key, *args, **kwargs)
2018-10-26 16:14:10,429 - Removing staged files from Autovnf
2018-10-26 16:14:10,508 - Files removed successfully
2018-10-26 16:14:10,967 - Copying the file to EM staging...
2018-10-26 16:14:47,430 - XML REQUEST COMMAND <ns0:vnf-put-file
xmlns:ns0="http://www.cisco.com/usp/scm/vnf-utils">
  <file xmlns="http://www.cisco.com/usp/scm/vnf-utils">/tmp/staging/em-6_3_0_4765.qcow2</file>

  <vnfs xmlns="http://www.cisco.com/usp/scm/vnf-utils">
    <vnfd xmlns="http://www.cisco.com/usp/scm/vnf-utils">suneduvv-autovnf-vpc-suneduvv</vnfd>

  </vnfs>
  <destination-path xmlns="http://www.cisco.com/usp/scm/vnf-utils">/fash</destination-path>
</ns0:vnf-put-file>

2018-10-26 16:14:47,602 - rpc executed <?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
```

```
message-id="urn:uuid:95ebbb6d-aa16-48ba-855b-b73cf14ac5a2"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><status
xmlns='http://www.cisco.com/usp/scm/vnf-utils'>Success</status>
</rpc-reply>
2018-10-26 16:14:47,607 - XML REQUEST FOR STATUS COMMAND <show>
  <vnf-put-files-status xmlns="http://www.cisco.com/usp/scm/vnf-utils"/>
</show>

2018-10-26 16:14:47,676 - res is <?xml version="1.0" encoding="UTF-8"?><data
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><vnf-put-files-status
xmlns="http://www.cisco.com/usp/scm/vnf-utils"><puts><name>suneduvv-autovnf-vnfm-suneduvv</name><file>/tmp/staging/en630476.qcow2</file><destination-path>/flash/</destination-path><start-time>2018-10-26 16:14:46.338</start-time><status>In
 progress</status></puts></vnf-put-files-status></data>
2018-10-26 16:14:47,681 - status is In progress
2018-10-26 16:14:47,799 - res is <?xml version="1.0" encoding="UTF-8"?><data
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><vnf-put-files-status
xmlns="http://www.cisco.com/usp/scm/vnf-utils"><puts><name>suneduvv-autovnf-vnfm-suneduvv</name><file>/tmp/staging/en630476.qcow2</file><destination-path>/flash/</destination-path><start-time>2018-10-26 16:14:46.338</start-time><status>In
 progress</status></puts></vnf-put-files-status></data>
2018-10-26 16:14:47,805 - status is In progress
2018-10-26 16:14:47,874 - res is <?xml version="1.0" encoding="UTF-8"?><data
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><vnf-put-files-status
xmlns="http://www.cisco.com/usp/scm/vnf-utils"><puts><name>suneduvv-autovnf-vnfm-suneduvv</name><file>/tmp/staging/en630476.qcow2</file><destination-path>/flash/</destination-path><start-time>2018-10-26 16:14:46.338</start-time><status>In
 progress</status></puts></vnf-put-files-status></data>
2018-10-26 16:14:47,879 - status is In progress
2018-10-26 16:14:47,997 - res is <?xml version="1.0" encoding="UTF-8"?><data
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"><vnf-put-files-status
xmlns="http://www.cisco.com/usp/scm/vnf-utils"><puts><name>suneduvv-autovnf-vnfm-suneduvv</name><file>/tmp/staging/en630476.qcow2</file><destination-path>/flash/</destination-path><start-time>2018-10-26 16:14:46.338</start-time><status>Failed</status></puts></vnf-put-files-status></data>
2018-10-26 16:14:48,009 - Deployment upload-file: suneduvv-autovnf failed
2018-10-26 16:14:48,027 - Send Deployment notification for: suneduvv-autovnf-instance
2018-10-26 16:14:48,040 - One or more tasks failed, break the pipeline
2018-10-26 16:14:48,046 - Deployment upload-file: suneduvv-autovnf failed
2018-10-26 16:14:48,103 - Send Deployment notification for: suneduvv-autovnf-instance
```

CHAPTER 26

SRVCC Delete Bearer Request Handling

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	**Release**
SRVCC Delete Bearer Request Handling introduced to release 21.12.	21.12.9
SRVCC Delete Bearer Request Handling introduced to release 21.11.	21.11.4
SRVCC Delete Bearer Request Handling introduced to release 21.5.	21.5.20

Revision Details	Release
First introduced.	Pre 21.5

Feature Changes

With this release, MME can be configured to ignore the Delete Bearer Request (DBR) initiated from PGW while the Single Radio Voice Call Continuity (SRVCC) is ongoing, a new CLI command **policy srvcc dbr ignore** is introduced in the MME-Service configuration mode to enable the same.

Previous Behavior: The MME aborts the SRVCC when it receives P-GW initiated "Delete Bearer Request" for Voice bearer (QCI 1).

New Behavior: The MME processes the "Delete Bearer Request" initiated from P-GW while the SRVCC is ongoing. MME will not abort the SRVCC procedure.

Command Changes

Configuring DBR Handling while SRVCC is Ongoing

Use the below configuration for handling the Delete Bearer Request (DBR) from P-GW while SRVCC is Ongoing.

```
configure
  context context_name
    mme-service service_name
       [ no ]policy srvcc dbr ignore
       default policy srvcc dbr
       end
```

Notes:

- **no** Returns the command to its default behavior, where the MME abort the SRVCC when it receives P-GW initiated "Delete Bearer Request" for Voice bearer (QCI 1).
- The **default** Returns the command to its default behavior, where the MME abort the SRVCC when it receives P-GW initiated "Delete Bearer Request" for Voice bearer (QCI 1).
- The **dbr** Configures the behavior to handle "Delete-Bearer-Request" message.
- The **ignore** Ignores the DBR (Voice Bearer) initiated from P-GW while SRVCC is ongoing.

CHAPTER 27

SRVCC HO Timer Configuration for ESM Notification

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	**Release**
Introduced to 21.11 release.	21.11.9
Introduced to 21.12 release.	21.12.12
First introduced.	21.5.19

Feature Changes

Previous Behavior: During SRVCC Handover, if handover cancel is triggered due to UE context release received from eNB due to lost radio connection with UE, ESM notification will not be sent to UE.

New Behavior: During SRVCC Handover, if handover cancel is triggered due to UE context release received from eNB due to lost radio connection with UE, UE goes to IDLE mode. When UE comes back through service request or TAU request within the configured timer value, ESM notification will be sent to UE and UE will re-establish the session.

Command Changes

Configuring UE Come Back Time

Use the following configuration to configure UE come back time after UE context release due to radio radio connection when UE:

```
configure
  call-control-profile profile_name
    srvcc ho-timer ho_timer
    end
```

Notes:

- **srvcc**: Configures the basic SRVCC support on the MME.
- **ho-timer** *ho_timer*: Configures UE come back time in seconds after UE context released due to lost radio connection with UE. *ho_timer* must be an integer value from 1 to 100.

CHAPTER 28

MME Support for Service Impacting KPI Bulk Statistics

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**
Introduced to 21.12 release.	21.12.12
First introduced.	21.11.3

Feature Description

New Counters under show command outputs and bulk statistics are introduced to improve debugging and health monitoring.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the MME Support for Service impacting KPI Bulk Statistics.

Show Commands and Outputs

show mme-service statistics recovered-values

The output of this command includes the following fields:

EMM Control Messages:

- Congestion
- Protocol Errors
- Svc Opt Tmp OutOfOrder
- Authentication Fail
- Authentication Failed
- Insufficient Resource
- Severe Network Failure
- Network Failure
- Rejected By PGW/SGW
- Activation Rejected

Procedure Failure Reasons:

- Max retx auth req
- Max retx sec mode cmd
- Max retx attach accept
- Setup timeout expiry
- SCTP/S1-failure
- Internal guard timeout
- Max retx ESM info req

Bulk Statistics

The following bulk statistics variables are added in the mme-bk schema:

Bulk Statistics	Description
recovered-emm-msgtx-attach-reject-congestion	The total number of EMM Attach Reject messages sent with cause code 22.
recovered-emm-msgtx-attach-rej-protocol-error	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with any of the following Protocol Error cause codes 95-101, or 111.
recovered-emm-msgtx-attach-rej-svc-temp-out-of-order	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with cause code 34 - Service Option Temporarily Out of Order.
recovered-emm-msgtx-attach-auth-failed	The total number of authentication failed and an Attach Accept or Reject message is not sent.
recovered-attach-proc-fail-max-retx-auth-req	The total number of attach-triggered authentication procedures failed due to maximum retransmissions of authentication request.
recovered-attach-proc-fail-max-retx-sec-mode-cmd	The total number of attach-triggered authentication procedures failed due to maximum retransmissions of security mode command.
recovered-attach-proc-fail-max-retx-attach-accept	The total number of attach procedures failed due to maximum retransmissions of attach accept.
recovered-attach-proc-fail-setup-timeout-exp	The total number of attach procedure cleared due to expiry of setup-timeout.
recovered-attach-proc-fail-sctp-fail	The total number of attach procedures cleared due to SCTP down.
recovered-attach-proc-fail-guard-timeout-exp	The total number of attach procedures cleared due to expiry of internal guard timer. This also includes internal guard timeout of authentication procedure. If authentication procedure is called, and authentication procedure aborts due to its guard timer, the counter will be accounted for in attach procedure.
recovered-attach-proc-fail-max-retx-esm-info-req	The total number of attach procedures failed due to maximum retransmissions of ESM info request.
recovered-emm-msgtx-attach-rej-gw-auth-failed	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with cause code 29 - User Authentication Failed.
recovered-emm-msgtx-attach-rej-insuff-resources	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with cause code 26 - Insufficient Resources.

Bulk Statistics	Description
recovered-emm-msgtx-attach-reject-severe-network-failure	The total number of EMM Attach Reject messages sent with cause 42 - Severe Network Failure.
recovered-emm-msgtx-network-failure	The total number of EMM Attach Reject messages sent with the cause code 17 - Network Failure.
recovered-emm-msgtx-attach-rej-gw-reject	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with cause code 30 - Rejected by SGW or P-GW.
recovered-emm-msgtx-attach-rej-activation-reject	The total number of EMM Attach Reject messages sent due to an ESM procedure failure with cause code 31- Request rejected, unspecified.
recovered-emm-msgtx-tau-network-fail	The total number of TAU Reject messages sent (for either an Inter-node or Intra-MME TAU request), with a cause code of 17 - Network failure.

CHAPTER 29

SGs SCTP Association Counters

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
SGs SCTP Association Counters was first introduced in release 21.11. With this release, this feature is also applicable to release 21.5.16.	21.5.16
First introduced.	21.11

Feature Description

MME supports display of SCTP associated counters for SGS service. New command `show sgs-service sctp-association { all | peerid }` is introduced to display SCTP associated counters for SGS Service.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the SGs SCTP Association Counters feature.

Show Commands and Outputs

show sgs-service sctp-association { all | peerid }

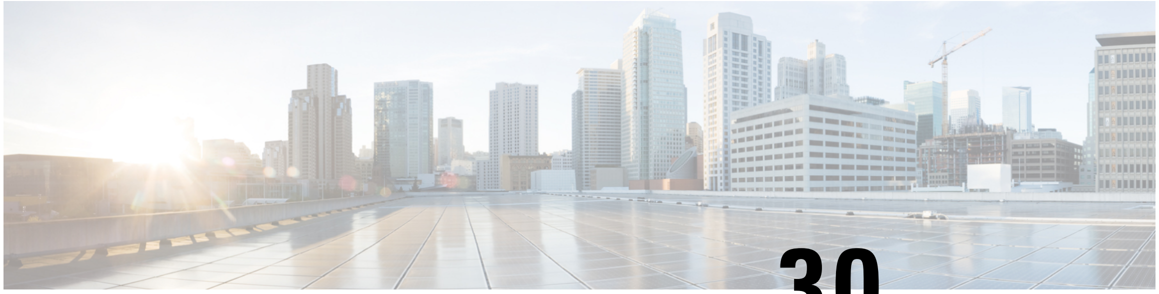
The output of this command includes the following fields:

- Flow control flag
- Peer INIT tag
- Local INIT tag
- Next TSN
- Lowest cumulative TSN acknowledged
- Cumulative peer TSN
- Last peer TSN sent in the SACK
- Local RWND
- Peer RWND (advertised) in the SACK
- Peer RWND(estimated)
- Retransmissions
- ZWnd probing flag
- Last TSN received during ZWnd Probing
- Bytes outstanding
- Congestion queue length
- Ordered TSN waiting QLen
- Unordered TSN waiting QLen
- GAP ACKs sent
- GAP ACKs received

No.	Source Address	Destination Address	Path Status

- Path No.
- Current CWND
- SSThresh
- Partial bytes acked
- Bytes outstanding
- Current RTO (in ms)

Important `sctp all` displays cumulative statistics for the peer VLRs where as `sctp peerid` displays statistics for a particular Peer ID.



CHAPTER 30

Service Impacting SGSN KPI Bulk Statistics

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled - Always On
Related Changes in This Release	Not Applicable
Related Documentation	• *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Introduced to 21.12 release.	21.12.12
First introduced.	21.11.3

Feature Description

SGSN will backup KPI counters during session manager crash or restart.

Following backup counters are introduced to record the data during session manager crash or restart:

- 2G-attach-fail-internal-failure-bk
- 3G-actv-rej-insufficient-resources-int-bk

Once the session manager crashes or restarts all the backup counters will be restored to session manager.

Monitoring and Troubleshooting

This section provides information regarding Bulk Statistics available to monitor and troubleshoot the MME Support for Service impacting KPIs.

Bulk Statistics

New backup counters "3G-actv-rej-insufficient-resources-int-bk" is added to iups-bk schema and "2G-attach-fail-internal-failure-bk" to gprs-bk schema to support Service Impactiing SGSN KPI Bulk Statistics feature.

CHAPTER 31

Short Message Service

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • UGP • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
"New sub traffic type SMS added under traffic PS to configure Heuristic paging" was introduced in release 21.11. With this release, this feature is also applicable to release 21.8.9.	21.8.9
New sub traffic type SMS added under traffic PS to configure Heuristic paging.	21.11
First introduced.	21.8

Feature Description

The Short Message Service (SMS) is a means of sending messages of limited size to and from GSM/UMTS/EPS devices. SMS is a Store and Forward service, where messages are first sent to an entity called the Short Message Service Center (SMSC) and then forwarded to the recipient instead of transmitting directly to the destination.

If the recipient is not connected, the message is saved in the SMSC and when the receiver becomes available, the network will contact the SMSC and forward the SMS. Thus, a GSM/UMTS/EPS PLMN supports the transfer of short messages between service centers and UEs.

SMS is delivered over LTE through the following methods:

- **SMS over SGs**: The LTE UE device sends and retrieves circuit switched (CS) based SMS messages through the SGs interface. This method is already supported by the MME.
- **SMS over IP**: SIP based SMS messages are carried through IMS. The SMS to be transmitted is encapsulated in the SIP message. This method is not supported in this release.
- **SMS in MME**: SMS in MME delivers SMS services over the SGd interface to the SMSC. This method is intended for networks that do not deploy GERAN or UTRAN. This method is supported in this release.

How It Works

The SGd interface enables the transfer of short messages between the MME and the SMSC using Diameter protocol. SCTP is used as the transport protocol.

The Short Message Control Protocol (SM-CP) and Short Message Relay Protocol (SM-RP) are traditional SMS protocols between MSC/VLR and UE. The SMS will be sent by the MME bypassing the MSC/VLR.

SM-CP transmits the SMS and protects against loss caused by changing the dedicated channel. SM-RP manages the addressing and references.

With the new interface configuration towards SMSC, MME will setup an SCTP association with the peer SMSC and the Diameter capability exchange will be performed.

Limitations

This section lists the known limitations for the SMS feature:

- MME will attempt to fallback to the SGs mode if SGd and SGs are enabled and if HSS rejects SMS in MME. This functionality is not supported in this release.
- Multiple SMSC service association is not supported. Only one endpoint will be associated with an MME service. If multiple SMSC services are required, then the SMS router must be used.
- The Serving Node Identity AVP is not supported in the Alert-Service-Centre-Request command. Hence SMSC needs to perform the "Send Routing Info for SM" procedure to retrieve the address of the new serving node from the HSS.
- Sending or processing of the "Pending MT Short Message Indication" flag under Forward Relocation Request will not be supported.
- Sending and processing of "MME number for MT SMS" and "MME Identifier for MT SMS" under Forward Relocation Request/Response are not supported.
- SMS will not be processed when the MME common procedure is ongoing.
- Notify Request to HSS for each UE due to removal of SMSC service is not supported.
- Notify Request to HSS is not supported if UE does an IMSI Detach.
- Delete Subscription Data Request from HSS is not supported for MO/MT SMS.
- CDR generation is not supported.

Flows

This section describes the call flows related to the SMS feature.

Obtaining UE capability for SMS

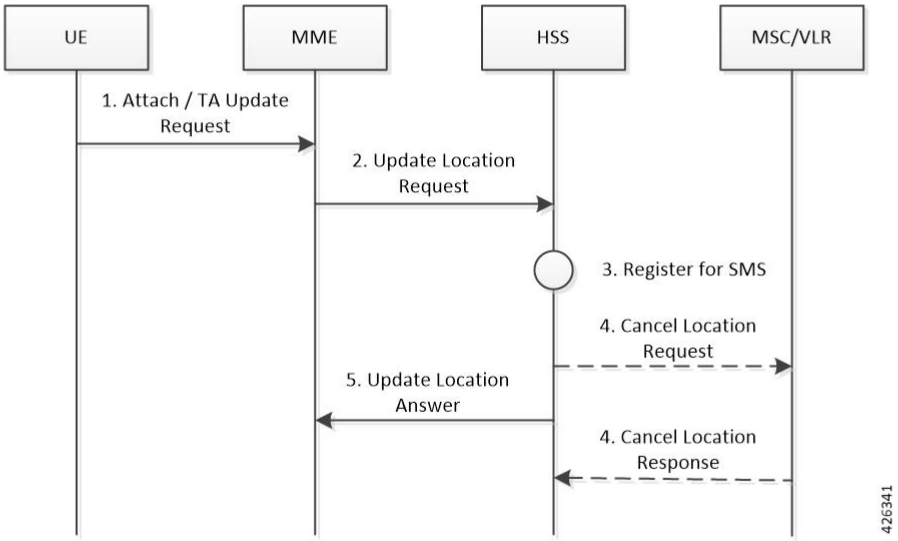
If the UE requests "SMS-only" in the Additional Update Type IE of combined attach and the network accepts the Attach Request for EPS services and "SMS-only", the network will indicate "SMS-only" in the Additional Update Result IE. If the SMS services are provided by SGd in the MME, the network will provide a TMSI and non-broadcast LAI in the Attach Accept message.

SMS Capability with HSS

A UE supporting SMS in MME needs to perform a registration with the HSS.

The following call flow illustrates the request for registration with the HSS.

Figure 2: SMS Capability with HSS

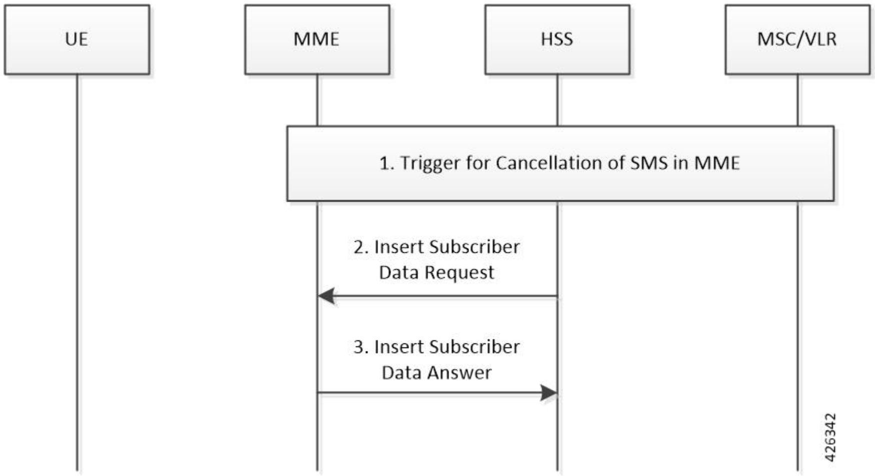

UE
MME
HSS
MSC/VLR
1. Attach / TA Update Request
2. Update Location Request
3. Register for SMS
4. Cancel Location Request
5. Update Location Answer
4. Cancel Location Response
426341

Step	Description
1	The UE initiates combined Attach Update or combined TAU/LAU to an MME.
2	The MME sends an Update Location Request message to the HSS with the following data: • SMS bit set in Feature-List in Supported-Features AVP. The Feature-List ID will be set to 2. • "SMS-only" indication bit set in ULR-Flags AVP. • MME address for MT-SMS routing in MME-Number-for-MT-SMS AVP. • "SMS-only" indication set in SMS-Register-Request AVP.
3	HSS registers the UE for SMS support in MME.
4	If the HSS accepts to register the MME identity as an MSC identity for terminating SMS services, then the HSS cancels the MSC/VLR registration from the HSS.
5	For successful registrations, HSS sends a Location Update Answer (indication that the MME has registered for SMS) message to the MME. HSS sets the "MME Registered for SMS" bit in ULA-Flags AVP.

HSS-initiated Removal of Registration for SMS

The following procedure is applied when the HSS needs to indicate to the MME that it is no longer registered for SMS.

Figure 3: Removal of Registration for SMS

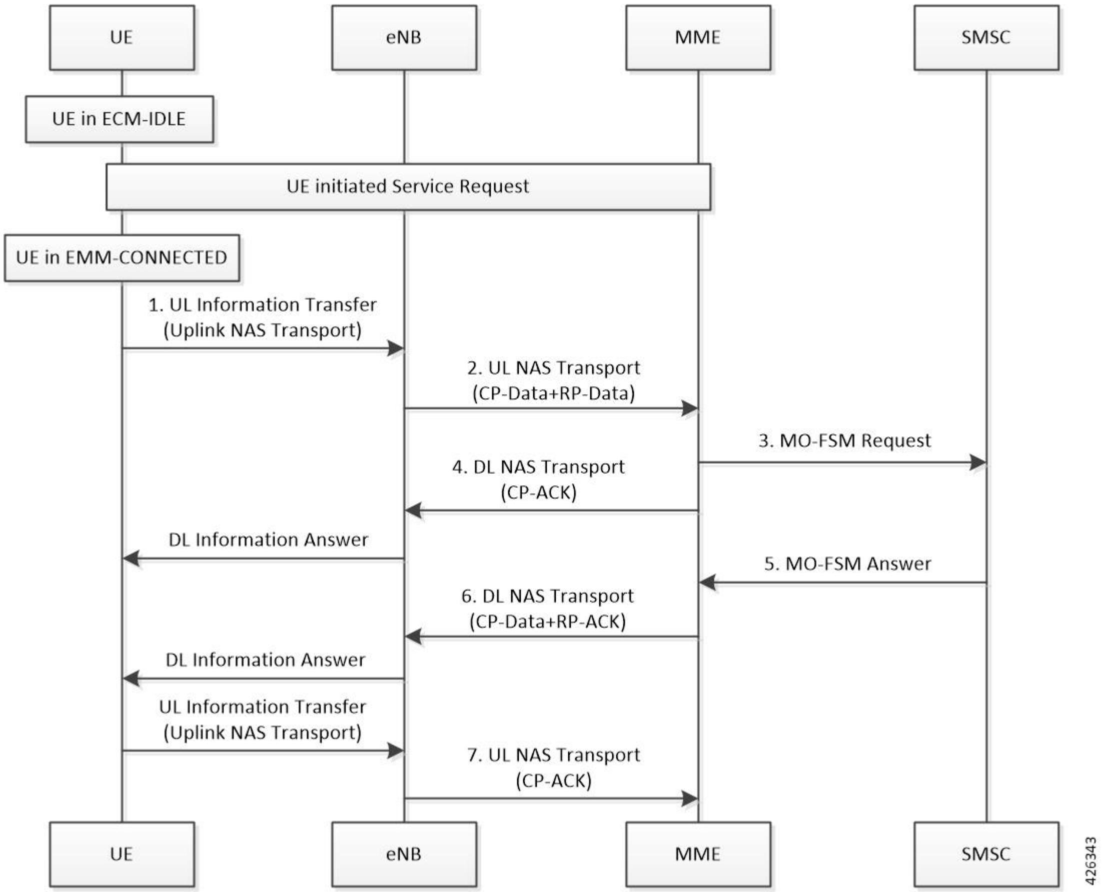

UE
MME
HSS
MSC/VLR
1. Trigger for Cancellation of SMS in MME
2. Insert Subscriber Data Request
3. Insert Subscriber Data Answer
426342

Step	Description
1	An event will trigger the cancellation of the MME being registered for SMS. For example, removal of the SMS subscription for the UE, CS location update, and so on.
2	The HSS sends an Insert Subscriber Data Request (Remove SMS registration) message to the MME to inform that it is no more registered for SMS in MME.
3	The MME sets the "MME Registered for SMS" parameter as not registered for SMS and the "SMS Subscription Data" is considered by the MME as invalid. It acknowledges with an Insert Subscriber Data Answer message to the HSS.

MO Forward Short Message Procedure

The MO Forward Short Message procedure is used between the serving MME and the SMSC to forward mobile originated short messages from a mobile user to a service center. MME checks the SMS related subscription data and forwards the short message.

Figure 4: MO Forward Short Message Procedure


UE
eNB
MME
SMSC
UE in ECM-IDLE
UE initiated Service Request
UE in EMM-CONNECTED
1. UL Information Transfer (Uplink NAS Transport)
2. UL NAS Transport (CP-Data+RP-Data)
3. MO-FSM Request
4. DL NAS Transport (CP-ACK)
DL Information Answer
5. MO-FSM Answer
6. DL NAS Transport (CP-Data+RP-ACK)
DL Information Answer
UL Information Transfer (Uplink NAS Transport)
7. UL NAS Transport (CP-ACK)
UE
eNB
MME
SMSC
426343

Step	Description
1	The UE sends mobile originated SMS to MME in the Uplink NAS Transport message.
2	MME will encapsulate the SMS in CP-DATA+RP-DATA.
3	The message will be encoded into MO-Forward-Short-Message-Request (OFR) message and sent to SMSC.
4	MME acknowledges the received SMS by sending CP-ACK to UE in the Downlink NAS Transport message.
5	SMSC processes the received OFR message and responds backs with MO-Forward-Short-Message-Answer (OFA) message to MME.
6	MME forwards the acknowledgement from SMSC in CP-DATA+RP-ACK to UE.
7	UE acknowledges the SMS delivery by sending CP-ACK to MME in the Uplink NAS Transport message.

MT Forward Short Message Procedure

The MT Forward Short Message procedure is used between the SMSC and the serving MME to forward mobile terminated short messages.

- When receiving the MT Forward Short Message Request, the MME checks if the user is known.

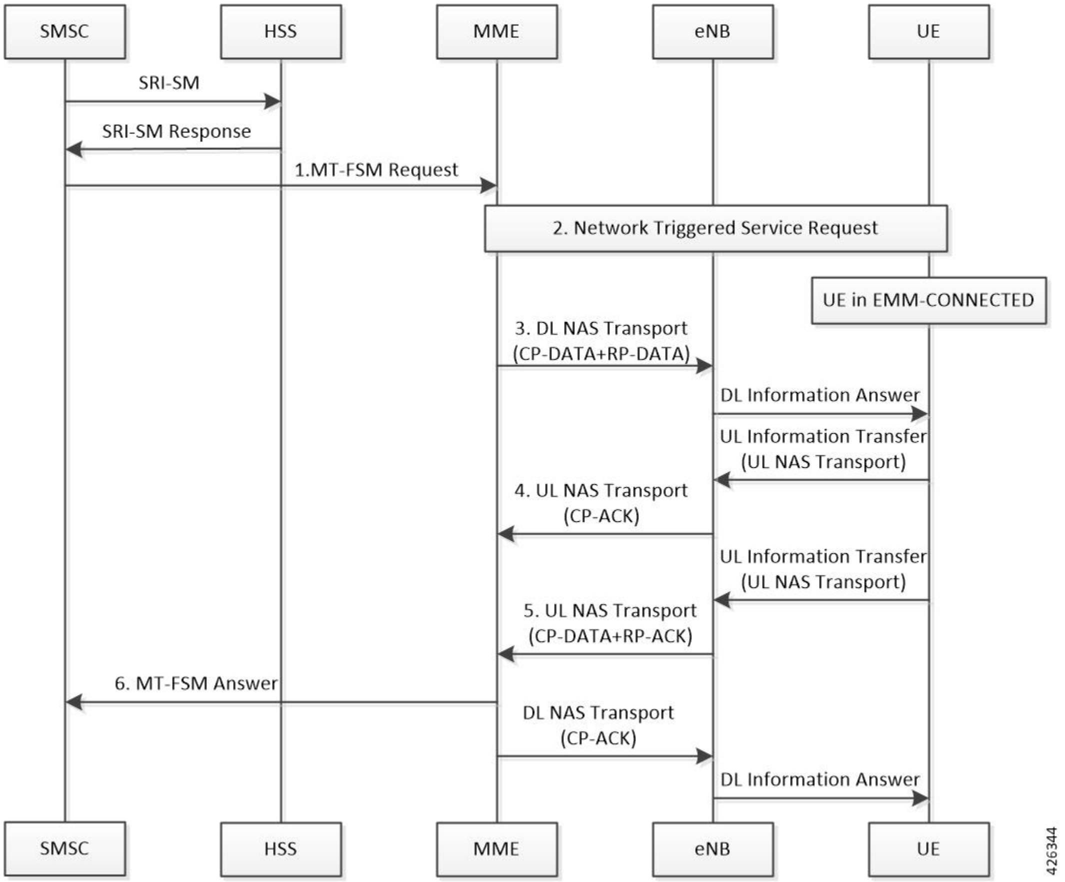
  If it is an unknown user, an Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN is returned.

- The MME attempts to deliver the short message to the UE.

  If the delivery of the short message to the UE is successful, the MME returns a Result-Code set to DIAMETER_SUCCESS.

- If the UE is not reachable via the MME, the MME sets the MNRF flag and returns an Experimental-Result-Code set to DIAMETER_ERROR_ABSENT_USER.
- If the delivery of the mobile terminated short message failed because the memory capacity exceeded, UE error, or UE not SM equipped, the MME returns an Experimental-Result-Code set to DIAMETER_ERROR_SM_DELIVERY_FAILURE with a SM Delivery Failure Cause indication.

Figure 5: MT Forward Short Message

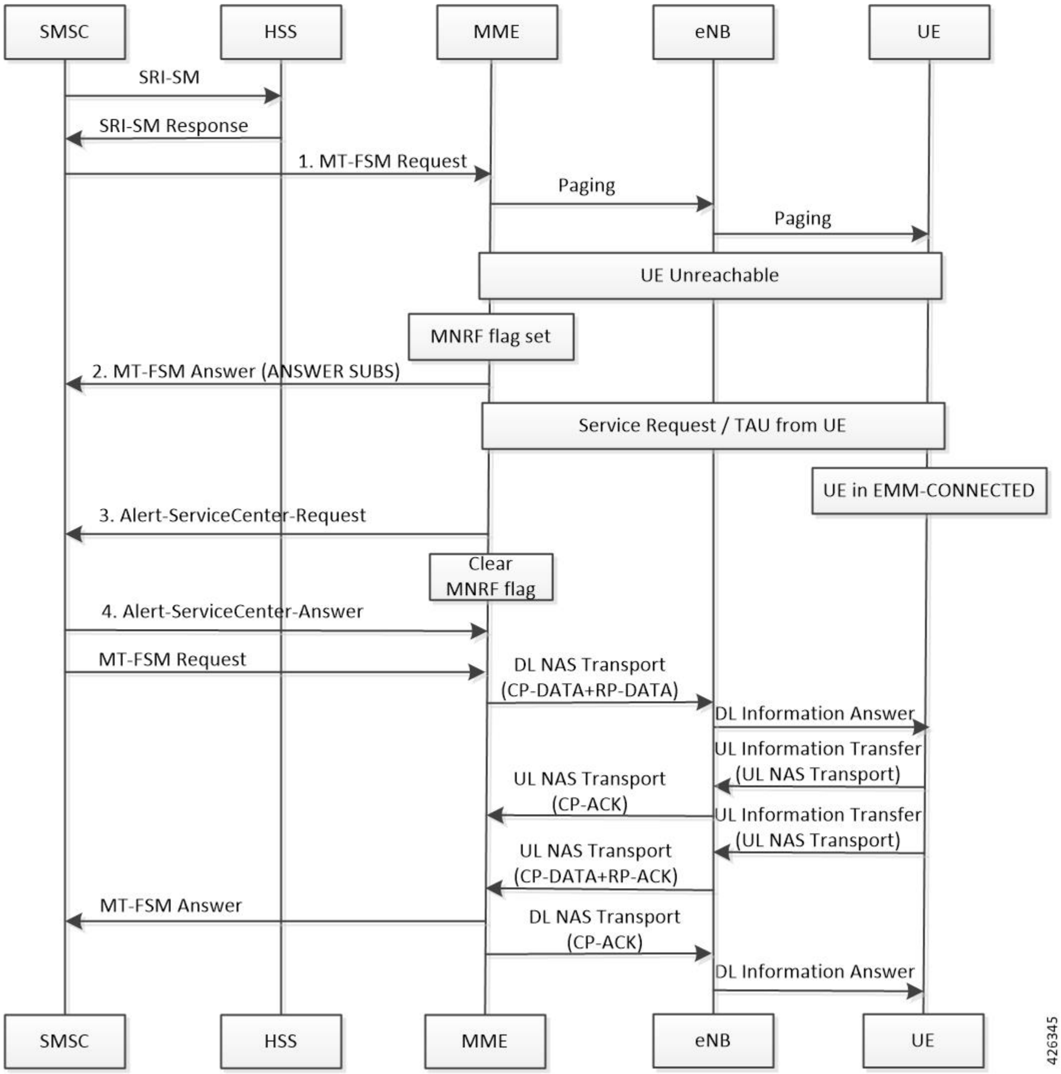

SMSC
HSS
MME
eNB
UE
SRI-SM
SRI-SM Response
1.MT-FSM Request
2. Network Triggered Service Request
UE in EMM-CONNECTED
3. DL NAS Transport (CP-DATA+RP-DATA)
DL Information Answer
UL Information Transfer (UL NAS Transport)
4. UL NAS Transport (CP-ACK)
UL Information Transfer (UL NAS Transport)
5. UL NAS Transport (CP-DATA+RP-ACK)
6. MT-FSM Answer
DL NAS Transport (CP-ACK)
DL Information Answer
SMSC
HSS
MME
eNB
UE
426344

Step	Description
1	The SMSC sends mobile terminated SMS to MME in the MT-Forward-Short-Message-Request (TFR) message.
2	If the UE is in IDLE mode then MME initiates paging and establishes an S1AP connection provided UE replies with paging response.
3	Once the UE is in CONNECTED mode, MME forwards the SMS in CP-DATA+RP-DATA to UE using the Downlink NAS Transport message.
4	The UE acknowledges the received message by sending CP-ACK in the Uplink NAS Transport message.
5	The UE processes the received SMS and sends CP-DATA+RP-ACK to MME.
6	The MME sends the MT-Forward-Short-Message-Answer (TFA) command to SMSC and forwards CP-ACK to the UE in the Downlink NAS Transport message.

MT Forward Short Message Procedure (UE Unreachable)

The MT Forward Short Message procedure is used between the SMSC and the serving MME to forward mobile terminated short messages for an UE that is unreachable.

Figure 6: MT Forward Short Message Procedure (UE Unreachable)


SMSC
HSS
MME
eNB
UE
SRI-SM
SRI-SM Response
1. MT-FSM Request
Paging
Paging
UE Unreachable
MNRF flag set
2. MT-FSM Answer (ANSWER SUBS)
Service Request / TAU from UE
UE in EMM-CONNECTED
3. Alert-ServiceCenter-Request
Clear MNRF flag
4. Alert-ServiceCenter-Answer
MT-FSM Request
DL NAS Transport (CP-DATA+RP-DATA)
DL Information Answer
UL Information Transfer (UL NAS Transport)
UL NAS Transport (CP-ACK)
UL Information Transfer (UL NAS Transport)
UL NAS Transport (CP-DATA+RP-ACK)
MT-FSM Answer
DL NAS Transport (CP-ACK)
DL Information Answer
426345

Step	Description
1	The SMSC sends mobile terminated SMS to MME in the MT-Forward-Short-Message-Request (TFR) message.
2	If the UE is paged but is not reachable, MME sets the MNRF flag and sends the MT-Forward-Short-Message-Answer (TFA) message with Subscriber-absent cause to the SMSC.
3	When the UE becomes available and gets connected to the core network, MME clears the MNRF flag. MME sends the Alert-Service-Centre-Request (ALR) message to SMSC to inform that UE is reachable and that SMS delivery can be re-attempted. This is controlled by the **mme sgd send message alr trigger mnrf** CLI command and disabled by default.

Step	Description
4	The SMSC responds with the Alert-Service-Centre-Answer (ALA) command to the MME and then follows the route procedure of sending MT SMS to UE.
5	Also, the Notify Request to HSS will be sent with alert reason "user available". This is controlled by the **mme s6a send message nor trigger mnrf** CLI command and enabled by default.

MT Forward Short Message Procedure (UE Memory Unavailable)

This procedure is used between the SMSC and the serving MME to forward mobile terminated short messages for an UE that has unavailable memory.

Step	Description
1	The SMSC sends mobile terminated SMS to MME in the MT-Forward-Short-Message-Request (TFR) message, but UE memory is full and returns the RP Error with cause code "Memory capacity exceeded". MME sets the MNRF flag and sends the MT-Forward-Short-Message-Answer (TFA) message with cause code "SM Delivery Failure" and failure cause "Memory capacity exceeded" to SMSC.
2	Once the UE memory is available, it will send RP-SMMA message to MME. MME clears the MNRF flag and sends the Alert-Service-Centre-Request (ALR) message to SMSC to inform that UE memory is available and the SMS delivery can be re-attempted. This is controlled by the **mme sgd send message alr trigger mnrf** CLI command and disabled by default.
3	The SMSC responds with the Alert-Service-Centre-Answer (ALA) command to the MME and then follows the route procedure of sending MT SMS to UE.
4	The Notify Request to HSS will also be sent with alert reason "user memory available". This is controlled by the **mme s6a send message nor trigger mnrf** CLI command and enabled by default.

MT Forward Short Message Procedure (UE Moves due to HO)

This procedure is used between the SMSC and the serving MME to forward mobile terminated short messages for an UE that moves due to handover.

Step	Description
1	While the MNRF flag is set due to UE unreachable or UE memory unavailable, UE may do a handover (HO) and move to another MME or SGSN.
2	Since the MNRF flag was set, MME will send the Alert-Service-Centre-Request (ALR) message to SMSC to inform that UE has moved to another MME or SGSN. This is controlled by the **mme sgd send message alr trigger mnrf** CLI command and disabled by default.
3	The SMSC responds with the Alert-Service-Centre-Answer (ALA) command to the MME and then follows the route procedure of sending MT SMS to UE.

Step	Description
4	The Notify Request to HSS will also be sent with alert reason "user memory available". This is controlled by the **mme s6a send message nor trigger mnrf** CLI command and enabled by default.

Important This procedure has the following limitations:

- New Serving Node Identity AVP is not supported and SMSC needs to perform the "Send Routing Info for SM" procedure to retrieve the new serving node's address from the HSS.
- Sending or processing of the "Pending MT Short Message Indication" flag under Forward Relocation Request will not be supported.

Standards Compliance

The SMS feature complies with the following standards:

- 3GPP TS 23.040 version 12.2.0: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of the Short Message Service (SMS)
- 3GPP TS 24.011 version 12.0.0: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface
- 3GPP TS 24.301 version 13.12.0: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
- 3GPP TS 24.301 version 15.1.0: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
- 3GPP TS 29.272 version 12.11.0: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.272 version 15.2.0: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.338 version 13.4.0: Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)
- 3GPP TS 29.338 version 14.3.0: Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)

Configuring SMS Support

This section provides information on the CLI commands to configure the SMSC service for SMS support in MME.

Creating and Configuring SMSC Service

Use the following configuration to enable the SMSC service and configure the parameters in SMSC service to support MO/MT SMS delivery between SMSC, MME, and UE.

```
configure
  context context_name
    smsc-service smsc_svc_name
      diameter { dictionary standard | endpoint endpoint_name }
      mme-address mme_address
      tmsi tmsi_value non-broadcast mcc mcc_value mnc mnc_value lac lac_value
      default diameter dictionary
      no { diameter endpoint | mme-address | tmsi }
      end
```

NOTES:

- **context** *context_name*: Creates or specifies an existing context and enters the Context Configuration mode. *context_name* specifies the name of a context entered as an alphanumeric string of 1 to 79 characters.
- **smsc-service** *smsc_svc_name*: Creates and configures an SMSC Peer service to allow communication with SMSC peer. *smsc_svc_name* specifies the name of the SMSC service as an alphanumeric string of 1 to 63 characters.

  Entering this command in the Context mode results in the following prompt:

  [context_name]host_name(config-smsc-service)#
- **diameter { dictionary standard | endpoint** *endpoint_name* **}**: Configures the Diameter interface to be associated with the SMSC service.
  - **dictionary standard**: Configures the standard SGd dictionary.
  - **endpoint** *endpoint_name*: Enables Diameter to be used for accounting and specifies which Diameter endpoint to use. *endpoint_name* must be an alphanumeric string of 1 to 63 characters.
- **mme-address** *mme_address*: Configures the MME address to send SMS on the SGd interface. *mme_address* specifies the MME address (ISDN identity) as an integer from 1 to 15.
- **tmsi** *tmsi_value* **non-broadcast mcc** *mcc_value* **mnc** *mnc_value* **lac** *lac_value*: Configures the TMSI to be sent to UE. *tmsi_value* specifies the 4-byte M-TMSI as an integer from 1 to 4294967295.
  - **non-broadcast**: Configures the non-broadcast Location Area Identifier (LAI).
  - **mcc** *mcc_value*: Configures the mobile country code (MCC) portion of non-broadcast LAI for the SMSC service as an integer from 100 through 999.
  - **mnc** *mnc_value*: Configures the mobile network code (MNC) portion of non-broadcast LAI for the SMSC service as a 2- or 3-digit integer from 00 through 999.
  - **lac** *lac_value*: Configures the location area code (LAC) value as an integer from 1 to 65535.
- **default**: Configures the standard Diameter SGd dictionary by default.
- **no**: Disables the specified configuration.

Verifying the Configuration

Use the following command to verify the configuration for all SMSC services or a specified SMSC service:

```
show smsc-service { all | name smsc_svc_name | statistics { all | name
smsc_svc_name | summary } }
```

Configuring MME Preference for SMS

Use the following configuration to configure the MME preference for SMS and SMSC address.

```
configure
   call-control-profile profile_name
      sms-in-mme { preferred [ smsc-address smsc_address ] | smsc-address
smsc_address | subscribe [ notify ue ] }
     no sms-in-mme { preferred [ smsc-address ] | smsc-address | subscribe
 [ notify ue ] }
      default sms-in-mme { subscribe [ notify ue ] }
      end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of a call control profile entered as an alphanumeric string of 1 to 64 characters.
- **sms-in-mme**: Configures the SMS capability (SGd interface for SMS) in MME.
- **preferred**: Configures the SMS preference in MME.
- **smsc-address** *smsc_address*: Configures the SMSC address (ISDN identity) for the MME to send SMS on the SGd interface. *smsc_address* must be an integer from 1 to 15.
- **subscribe [notify ue]**: Enables the Subscription Request for SMS services (via SGd) to HSS for all users.
  - **notify**: Configures the notification to be sent to the users.
  - **ue**: Sends SMS-Only indication to UE in Attach/TAU Accept message (only if HSS accepts SMS Registration for SGd).
- **default**: Restores the default configuration, which is to enable the Subscription Request for SMS services (via SGd) to HSS for all users.
- **no**: Deletes the specified configuration.

Associating SMSC Service with MME Service

Use the following configuration to associate an SMSC service with the MME service.

```
configure
   context context_name
      mme-service service_name
         associate smsc-service smsc_svc_name [ context ctx_name ]
         end
```

NOTES:

- **context** *context_name*: Creates or specifies an existing context and enters the Context Configuration mode. *context_name* specifies the name of a context entered as an alphanumeric string of 1 to 79 characters.
- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.
- **associate smsc-service** *smsc_svc_name*: Associates an SMSC service with the MME service. *smsc_svc_name* specifies the name for a pre-configured SMSC service to associate with the MME service as an alphanumeric string of 1 to 63 characters.
- **context** *ctx_name*: Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the MME service. *ctx_name* must be an alphanumeric string of 1 to 63 characters.

Configuring Alert SC Request on SGd interface

Use the following configuration to control sending the Alert SC Request (ALR) on SGd interface.

The user sends the Alert SC Request on SGd interface to SMSC in the event of user availability to received SMS (if user moved to active state from idle or user's memory is available). It is also sent if the user did a handover to the new MME/SGSN and any MT SMS was pending for the user.

```
configure
  call-control-profile profile_name
    [ no ] mme sgd send message alr trigger mnrf
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of a call control profile entered as an alphanumeric string of 1 to 64 characters.
- **mme**: Configures MME capability.
- **sgd**: Configures MME capability on SGd interface.
- **send**: Configures MME capability to send on SGd interface.
- **message**: Configures MME capability to send message on SGd interface.
- **alr**: Configures MME capability to send Alert SC Request (ALR) on SGd interface.
- **trigger**: Configures trigger to send the message.
- **mnrf**: Sends message to trigger MNRF flag on SGd interface (SMS in MME).
- **no**: Disables sending the ALR on SGd interface.
- This command is disabled by default.

Verifying the Configuration

Use the following command to verify whether Alert SC Request (MME SGd Message Options) is enabled or disabled:

```
show call-control-profile full all
```

Configuring Notify Request on S6a Interface

Use the following configuration to control sending the Notify Request (NOR) on S6a interface.

The user sends the Notify Request on S6a interface to HSS in the event of user availability to received SMS (user moved to active state from idle or user's memory is available).

```
configure
   call-control-profile profile_name
      [ no ] mme s6a send message nor trigger mnrf
      end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of a call control profile entered as an alphanumeric string of 1 to 64 characters.
- **mme**: Configures MME capability.
- **s6a**: Configure MME capbility on S6a interface.
- **send**: Configures MME capability to send on S6a interface.
- **message**: Configures MME capability to send message on S6a interface.
- **nor**: Configures MME capability to send Notify Request (NOR) on S6a interface.
- **trigger**: Configures trigger to send the message.
- **mnrf**: Sends message to trigger MNRF flag on S6a interface (SMS in MME).
- **no**: Disables sending the NOR on S6a interface.
- This command is enabled by default.

Verifying the Configuration

Use the following command to verify whether Notify Request (MME S6a Message Options) is enabled or disabled:

```
show call-control-profile full all
```

Configuring Queue Timers

Use the following configuration to configure the MT Queue, TC1N, TR1N, and TR2N timers.

```
configure
   context context_name
      mme-service mme_svc_name
         emm { mt-queue-timeout mtq_timer | tc1n-timeout tc1n_timer | 
tr1n-timeout tr1n_timer | tr2n-timeout tr2n_timer }
         default emm { mt-queue-timeout | tc1n-timeout | tr1n-timeout | 
tr2n-timeout }
         end
```

NOTES:

- **context** *context_name*: Creates or specifies an existing context and enters the Context Configuration mode. *context_name* specifies the name of a context entered as an alphanumeric string of 1 to 79 characters.
- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.
- **mt-queue-timeout** *mtq_timer*: Configures the timer to hold MT SMS in MT queue. MT SMS will be present in the queue while the previous SMS is being processed. The timer expiry will return error to SMSC for an absent subscriber. *mtq_timer* specifies the timeout in seconds, as an integer from 1 to 300.

  Default: 30 seconds
- **tc1n-timeout** *tc1n_timer*: Configures the retransmission timer to send CP SMS data to UE for MO/MT scenario. *tc1n_timer* specifies the timeout in seconds, as an integer from 1 to 20.

  Default: 5 seconds
- **tr1n-timeout** *tr1n_timer*: Configures the wait time to receive RP-Ack from UE for MT SMS, before sending error to SMSC. *tr1n_timer* specifies the timeout in seconds, as an integer from 1 to 300.

  Default: 30 seconds
- **tr2n-timeout** *tr2n_timer*: Configures the wait time to send RP-Ack to UE for MO SMS, before sending protocol error to UE. *tr2n_timer* specifies the timeout in seconds, as an integer from 1 to 300.

  Default: 30 seconds
- **default**: Resets the specified timer timeout to the default value.

Verifying the Configuration

Use the following command to verify the configuration for TC1N, TR1N, TR2N, and MT Queue timeout:

```
show mme-service [ all | name service_name ]
```

Configuring CP Data Retransmissions

Use the following configuration to configure the maximum number of retransmissions of CP data for MO or MT SMS scenario in MME.

```
configure
   context context_name
      mme-service service_name
         [ default ] cp-data-max-retransmissions num_retrans
         end
```

NOTES:

- **context** *context_name*: Creates or specifies an existing context and enters the Context Configuration mode. *context_name* specifies the name of a context entered as an alphanumeric string of 1 to 79 characters.
- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.

- **cp-data-max-retransmissions** *num_retrans*: Configures the number of times CP Data for SMS is retransmitted. *num_retrans* must be an integer from 1 to 10.
- **default**: Sets the default value to 2.

Verifying the Configuration

Use the following command to verify the count for maximum retransmissions of CP Data:

```
show mme-service [ all | name service_name ]
```

Configuring Heuristic paging for PS-SMS traffic via MME

Use the following configuration to configure Heuristic paging for PS-SMS traffic via MME.

```
configure
   context context_name
      lte-policy
         paging-map  LTE_paging_map_name
            precedence  map_precedence  traffic-type ps sms paging-profile
LTE_paging_profile_name
         end
```

NOTES:

- **sms**: Configures paging profile for SMS via SGd.

Important For more information on Heuristic paging see *Heuristic and Intelligent Paging* section of *MME Administration Guide*.

Monitoring and Troubleshooting

This section provides information on the show commands and bulk statistics available for the SMS Support feature.

Show Commands and/or Outputs

This section provides information regarding show commands and their outputs for the SMS Support feature.

show call-control-profile full all

The output of this command includes the following fields:

- SMS in MME — Displays the configured value (preferred / not-preferred) for SMS in MME.
- SMSC Address — Displays the configured SMSC address.
- Send SMS Subscription Request to HSS — Indicates whether the SMS Subscription Request to HSS is enabled or disabled.

- Send SMS Subscription Notification to UE — Indicates whether the SMS Subscription Notification to UE is enabled or disabled.
- MME S6a Message Options:
  - Notify Req (Trigger : MNRF flag) — Indicates whether the MNRF flag trigger for Notify Request is enabled or disabled.
- MME SGd Message Options:
  - Alert SC Request (Trigger : MNRF flag) — Indicates whether the MNRF flag trigger for Alert SC Request is enabled or disabled.

show mme-service all

The output of this command includes the following fields:

- SMSC Context — Displays the name of the context in which SMSC service is configured.
- SMSC Service — Displays the name of the SMSC service associated with the MME service.
- TC1N Timeout — Displays the timeout duration configured for the TC1N timer. This timer can be configured to any value between 1 and 20 seconds. By default, it is 5 seconds.
- TR1N Timeout — Displays the timeout duration configured for the TR1N timer. This timer can be configured to any value between 1 and 300 seconds. By default, it is 30 seconds.
- TR2N Timeout — Displays the timeout duration configured for the TR2N timer. This timer can be configured to any value between 1 and 300 seconds. By default, it is 30 seconds.
- MT Queue Timeout — Displays the timeout duration configured for the MT Queue timer. This timer can be configured to any value between 1 and 300 seconds. By default, it is 30 seconds.
- CP Data Max Retransmissions Count — Displays the number of times CP Data for SMS is retransmitted.

show mme-service session full all

The output of this command includes the following fields:

- SMS Capability Information:
  - SGd Enabled — Displays Yes or No to indicate whether SGd is enabled or not.
  - MS Not Reachable — Displays Yes or No to indicate whether MS Not Reachable is enabled or not.
  - MS Memory Capacity Exceeded — Displays Yes or No to indicate whether MS memory capacity has exceeded.

show mme-service statistics

The output of this command includes the following fields:

- Paging Initiation for PS SMS Events:
  - Attempted — The total number of ECM statistics-related PS SMS Paging Initiation events that were attempted.

- Success — The total number of ECM statistics-related PS SMS Paging Initiation events that were successful.
- Failures — The total number of ECM statistics-related PS SMS Paging Initiation events that failed.
- Success at Last n eNB — The total number of ECM statistics-related PS SMS Paging Initiation events that succeeded at the last known eNodeB.
- Success at Last TAI — The total number of ECM statistics-related PS SMS Paging Initiation events that succeeded at an eNodeB in the TAI from which the UE was last heard.
- Success at TAI List — The total number of ECM statistics-related PS SMS Paging Initiation events that succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE.

show smsc-service name <smsc_svc_name>

The output of this command includes the following fields:

- Service name — Displays the name of the configured SMSC service.
- Context — Displays the name of the configured context.
- Status — Displays the status of the SMSC service.
- Diameter endpoint — Displays the configured Diameter endpoint name.
- Diameter dictionary — Displays the configured Diameter dictionary.
- Tmsi — Displays the configured TMSI value.
- Non-broadcast-Lai — Displays the configured non-broadcast MCC, MNC, and LAC values.
- MME-address — Displays the configured MME address.

show smsc-service statistics all

The output of this command includes the following fields:

- Session Stats:
  - Total Current Sessions — Displays the total number of current SMSC sessions.
  - Sessions Failovers — Displays the number of SMSC session failovers.
  - Total Starts — Displays the total number of SMSC session starts.
  - Total Session Updates — Displays the total number of SMSC session updates.
  - Total Terminated — Displays the total number of terminated SMSC sessions.
- Message Stats:
  - Total Messages Rcvd — Displays the total number of messages received.
  - Total Messages Sent — Displays the total number of messages sent.
  - OF Request — Displays the total number of OF requests.
  - OF Answer — Displays the total number of OF answers.

  - OFR Retries — Displays the total number of OFR retries.
  - OFR Timeouts — Displays the total number of OFR timeouts.
  - OFA Dropped — Displays the total number of OFA dropped.
  - TF Request — Displays the total number of TF requests.
  - TF Answer — Displays the total number of TF answers.
  - TFR Retries — Displays the total number of TFR retries.
  - TFA Timeouts — Displays the total number of TFA timeouts.
  - TFA Dropped — Displays the total number of TFA dropped requests.
  - AL Request — Displays the total number of AL requests.
  - AL Answer — Displays the total number of AL answers.
  - ALR Retries — Displays the total number of ALR retries.
  - ALR Timeouts — Displays the total number of ALR timeouts.
  - ALA Dropped — Displays the total number of ALA dropped.

- Message Error Stats:
  - Unable To Comply — Displays the total number of message errors containing the result code "Unable To Comply".
  - User Unknown — Displays the total number of message errors containing the result code "User Unknown".
  - User Absent — Displays the total number of message errors containing the result code "User Absent".
  - User Illegal — Displays the total number of message errors containing the result code "User Illegal".
  - SM Delivery Failure — Displays the total number of message errors containing the result code "SM Delivery Failure".
  - User Busy for MT SMS — Displays the total number of message errors containing the result code "User Busy for MT SMS".
  - Other Errors — Displays the total number of message errors containing the result code "Other Errors".

- Bad Answer Stats:
  - Auth-Application-Id — Displays the absence or unexpected value in Auth-Application-Id AVP.
  - Session-Id — Displays the absence or unexpected value in Session-Id AVP.
  - Origin-Host — Displays the absence of Origin-Host AVP.
  - Origin Realm — Displays the absence of Origin-Realm AVP.
  - Parse-Message-Errors — Displays the total number of parse errors in the message.
  - Parse-Mscc-Errors — Displays the total number of parse errors in MSCC AVP.

  - Miscellaneous — Displays the total number of other miscellaneous errors.

show smsc-service statistics summary

The output of this command includes the following fields:

- SMSC Session Stats:
  - Total Current Sessions — Displays the total number of current SMSC sessions.
  - Sessions Failovers — Displays the total number of SMSC session failovers.
  - Total Starts — Displays the total number of SMSC session starts.
  - Total Session Updates — Displays the total number of SMSC session updates.
  - Total Terminated — Displays the total number of terminated SMSC sessions.

show sms statistics mme-only verbose

The output of this command includes the following fields:

SMS Statistics:

Session Statistics:

- MO SMS (In Progress) — The total number of mobile originated (MO) SMS messages that are waiting in the MME to be delivered.
- MT SMS (In Progress) — The total number of mobile terminated (MT) SMS messages that are waiting in the MME to be delivered.
- MT SMS (In Queue) — The total number of mobile terminated SMS messages in the queue.
- SMMA (In Progress) — The total number of procedures for retrieval of available SMS memory in progress.
- MO-SMS Attempted — The total number of mobile originated SMS messages that are attempted to be delivered by the network.
- MO-SMS Successful — The total number of mobile originated SMS messages that are successfully delivered by the network.
- MT-SMS Attempted — The total number of mobile terminated SMS messages that are attempted to be delivered by the network.
- MT-SMS Successful — The total number of mobile terminated SMS messages that are successfully delivered by the network.
- SMMA Attempted — The total number of procedures for retrieval of available SMS memory attempted.
- SMMA Successful — The total number of procedures for retrieval of available SMS memory successful.

Message Statistics:

- CP Layer Messages:
  - CP Data (Tx) — The total number of protocol data units sent during connection setup.

  - CP Data (Rx) — The total number of protocol data units received during connection setup.
  - CP Ack (Tx) — The total number of Ack messages sent during connection setup.
  - CP Ack (Rx) — The total number of Ack messages received during connection setup.
  - CP Error (Tx) — The total number of protocol errors during connection setup in Tx message.
  - CP Error (Rx) — The total number of protocol errors during connection setup in Rx message.

- CP Error Cause Stats:
  - Network Failure (Tx)/(Rx) — The total number of protocol errors during connection setup due to network failure in Tx/Rx message.
  - Congestion (Tx)/(Rx) — The total number of protocol errors during connection setup due to congestion in Tx/Rx message.
  - Invalid TID (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid transaction ID (TID) in Tx/Rx message.
  - Invalid Semantic (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid semantics in Tx/Rx message.
  - Invalid Mand Info (Tx)/(Rx) — The total number of protocol errors during connection setup as mandatory information in Tx/Rx message is invalid.
  - Invalid Msg Type (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid Tx/Rx message type.
  - Invalid Prot State (Tx)/(Rx) — The total number of protocol errors during connection setup as protocol state in Tx/Rx message is invalid.
  - Invalid IE (Tx)/(Rx) — The total number of protocol errors during connection setup as information element in Tx/Rx message is invalid.
  - Protocol Error (Tx)/(Rx) — The total number of protocol errors during connection setup as protocol error in Tx/Rx message.
  - Undefined Cause (Tx)/(Rx) — The total number of protocol errors during connection setup due to unspecified error in Tx/Rx message.

- Message Drop Counters:
  - CP Data — The total number of CP data packets dropped during connection setup.
    - Retransmission Drops — The total number of data packets dropped during retransmission.
    - Unknown TID Drops — The total number of data packets dropped during connection setup due to unknown transaction ID (TID).
    - Invalid TID Drops — The total number of data packets dropped during connection setup due to invalid transaction ID (TID) received.
  - CP Ack — The total number of CP acknowledgement messages dropped during connection setup.
    - CP-ACK Drop for Invalid TID Rcvd — The total number of CP-Ack messages dropped during connection setup due to invalid transaction ID (TID) received.

  - CP Error — The total number of CP data packets dropped during connection setup due to error in connection.
    - CP-ERR Drop for Invalid TID Rcvd — The total number of CP-ERR messages dropped during connection setup due to invalid transaction ID (TID) received.

- RP Layer Messages:
  - RP Data (Tx) — The total number of protocol data units sent during message relay.
  - RP Data (Rx) — The total number of protocol data units received during message relay.
  - RP Ack (Tx) — The total number of Ack messages sent during message relay.
  - RP Ack (Rx) — The total number of Ack messages received during message relay.
  - RP Error (Tx) — The total number of protocol errors during message relay in Tx message.
  - RP Error (Rx) — The total number of protocol errors during message relay in Rx message.
  - RP SMMA (Rx) — The total number RP SMMA messages received.

- RP Error Cause Stats:
  - Unassigned Number (Tx) — The total number of protocol errors sent during message relay due to unassigned protocol number.
  - Opr. Determined Barring (Tx) — The total number of protocol errors sent during message relay due to operator determined barring.
  - Call Barred (Tx) — The total number of protocol errors sent during message relay due to call barring.
  - Reserved (Tx) — The total number of protocol errors sent during message relay due to reserved resources.
  - SM Transfer Rejected (Tx) — The total number of protocol errors sent during message relay due to session manager transfer rejection.
  - Destination Out Of Order (Tx) — The total number of protocol errors sent during message relay due to out of order on destination.
  - Unidentified Subscriber (Tx) — The total number of protocol errors sent during message relay due to unidentified subscriber.
  - Facility Rejected (Tx) — The total number of protocol errors sent during message relay due to facility rejection.
  - Unknown Subscriber (Tx) — The total number of protocol errors sent during message relay due to unknown subscriber.
  - Network Out Of Order (Tx) — The total number of protocol errors sent during message relay due to out-of-order network.
  - Temporary Failure (Tx) — The total number of protocol errors sent during message relay due to temporary failure in network.
  - Congestion (Tx) — The total number of protocol errors sent during message relay due to congestion in network.

    - Not Subscribed (Tx) — The total number of protocol errors sent during message relay as this service is not subscribed by subscriber.
    - Not Implemented (Tx) — The total number of protocol errors sent during message relay as this service is not yet implemented.
    - Interworking Error (Tx) — The total number of protocol errors sent during message relay due to interworking error between two networks or technology.
    - Resource Un-available (Tx) — The total number of protocol errors sent during message relay as resources are not available.
    - Memory Capacity Exceeded (Rx) — The total number of protocol errors received during message relay as capacity is exceeded.
    - Invalid Reference Number (Tx)/(Rx) — The total number of protocol errors during message relay as invalid reference in Tx/Rx message.
    - Invalid Semantic (Tx)/(Rx) — The total number of protocol errors during message relay due to invalid semantics in Tx/Rx message.
    - Invalid Mandatory Info (Tx)/(Rx) — The total number of protocol errors during message relay as mandatory information in Tx/Rx message is invalid.
    - Invalid Message Type (Tx)/(Rx) — The total number of protocol errors during message relay due to invalid Tx/Rx message type.
    - Invalid Protocol State (Tx)/(Rx) — The total number of protocol errors during message relay as protocol state in Tx/Rx message is invalid.
    - Invalid IE (Tx)/(Rx) — The total number of protocol errors during message relay as information element in Tx/Rx message is invalid.
    - Protocol Error (Tx)/(Rx) — The total number of RP ERROR messages sent/received with the cause Protocol Error in the message header.
    - Undefined Error (Tx)/(Rx) — The total number of protocol errors during message relay due to unspecified error in Tx/Rx message.

- Message Drop Counters:
    - RP Data — The total number of RP data packets dropped during message relay.
    - RP Ack — The total number of RP acknowledgement messages dropped during message relay.
    - RP Error — The total number of RP data packets dropped during message relay due to error in connection.
    - RP Decode Failures — The total number of messages dropped during message relay due to invalid transaction ID (TID) received.

General Statistics:

- Concatenated MO SMS — The total number of concatenated mobile originated SMS messages.
- CP Timer Expiry — The total number of events when timer expired during connection setup.

- TR1N Timer — The total number of events when TR1N timer expired during mobile terminated SMS is in wait state for RP-ACK.
- TR2N Timer — The total number of events when TR2N timer expired during mobile terminated SMS is in wait state to send RP-ACK.
- CP Data Retrans — The total number of protocol data units retransmitted during connection setup.
- RP Msg Encode Fail — The total number of message encoding failures during message relay.
- CP Data Tx Fail — The total number of protocol data units with Tx messages failed during connection setup.
- CP Data Inv TID — The total number of protocol data units with invalid transaction ID (TID) during connection setup.
- Max Retrans Reached — The total number of events when retransmission limit is exhausted during connection setup.
- SMSC Addr Restricted — The total number of SMSC addresses restricted.
- MO SMSC Addr Restricted — The total number of mobile originated SMSC addresses restricted.
- MT SMSC Addr Restricted — The total number of mobile terminated SMSC addresses restricted.
- CP-DATA No Cp Ack Rx — The total number of mobile terminated messages failed as no acknowledgement is received during connection setup.
  - Release Indication Waiting MO CP-ACK Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol acknowledgement messages that are being delivered.
  - Release Indication Waiting MO CP-DATA Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol data messages that are being delivered.
  - Release Indication Waiting MO CP-ERR Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol error messages that are being delivered.
  - Release Indication Waiting MT CP-DATA Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol data messages that are being delivered.
  - Release Indication Waiting MT CP-ACK Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol acknowledgement messages that are being delivered.
  - Release Indication Waiting MT CP-ERR Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol error messages that are being delivered.
- MT-SMS Failures:
  - IMSI Record Not Found — The total number of mobile terminated messages failed as IMSI record is not available.
  - Busy Subscriber — The total number of mobile terminated messages failed due to busy subscriber.

- Detached Subscriber — The total number of mobile terminated messages failed due to detached subscriber.
- MT Queue Full — The total number of mobile terminated messages failed as messaged queue was full.

Bulk Statistics

This section provides information on the bulk statistics supported for the SMS feature.

MME Schema

The following SMS feature related bulk statistics are available in the MME schema.

Bulk Statistics	Description
ps-sms-paging-init-events-attempted	The total number of PS SMS Paging Initiation events that were attempted.
ps-sms-paging-init-events-success	The total number of PS SMS Paging Initiation events that were successful.
ps-sms-paging-init-events-failures	The total number of PS SMS Paging Initiation events that failed.
ps-sms-paging-last-enb-success	The total number of PS SMS Paging Initiation events that succeeded at the last known eNodeB.
ps-sms-paging-last-tai-success	The total number of PS SMS Paging Initiation events that succeeded at an eNodeB in the TAI from which the UE was last heard.
ps-sms-paging-tai-list-success	The total number of PS SMS Paging Initiation events that succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE.

MME-SMS Schema

The following SMS feature related bulk statistics are available in the MME-SMS schema.

Bulk Statistics	Description
mo-sms-in-progress	The total number of mobile originated (MO) SMS messages that are waiting in the MME to be delivered.
mt-sms-in-progress	The total number of mobile terminated (MT) SMS messages that are waiting in the MME to be delivered.
mt-sms-in-queue	The total number of mobile terminated SMS messages in the queue.

Bulk Statistics	Description
sms-memory-available-in-progress	The total number of procedures for retrieval of available SMS memory in progress.
mo-sms-attempted	The total number of mobile originated SMS messages that are attempted to be delivered by the network.
mo-sms-successful	The total number of mobile originated SMS messages that are successfully delivered by the network.
mt-sms-attempted	The total number of mobile terminated SMS messages that are attempted to be delivered by the network.
mt-sms-successful	The total number of mobile terminated SMS messages that are successfully delivered by the network.
sms-memory-available-attempted	The total number of procedures for retrieval of available SMS memory attempted.
sms-memory-available-successful	The total number of procedures for retrieval of available SMS memory successful.
conn-prot-data-tx	The total number of protocol data units sent during connection setup.
conn-prot-data-rx	The total number of protocol data units received during connection setup.
conn-prot-ack-tx	The total number of Ack messages sent during connection setup.
conn-prot-ack-rx	The total number of Ack messages received during connection setup.
conn-prot-error-tx	The total number of protocol errors during connection setup in Tx message.
conn-prot-error-rx	The total number of protocol errors during connection setup in Rx message.
conn-prot-error-nwt-fail-tx	The total number of protocol errors during connection setup due to network failure in Tx message.
conn-prot-error-nwt-fail-rx	The total number of protocol errors during connection setup due to network failure in Rx message.
conn-prot-error-congestion-tx	The total number of protocol errors during connection setup due to congestion in Tx message.
conn-prot-error-congestion-rx	The total number of protocol errors during connection setup due to congestion in Rx message.

Bulk Statistics	Description
conn-prot-error-invalid-tid-tx	The total number of protocol errors during connection setup due to invalid transaction ID (TID) in Tx message.
conn-prot-error-invalid-tid-rx	The total number of protocol errors during connection setup due to invalid transaction ID (TID) in Rx message.
conn-prot-error-invalid-semantic-tx	The total number of protocol errors during connection setup due to invalid semantics in Tx message.
conn-prot-error-invalid-semantic-rx	The total number of protocol errors during connection setup due to invalid semantics in Rx message.
conn-prot-error-invalid-mand-info-tx	The total number of protocol errors during connection setup as mandatory information in Tx message is invalid.
conn-prot-error-invalid-mand-info-rx	The total number of protocol errors during connection setup as mandatory information in Rx message is invalid.
conn-prot-error-invalid-msg-type-tx	The total number of protocol errors during connection setup due to invalid Tx message type.
conn-prot-error-invalid-msg-type-rx	The total number of protocol errors during connection setup due to invalid Rx message type.
conn-prot-error-invalid-prot-state-tx	The total number of protocol errors during connection setup as protocol state in Tx message is invalid.
conn-prot-error-invalid-prot-state-rx	The total number of protocol errors during connection setup as protocol state in Rx message is invalid.
conn-prot-error-invalid-ie-tx	The total number of protocol errors during connection setup as information element in Tx message is invalid.
conn-prot-error-invalid-ie-rx	The total number of protocol errors during connection setup as information element in Rx message is invalid
conn-prot-error-protocol-error-tx	The total number of protocol errors during connection setup as protocol error in Tx message.
conn-prot-error-protocol-error-rx	The total number of protocol errors during connection setup as protocol error in Rx message.
conn-prot-error-undefined-cause-tx	The total number of protocol errors during connection setup due to unspecified error in Tx message.
conn-prot-error-undefined-cause-rx	The total number of protocol errors during connection setup due to unspecified error in Rx message.

Bulk Statistics	Description
conn-prot-data-dropped	The total number of data packets dropped during connection setup.
conn-prot-ack-dropped	The total number of Ack messages dropped during connection setup.
conn-prot-error-dropped	The total number of data packets dropped during connection setup due to error in connection.
conn-prot-inval-tid-rcvd	The total number of messages dropped during connection setup due to invalid transaction ID (TID) received.
relay-prot-data-tx	The total number of protocol data units sent during message relay.
relay-prot-data-rx	The total number of protocol data units received during message relay.
relay-prot-ack-tx	The total number of Ack messages sent during message relay.
relay-prot-ack-rx	The total number of Ack messages received during message relay.
relay-prot-err-tx	The total number of protocol errors during message relay in Tx message.
relay-prot-err-rx	The total number of protocol errors during message relay in Rx message.
relay-prot-err-unassigned-num	The total number of protocol errors during message relay due to unassigned protocol number.
relay-prot-err-opr-determ-barring	The total number of protocol errors during message relay due to operator determined barring.
relay-prot-err-call-barred	The total number of protocol errors during message relay due to call barring.
relay-prot-err-reserved	The total number of protocol errors during message relay due to reserved resources.
relay-prot-err-sm-transfer-rej	The total number of protocol errors during message relay due to session manager transfer rejection.
relay-prot-err-dest-out-of-order	The total number of protocol errors during message relay due to out of order on destination.
relay-prot-err-unidentified-subs	The total number of protocol errors during message relay due to unidentified subscriber.

Bulk Statistics	Description
relay-prot-err-facility-rej	The total number of protocol errors during message relay due to facility rejection.
relay-prot-err-unknown-subs	The total number of protocol errors during message relay due to unknown subscriber.
relay-prot-err-netwk-out-of-order	The total number of protocol errors during message relay due to out-of-order network.
relay-prot-err-temp-fail	The total number of protocol errors during message relay due to temporary failure in network.
relay-prot-err-congestion	The total number of protocol errors during message relay due to congestion in network.
relay-prot-err-not-subscribed	The total number of protocol errors during message relay as this service is not subscribed by subscriber.
relay-prot-err-not-implemented	The total number of protocol errors during message relay as this service is not yet implemented.
relay-prot-err-interworking-err	The total number of protocol errors during message relay due to interworking error between two networks or technology.
relay-prot-err-res-unavail	The total number of protocol errors during message relay as resources are not available.
relay-prot-err-mem-capacity-exceed	The total number of protocol errors during message relay as capacity is exceeded.
relay-prot-err-inval-ref-num-tx	The total number of protocol errors during message relay as invalid reference in Tx message.
relay-prot-err-inval-ref-num-rx	The total number of protocol errors during message relay as invalid reference in Rx message.
relay-prot-err-inval-semantic-tx	The total number of protocol errors during message relay due to invalid semantics in Tx message.
relay-prot-err-inval-semantic-rx	The total number of protocol errors during message relay due to invalid semantics in Rx message.
relay-prot-err-inval-mand-info-tx	The total number of protocol errors during message relay as mandatory information in Tx message is invalid.
relay-prot-err-inval-mand-info-rx	The total number of protocol errors during message relay as mandatory information in Rx message is invalid.
relay-prot-err-inval-msg-type-tx	The total number of protocol errors during message relay due to invalid Tx message type.

Bulk Statistics	Description
relay-prot-err-inval-msg-type-rx	The total number of protocol errors during message relay due to invalid Rx message type.
relay-prot-err-inval-prot-state-tx	The total number of protocol errors during message relay as protocol state in Tx message is invalid.
relay-prot-err-inval-prot-state-rx	The total number of protocol errors during message relay as protocol state in Rx message is invalid.
relay-prot-err-inval-ie-tx	The total number of protocol errors during message relay as information element in Tx message is invalid.
relay-prot-err-inval-ie-rx	The total number of protocol errors during message relay as the information element in Rx message is invalid.
relay-prot-err-protocol-error-rx	The total number of RP ERROR messages sent with the cause Protocol Error in the message header.
relay-prot-err-protocol-error-tx	The total number of protocol errors during message relay when there are protocol errors in the transmitted message.
relay-prot-err-unidentified-error-tx	The total number of protocol errors during message relay due to unspecified error in Tx message.
relay-prot-err-unidentified-error-rx	The total number of protocol errors during message relay due to unspecified error in Rx message.
relay-prot-smma-rx	The total number RP SMMA messages received.
relay-prot-data-dropped	The total number of data packets dropped during message relay.
relay-prot-ack-dropped	The total number of Ack messages dropped during message relay.
relay-prot-error-dropped	The total number of data packets dropped during message relay due to error in connection.
relay-prot-decode-failure	The total number of messages dropped during message relay due to invalid transaction ID (TID) received.
concat-mo-sms	The total number of concatenated mobile originated SMS messages.
conn-prot-timer-expiry	The total number of events when timer expired during connection setup.
tr1n-timer-expiry	The total number of events when TR1N timer expired during mobile terminated SMS is in wait state for RP-ACK.

Bulk Statistics	Description
tr2n-timer-expiry	The total number of events when TR2N timer expired during mobile terminated SMS is in wait state to send RP-ACK.
conn-prot-data-retrans	The total number of protocol data units retransmitted during connection setup.
relay-prot-msg-encode-fail	The total number of message encoding failures during message relay.
conn-prot-data-tx-fail	The total number of protocol data units with Tx messages failed during connection setup.
conn-prot-data-inval-tid	The total number of protocol data units with invalid transaction ID (ID) during connection setup.
conn-prot-max-retrans-reached	The total number of events when retransmission limit is exhausted during connection setup.
mt-fail-no-db-rec	The total number of mobile terminated messages failed as database record is not available.
mt-fail-conn-prot-data-no-ack-rcvd	The total number of mobile terminated messages failed as no acknowledgement is received during connection setup.
mt-fail-fwd-busy-subs	The total number of mobile terminated messages failed due to busy subscriber.
mt-fail-fwd-detached-subs	The total number of mobile terminated messages failed due to detached subscriber.
mt-fail-mt-queue-full	The total number of mobile terminated messages failed as messaged queue was full.

CHAPTER 32

Support for OSP 13 with RHEL 7.5

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required
Related Features in this Release	Not Applicable
Related Documentation	• *Ultra Gateway Platform System Administration Guide* • *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide* • *Cisco Ultra Services Platform NETCONF API Guide*

Revision History

Revision Details	**Release**
First introduced.	6.5

Feature Description

This release includes support for RedHat 7.5/OSP 13 for use as the VIM.

OSP 13 with RHEL 7.5 has been validated only for Standalone AutoVNF-based deployments of the UGP VNF.

For more information on deploying RHEL 7.5/OSP 13, see the RedHat user documentation.

CHAPTER 33

TCP Proxy-Enabled Flows

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
With this release, behavior has changed for TCP proxy-enabled flows, when Port-reuse feature CLI command is either enabled or disabled.	21.11.7
First introduced.	Pre 21.2

Feature Changes

The change in behavior is related to the following scenarios:

- Scenario #1: When the Port-reuse feature CLI command is not used, that is, flow may be active, in 2msl, or pending deletion state.
- Scenario #2: When the Port-reuse feature CLI command is used, that is, flow is in 2msl state.

Previous Behavior: In Scenario #1, new SYN with existing 5-tuple was handled by the application on the old flow. The remaining packets, following the SYN, were treated as a non-SYN flow.

In Scenario #2, the application sent the last ACK toward the server, cleared the flow, and created a new flow to send the new SYN.

New Behavior: For Scenario#1, if flow is in active state, new SYN is dropped until flow exists on the chassis. If flow is in 2msl or pending deletion state, the flow is cleared immediately. New SYN is always handled on a new flow. Non-SYN flow is not created in this scenario.

For Scenario #2, old flow is cleared immediately (last ACK will already be sent by the Gi stack), and new SYN is handled on a new flow.

Customer Impact: This behavior change is applicable only to TCP proxy-enabled flows. There is no change in behavior for non-proxied flows.

CHAPTER 34

User Session Management for UAS and UEM VMs

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	UGP
Feature Default	Enabled - Always On
Related Features in this Release	Not Applicable
Related Documentation	• *Ultra Services Platform Deployment Automation Guide* • *UEM-based VNF Deployment Guide*

Revision History

Revision Details	**Release**
First introduced.	6.5

Feature Description

UAS manages the session idle timeout configuration in order to be compliant with PSB requirements. The system idle timeout is now set to 5 minutes, after which the SSH session and CONFD CLI session will be terminated automatically.