Release Change Reference, StarOS Release 21.19/Ultra Services Platform Release 6.13

First Published: 2020-04-30

Last Modified: 2021-07-16

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

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

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

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

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

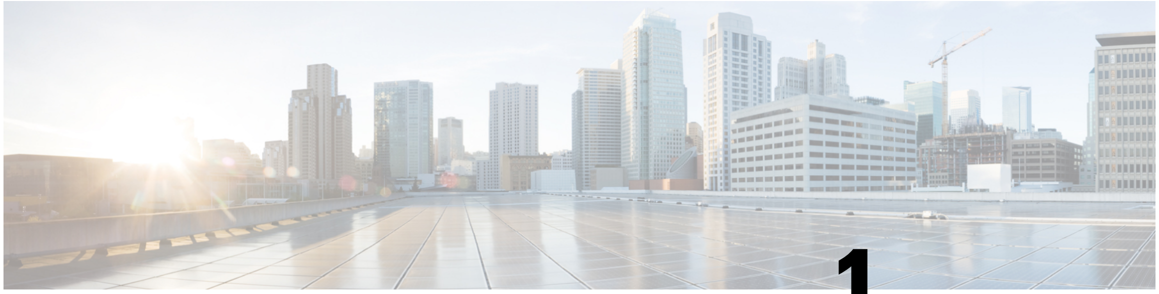
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

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

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

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



CHAPTER 1

Release 21.19/N6.13 Features and Changes Quick Reference

Release 21.19/6.13 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Bearer Re-establishment	SAEGW P-GW	21.19.1
Customized Interface Between MME/SGSN and GMPC, on page 17	MME SGSN	21.19
Cisco Ultra Traffic Optimization	SAEGW P-GW	21.19.1
Deprecation of Manual Scaling, on page 69	UAS	6.0
Events Monitoring, on page 71	MME	21.19
HSS and AuC Interworking Configuration Enhancement, on page 103	MME	21.19
Ignoring SAI, RAI, or CGI in Change Notification Request Messages, on page 105	P-GW S-GW	21.19.11
Migrating 3G to 4G Context , on page 109	P-GW	21.19.9
Non-IP Data Over SCEF, on page 111	MME C-SGN	21.19
NR UE Security Capability IE for 5G Security Support on MME, on page 121	MME	21.19

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
N26 Interface Support, on page 125	MME	21.19
Rewrite TTL on Downlink Packets, on page 147	ECS	21.19.1
Routing Based on Realm Name S6B	SAEGW P-GW	21.19.1
Supporting Larger Source to Target Container IE in Handover, on page 155	MME	21.19.6
Support for aaa-acct-arch Bulkstats Counter at System Level, on page 159	P-GW	21.19.6

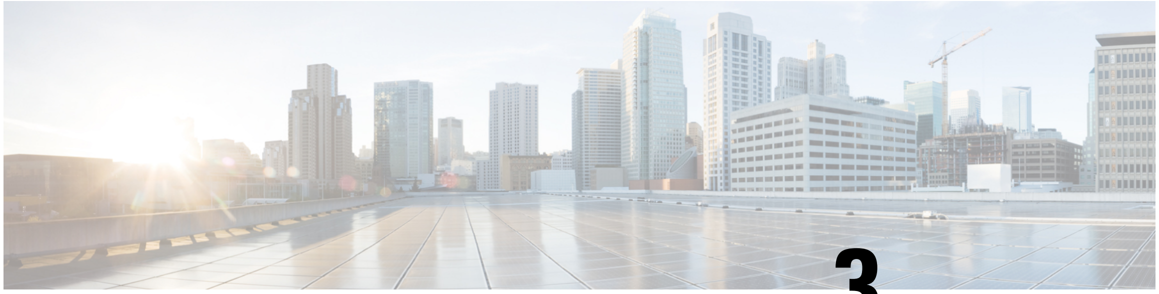
CHAPTER 2

Feature Defaults Quick Reference

Feature Defaults

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

Feature	**Default**
Bearer Re-establishment	Disabled - Configuration Required
Customized Interface between MME/SGSN and GMPC	Disabled - Configuration Required
CUTO TODR Enhancements with IMSI, FLOW-ID and ULI Information	Disabled - Configuration Required
Deprecation of Manual Scaling	Disabled - Configuration Required
Events Monitoring	Disabled - Configuration Required
HSS and AuC Interworking Configuration Enhancement	Enabled - Always-on
Ignoring SAI, RAI, or CGI in Change Notification Request Messages	Disabled - Configuration Required
Migrating 3G to 4G Context	Enabled - Configuration Required
Non-IP Data Over SCEF	Disabled - Configuration Required
NR UE Security Capability IE for 5G Security Support on MME	Enabled - Configuration Required
N26 Interface Support	Enabled - Always-on
Rewrite TTL on Downlink Packets	Disabled - Configuration Required
Routing Based Realm Name S6B	Disabled - Configuration Required
Supporting Larger Source to Target Container IE in Handover	Enabled - Always On
Support for aaa-acct-arch Bulkstats Counter at System Level	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 21.19 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 21.19 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 7
- Deprecated Bulk Statistics, on page 8

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.19.

MME Schema

The following bulk statistics are added in the MME schema in support of the Monitoring Events feature.

Counters	Description
monitored-subscribers	The current total number of monitored subscribers for monitoring events.
monitored-loss-of-connectivity	The current total number of loss of connectivity events configured.
monitored-ue-reachability	The current total number of UE reachability events configured.
monitored-location-reporting	The current total number of location reporting events configured.
monitored-communication-failure	The current total number of communication failure events configured.
monitored-availability-after-ddn-failure	The current total number of availability after DDN failure events configured.

Counters	Description
monitored-availability-after-ddn-failure-idleind	The current total number of availability after DDN failure and idle status indication events configured.
monitored-ue-reachability-idleind	The current total number of UE reachability and idle status indication events configured.
monitored-pdn-connecitivty-status	The current total number of PDN connectivity status events configured.
monte-rx-loss-of-connectivity	The total number of loss of connectivity monitoring events configured.
monte-rx-ue-reachability	The total number of UE reachability monitoring events configured.
monte-rx-location-reporting	The total number of location reporting monitoring events configured.
monte-rx-communication-failure	The total number of communication failure monitoring events configured.
monte-rx-availability-after-ddnfailure	The total number of availability after DDN failure monitoring events configured.
monte-rx-number-of-ue-geoarea	The total number of UEs present in a geographical area monitoring events configured.
monte-rx-uereachability-idleind	The total number of UE reachability and idle status indication monitoring events configured.
monte-rx-availability-ddnfailure-idleind	The total number of availability after DDN failure and idle status indication monitoring events configured.
monte-rx-pdn-connectivity-status	The total number of PDN connectivity status monitoring events configured.
monte-tx-loss-of-connectivity	The total number of loss of connectivity monitoring reports sent.
monte-tx-ue-reachability	The total number of UE Reachability monitoring reports sent.
monte-tx-location-reporting	The total number of location reporting monitoring reports sent.
monte-tx-communication-failure	The total number of communication failure monitoring reports sent.
monte-tx-availability-after-ddnfailure	The total number of availability after DDN failure monitoring reports sent.
monte-tx-number-of-ue-geoarea	The total number of number of UEs present in a geographical area monitoring reports sent.
monte-tx-uereachability-idleind	The total number of UE reachability and idle status indication monitoring reports sent.
monte-tx-availability-ddnfailure-idleind	The total number of availability after DDN failure and idle status indication monitoring reports sent.
monte-tx-pdn-connectivity-status	The total number of PDN connectivity status monitoring reports sent.

Counters	Description
monte-del-ue-reachability	The total number of deleted UE Reachability monitoring events.
monte-del-location-reporting	The total number of deleted location reporting monitoring events.
monte-del-communication-failure	The total number of deleted communication failure monitoring events.
monte-del-availability-after-ddn-failure	The total number of deleted availability after DDN failure monitoring events.
monte-del-uereachability-idleind	The total number of deleted UE reachability and idle status indication monitoring events.
monte-del-availability-ddnfailure-idleind	The total number of deleted availability after DDN failure and idle status indication monitoring events.
monte-del-pdn-connectivity-status	The total number of deleted PDN connectivity status monitoring events.
monte-del-loss-of-connectivity	The total number of deleted loss of connectivity monitoring events.

Modified Bulk Statistics

This section identifies the modified bulk statistics schemas modified in release 21.19.

The following bulk statistics are modified in the MME schema under the **show bulkstats variables** command.

- **apn-expansion**–The identification number of the context configured on the system that is currently facilitating the APN-QCI service. This is an internal reference number.
- **cs-network-ranap**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **cs-network-rtp**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **cs-network-sccp**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **fa**–The name of the VPN associated with the interface.
- **gprs-bk**–The name of the VPN associated with the interface.
- **gtpc** –The name of the context configured on the system that is currently facilitating the EGTPC service.
- **ha**–The identification number of the context configured on the system that is currently facilitating the MIPHA service. This is an internal reference number.
- **iups-bk**–The identification number of the context configured on the system that is currently facilitating the IUPS service. This is an internal reference number.
- **link-aggr** –Alphanumeric string indicating LAG.
- **map-bk**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.

- **ps-network-gtpu**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **ps-network-ranap**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **ps-network-sccp**–Indicates the name of the Packet Switch (PS) Network connected with specific HNB-GW on which statistics are collected or displayed.
- **rulebase**–The name of the billing plan associated with the subscriber.
- **tai**–Configured MME of a TAI.

Deprecated Bulk Statistics

None in this release.

CHAPTER 4

SNMP MIB Changes in StarOS 21.19 and USP 6.13

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.19 and Ultra Services Platform (USP) 6.13 software releases.

SNMP MIB Object Changes for 21.19

This section provides information on SNMP MIB alarm changes in release 21.19.

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 21.19.

- starX3ContextName
- starX3srcIPAddr
- starX3srcPort
- starX3dstIPaddr
- starX3dstPort
- StarX3ConnType
- starX3ConnCauseStr

Modified SNMP MIB Object

None in this release.

Deprecated SNMP MIB Object

None in this release.

SNMP MIB Alarm Changes for 21.19

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 21.19

This section provides information on SNMP MIB alarm changes in release 21.19.

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

New SNMP MIB Conformance

None in the release.

Modified SNMP MIB Conformance

None in the release.

Deprecated SNMP MIB Conformance

None in the release.

SNMP MIB Object Changes for 6.13

There are no new, modified, or deprecated SNMP MIB object changes in this release.

SNMP MIB Alarm Changes for 6.13

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 6.13

There are no new, modified, or deprecated SNMP MIB conformance changes in this release.

CHAPTER 5

Bearer Re-establishment

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
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* • *P-GW Administration Guide* • *SAEGW Administration Guide*

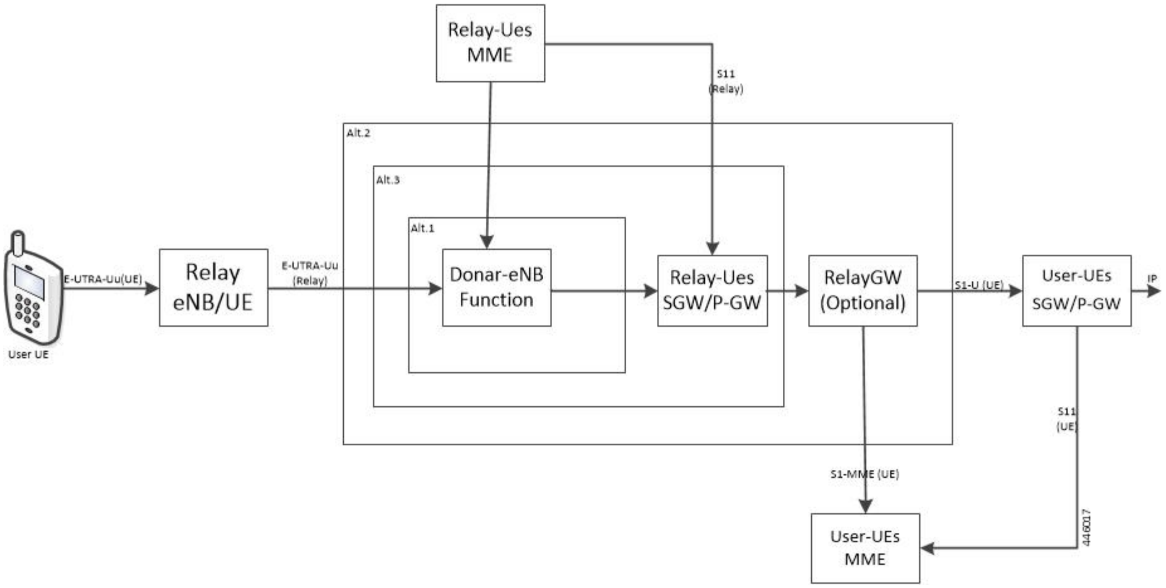
Table 1: Revision History

Revision Details	**Release**
First introduced	21.19

Introduction to Bearer Re-establishment

A UE Relay Network comprises of multiple RAN and EPC nodes. An example network configuration presented in 3GPP TS 36.806 is shown below.

Figure 1: Example of Network Configuration



In some deployments (unlike in the diagram above), one MME can play the role of both User-UE MME and Relay-UE MME.

In a UE Relay network, System Architecture Evolution Gateways (SAEGWs) are deployed to play the role of combined ‘Relay-UE’s SGW/P-GW’. The SAEGWs are configured using only local-policy (that is no connection to PCRF).

As part of initial attach request from Relay Node UE, P-GW (in the aforementioned SAEGW) creates dedicated bearers (for example, QCI-1 for GBR and QCI5 for non-GBR) on top of the default bearer (for example, QCI6). This is done based on an appropriate local policy configuration which is described in later sections of this chapter.

When RF condition degrades, Relay Node UE loses the RRC connection to macro eNB. As a result, macro eNB initiates an S1 Release procedure with abnormal cause (for example, ‘Radio Connection with UE lost’ or ‘unspecified’). For these type of causes MME typically preserves non-GBR bearer and deletes GBR bearers. As a result, GBR bearers (for example, QCI-1 bearer) is deleted by the MME.

After the RRC Connection is re-established, the Relay Node UE sends Service Request to the MME. The MME sends Initial Context Setup Request to macro eNB to set up the previously preserved non-GBR bearers. The MME does not re-establish the GBR bearer since it was not preserved. As a result, Relay Node UE does not have the GBR bearer until a full re-attach procedure occurs.

Since GBR bearer is not re-established, the GBR traffic is carried over the default non-GBR bearer and the voice performance is degraded.

Using this feature SAEGW is able to re-establish the previously deleted GBR bearer when MME sends the Modify Bearer Request to re-establish the preserved the non-GBR bearers.

How it Works

SAEGW re-establishes the previously deleted GBR bearer when MME sends the Modify Bearer Request, to re-establish the preserved non-GBR bearers.

This is achieved in SAEGW using two different mechanisms:

- Forwarding the Modify Bearer Request from SGW to P-GW
- P-GW to invoke local policy with a new event restore-bearers

Enabling Modify Bearer Request Forward from S-GW to P-GW

Use the following configuraion to enable forced forwarding of Modify Bearer Request from S-GW to P-GW:

```
configure
   context context_name
      sgw-service service_name
         enable-bearer-restore
         end
```

In S-GW service, whenever **enable-bearer-restore** option is set, modify bearer request is forwarded by S-GW to P-GW. It happens when the S-GW service is under SAEGW service.

For example:

```
config
   context ingress
     sgw-service sgw-service
        enable-bearer-restore
```

Note

- Without this CLI, S-GW only forwards the Modify Bearer Request message to P-GW if certain conditions are met. For example. RAT change, TimeZone change, ULI change, Handover indication flag, and so on as per 3GPP specifications.
- To avoid forwarding Modify Bearer Requests unnecessarily to P-GW, **enable-bearer-restore** should only be used when local policy is configured for **restore-bearer** event as described in next section.

P-GW Invokes Local Policy with New Event Restore-Bearers

A list of events supported under `eventbase` is enhanced with `restore-bearers`. This event is invoked when P-GW gets a Modify Bearer Request from S-GW. If local policy configuration has the **restore-bearer** event under **eventbase** then corresponding rules are applied.

Use the following configuration to re-establish missing bearers under local policy:

```
configure
   local-policy-service local_policy_name
      eventbase eventbase_name
```

```
[ no ] rule priority integer
  event restore-bearers ruledef ruledef_name actiondef actiondef_name
  end
```

Following is an example for local policy configuration:

```
  local-policy-service local_policy
    ruledef apn_apn2
      condition priority 100 apn match apn2.com
    #exit

ruledef apn_apn1
      condition priority 100 apn match apn1.com
    #exit

    ruledef ded_bearer_creation_fail
      condition priority 100 apn match apn2.com
      condition priority 200 cause-code match 72 73 90 100 110
    #exit

    actiondef apn2_newcall
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit

    actiondef apn2_restore_bearer_config
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit

    actiondef apn2_retry_dedicated_bearer
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
      action priority 700 retry-count 4
      action priority 2000 allow-session
    #exit

actiondef apn1_newcall
      action priority 100 allow-session
    #exit

eventbase default
      rule priority 100 event new-call ruledef apn_apn1 actiondef apn1_newcall
      rule priority 200 event new-call ruledef apn_apn2 actiondef apn2_newcall
     rule priority 400 event rule-report-status ruledef ded_bearer_creation_fail actiondef
 apn2_retry_dedicated_bearer
      rule priority 600 event restore-bearers ruledef apn_apn2 actiondef
apn2_restore_bearer_config
    #exit
```

The key point in the above configuration is that both "new-call" and "restore-bearers" events, the actiondefs comprise of same actions. As a result, any missing bearer (such as a QCI-1 GBR bearer) is established.

At the time of "new-call" event, both QCI-1 (GBR) and QCI-5 (non-GBR) bearers are created. At the time of "restore-bearer" event, local policy will return actions to create both QCI-1 and QCI-5 bearers but since QCI-5 bearer already exists (as it was preserved), only QCI-1 bearer is established.

Show Commands and Outputs

show saegw-service statistics all

The output of this command displays the number of times SGW forwards modify bearer request to PGW due to flag enable-bearer-restore:

The output of this command includes the following fields:

MBR:— Displays the Dynamic User Plane Selection Statistics:

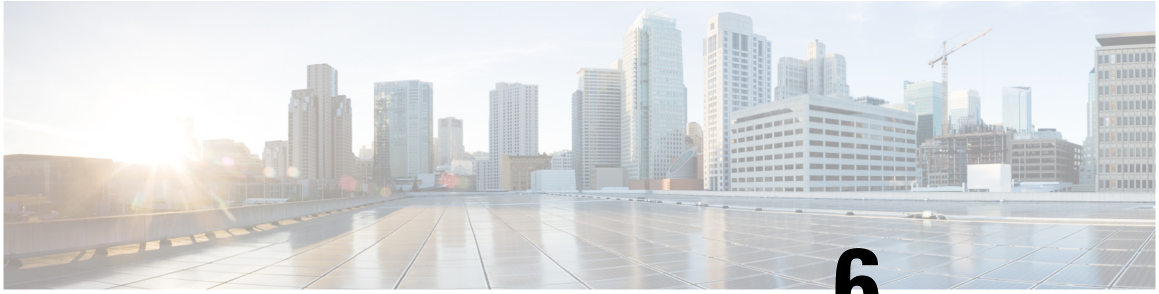
- Attempted — Displays the number of modify bearer request attempts between S-GW and P-GW due to flag enable bearers restore.
- Successful— Displays the total number of succesful modify bearer request between S-GW and P-GW due to flag enable bearers restore.
- Failure — Displays the total number of failure modify bearer request between S-GW and P-GW due to flag enable bearers restore.
- Mismatch DNS response — Displays mismatch DNS repsonse between S-GW and P-GW due to flag enable bearers restore.
- Negative DNS response — Displays negative DNS repsonse between S-GW and P-GW due to flag enable bearers restore.
- DNS timed out —Displays DNS timed out between S-GW and P-GW due to flag enable bearers restore.

show local-policy statistics all

The output of this command displays the list of events under event-base local-policy when S-GW sends modify bearer request to P-GW.

The output of this command includes the following fields:

Restore Bearers — Displays the restore-bearer enable and disable in local policy configuration.



CHAPTER 6

Customized Interface Between MME/SGSN and GMPC

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME/SGSN
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	• *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Table 2: Revision History

Revision Details	Release
First introduced	21.19

Feature Description

In the Customized Interface between MME/SGSN and Gateway Mobile Positioning Center (GMPC), reporting takes place in a new TCP based format to an external Gateway Mobile Positioning Center (GMPC).

The enhanced LBS services for LI enables control nodes to send all the subscriber information including subscription updates like Attach, Detach, Handover and so on, whenever an event gets triggered.

How it Works

In Customized Interface between MME/SGSN and GMPC, by implementing a new session manager event data process, it manages the MME and SGSN events in a similar fashion to that of the EDR/CDR feature, buffers them and transmits the event data through Conn-proxy to the GMPC server.

As per the new customization between Cisco MME/SGSNs and GMPC, the interface is TCP-based and the GMPC works as a server of the TCP connection and listens to a configurable TCP port. Cisco MME/SGSN then initiate the TCP connection to GMPC.

Note Cisco MME/SGSNs must be configured to send the TCP streams towards the LBS Load Balancer and VIP.

The following events take place to trigger Cisco MME/SGSN to send subscriber information:

- ATTACH
- RAU (SGSN RAU)
- ISRAU (Inter SGSN RAU)
- DEACTIVATE (PDP Deactivate)
- L_ATTACH (LTE Attach)
- L_DETACH (LTE Detach)
- L_HANDOVER (LTE Handover)
- L_TAU (LTE TAU)
- L_DEDICATED_BEARER_ACTIVATE (LTE Establish Bearer)
- L_DEDICATED_BEARER_DEACTIVATE (LTE Drop Bearer)
- L_PDN_CONNECT (LTE PDN Connect)
- L_PDN_DISCONNECT (LTE PDN Disconnect)

- L_SERVICE_REQUEST (LTE Service request)
- SERVICE_REQUEST (WCDMA Service Request)
- L_BEARER_MODIFY (LTE Modify Bearer)
- L_DEFAULT_BEARER_ACTIVATE (LTE Establish Default Bearer)
- L_DEFAULT_BEARER_DEACTIVATE (LTE Drop Default Bearer)
- UNKNOWN (SGSN UNKNOWN)

When any of the above events get triggered, MME sends subscriber information such as ECGI, SAI, IMSI, MSISDN, IMEI, Event ID and MME number to GMPC.

Similarly, SGSN also sends GPRS/UMTS based subscriber information such as (LAC/RAC/SAC)to GMPC.

Enabling GMPC Event-Report-Connection under Context

Use the following configuration to enable GMPC event-report-connection under context:

```
configure
   context context_name
      [ no ] event-report-conn event_report_conn_name
         gmpc-event-report { dest-addr { ipv4_address | ipv6_address } dest-port
 port_number | src-addr { ipv4_address | ipv6_address } src-port port_number }
         end
```

Configuring GMPC Multiple/Single

Use the following configuration to configure the connproxy mode to either “Single” or “Multi” mode:

```
configure
   [ no ] require gmpc-event-report-tcp-proxy { multiple | single }
   end
```

Note Connproxy mode must be either single or multiple mode.

Enabling GMPC Event-Report-Connection under Call-Control-Profile

Use the following configuration to enable GMPC event-report-connection under call-control-profile:

```
configure
   call-control-profile call_control_profile
      [ remove ] reporting-action { event-stream{ event-report-conn
event_report_conn_name } | mme-event-record }
     end
```

Binding GMPC Server Interface

Use the following configuration to bind card and port number with the GMPC source interface:

```
configure
  port ethernet port_number
     vlan tag_id
     no shutdown
     bind interface gmpc_interface_name context_name
     end
```

Note Enter the card or port number details for the ethernet.

Show Commands and Outputs

show event-report-conn all

The output of this command displays the number of events connected between MME/SGSN and GMPC.

The output of this command includes the following fields:

- src-addr— Displays gmpc-event-report source ip-address.
- src-port—Displays source port address of gmpc-event-report connection.
- dest-addr—Displays gmpc-event-report destination ip-address.
- dest-port—Displays destination port address of gmpc-event-report connection.

show event-report-conn name <event_report_conn_name>

The output of this command includes the event report connection name to display the number of events connected between MME/SGSN and GMPC.

The output of this command includes the following fields:

- src-addr— Displays gmpc-event-report source ip-address.
- src-port—Displays source port address of gmpc-event-report connection.
- dest-addr—Displays gmpc-event-report destination ip-address.
- dest-port—Displays destination port address of gmpc-event-report connection.

show gmpc-event-report statistics event-report-conn all

The output of this command displays the statistics of gmpc-event-report connections between MME/SGSN and GMPC.

The output of this command includes the following fields:

- Total number of events—Displays the total number of gmpc-event-report connections.
- Number of events sent—Displays the total number of gmpc-event-report connections sent.
- Number of events dropped—Displays the total number of gmpc-event-report connections dropped.

show gmpc-event-report statistics event-report-conn name <event_report_conn_name>

The output of this command includes the event report connection name to display the statistics of gmpc-event-report connections between MME/SGSN and GMPC.

The output of this command includes the following fields:

- Total number of events—Displays the total number of gmpc-event-report connections.
- Number of events sent—Displays the total number of gmpc-event-report connections sent.
- Number of events dropped—Displays the total number of gmpc-event-report connections dropped.

CHAPTER 7

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • Ultra Gateway Platform
Feature Default	Disabled - License 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 release 21.2 and N5.1.

Revision Details	Release
In this release the following three new parameters are added in Large TODR: **1.** International Mobile Subscriber Identity (IMSI) **2.** Flow-ID and Flow-ID list **3.** User Location Information (ULI) For more information, refer the *Large TODR Enhancement* section.	21.19.1
The Cisco Ultra Traffic Optimization library version has been upgraded from 3.0.9 to 3.0.11.	21.14.2
With this release, new keywords **large-flows-only** and **managed-large-flows-only** are implemented as part of the **data-record** command to enable the CUTO library to stream respective statistics to the external server. New bulk statistics are added in support of this enhancement	21.14
With this release, Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.3.17
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.3.x
Multi-Policy support for Cisco Ultra Traffic Optimization solution.	21.6
Cisco Ultra Traffic Optimization solution is supported in Ultra Gateway Platform (UGP).	21.6
Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.5
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.5
First introduced.	21.2

Overview

In a high-bandwidth bulk data flow scenario, user experience is impacted due to various wireless network conditions and policies like shaping, throttling, and other bottlenecks that induce congestion, especially in the RAN. This results in TCP applying its saw-tooth algorithm for congestion control and impacts user experience, and overall system capacity is not fully utilized.

The Cisco Ultra Traffic Optimization solution provides clientless optimization of TCP and HTTP traffic. This solution is integrated with Cisco P-GW and has the following benefits:

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.

- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

How Cisco Ultra Traffic Optimization Works

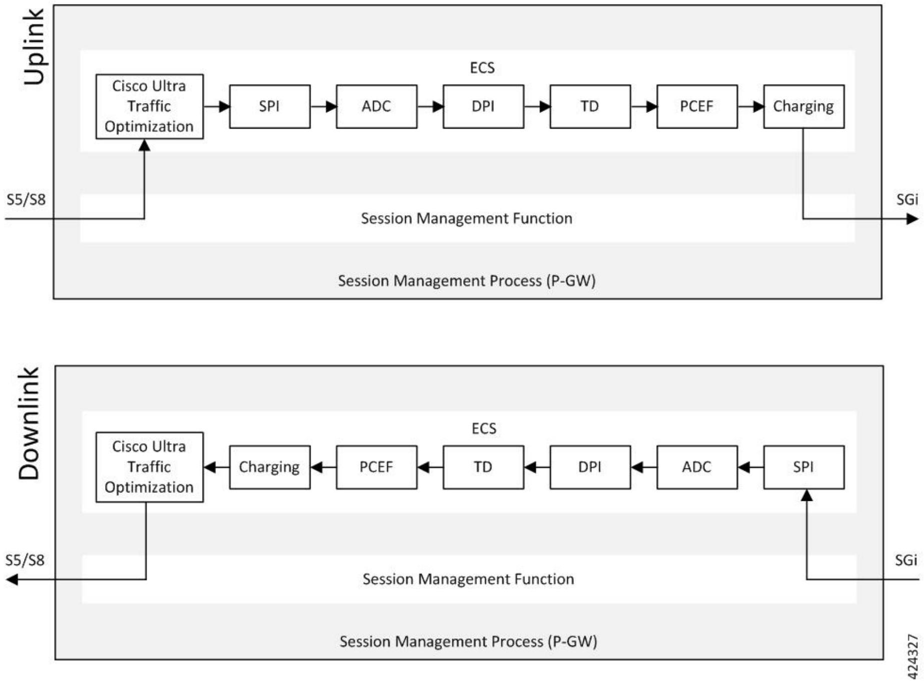
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested channel. Cisco Ultra Traffic Optimization then flow-controls video to varying levels and time, depending on the degree of detected congestion, and efficiently aligns delivery of the video traffic to less-congested moments while still providing adequate bandwidth to videos to maintain their quality. The result is less network latency and higher user throughputs while maintaining HD video. Cisco Ultra Traffic Optimization does not drop packets or modify data payloads in any way.

The Cisco Ultra Traffic Optimization integrates with standard Cisco P-GW functions such as Application Detection and Control (ADC), allowing mobile operators to define optimization policies that are based on the traffic application type as well as APN, QCI, and other common traffic delineations. Cisco Ultra Traffic Optimization is fully radio network aware, allowing management on a per eNodeB cell basis.

Architecture

StarOS has a highly optimized packet processing framework, the Cisco Ultra Traffic Optimization engine, where the user packets (downlink) are processed in the operating systems user space. The high-speed packet processing, including the various functions of the P-GW, is performed in the user space. The Cisco Ultra Traffic Optimization engine is integrated into the packet processing path of Cisco’s P-GW with a well-defined Application Programming Interface (API) of StarOS.

The following graphic shows a high-level overview of P-GW packet flow with traffic optimization.


Uplink
ECS
Cisco Ultra Traffic Optimization
SPI
ADC
DPI
TD
PCEF
Charging
S5/S8
SGi
Session Management Function
Session Management Process (P-GW)
Downlink
ECS
Cisco Ultra Traffic Optimization
Charging
PCEF
TD
DPI
ADC
SPI
S5/S8
SGi
Session Management Function
Session Management Process (P-GW)
424327

Licensing

The Cisco Ultra Traffic Optimization is a licensed Cisco solution. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations and Restrictions

Handling of Traffic Optimization Data Record

The Traffic Optimization Data Record (TODR) is generated only on the expiry of idle-timeout of the Cisco Ultra Traffic Optimization engine. No statistics related to session or flow from P-GW is included in this TODR. The data records are a separate file for the Traffic Optimization statistics, and available to external analytics platform.

Large TODR Enhancement

In 21.19.1 and later releases, the following three new parameters are added in large TODR:

1. International Mobile Subscriber Identity (IMSI)
2. Flow-ID and Flow-ID list
3. User Location Information (ULI)

The Flow-ID is used to correlate the ACS Flow ID that is visible in End Point Detection and Response ("sn-flow-id" attribute) and then the ULI is correlated with RAN counters.

Note These new fields are only available in Large TODRs generated on non-VPP based P-GW and SAEGW.

Enhancing Large TODR

Use the following configuration to enable enhanced large TODR.

```
configure
   active-charging service service_name
      traffic-optimization-profile
         data-record
            enhanced-large-todr [ imsi | acs-flow-id | uli ]
            end
```

Example 1: When all fields are to be displayed:

```
enhanced-large-todr
```

Example 2: When IMSI and ULI are to be displayed:

```
enhanced-large-todr imsi
enhanced-large-todr uli
```

Show Commands and Outputs

```
show active-charging traffic-optimization info
```

Output Example 1:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: DISABLED
[local]laas-setup#
```

Output Example 2 for IMSI and ULI:

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: ENABLED, Fields: imsi uli
[local]laas-setup#
```

The output of this command includes the following fields:

- Enhanced Large TODR

Enhancement to the Existing Large TODRs

1. **Large TODRs with IMSI**

   IMSI: Indicates the International Mobile Subscriber Identity.

   IMSI value is 0 if it is a trusted build.

2. **ACS Flow ID**

   ACS Flow ID is a newly introduced field. As there could be a lot of flow, it is limited to a maximum of 20 flows as a part of TODR.

   acs_flow_id_count: Number of ACS Flow Ids present in this TODR. A Maximum of 20 ACS Flow IDs is present.

   acs_flow_id_list: List of individual ACS Flow Ids. For examples, acs_flow_id1, acs_flow_id2 and so on.

   a. **EDR ACS Flow ID**

      In EDR, each ACS flow ID is printed by enabling the attribute ‘sn-flow-id’ in EDR config as given below :

      ```
      config
      active-charging service ACS
          edr-format EDR_SN
          delimiter comma
            attribute sn-flow-id priority 10
            rule-variable bearer 3gpp imsi priority 15
            rule-variable bearer qci priority 20
      ```

      It is printed out in EDR in the following format **92:30278:14786055** where:

      - 92 is the Session Manager instance
      - 30278 is the Session Handle orsession number
      - 14786055 is the ACS flow identifier

   b. **TODR ACS Flow ID**

      TODR ACS flow idshould follow the same format as in EDR so customers can correlate TODRs with EDRs. Therefore, each flow ID in the list acs_flow_id_list that is acs_flow_id1, acs_flow_id2, and so on should get printed out in TODR as `smgr instance:session handle: flow id`.

      An example is **92:30278:14786055** where:

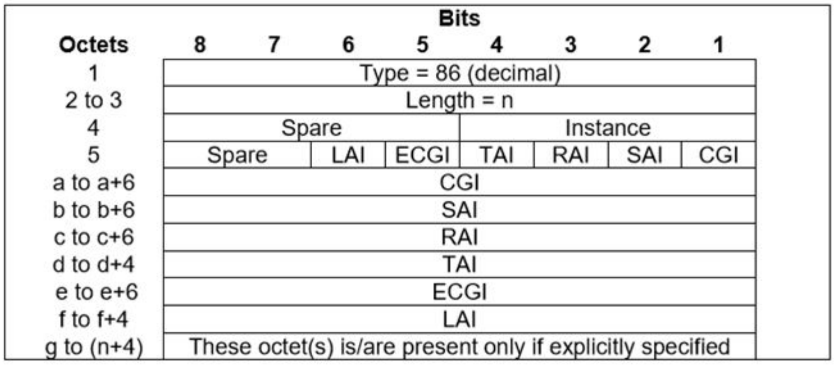
      - 92 is the Session Manager instance
      - 30278 is the Session Handle orsession number
      - 14786055 is the ACS flow identifier

3. **ULI**

   Even though the original requirment was to print ECGI, it does not cover all the scenarios. For example, when PGW is the anchor for a call that moves from 4G to 3G, ECGI does not make sense as the ULI (User Location Information) indicates CGI rather than ECGI as the user is now in 3G. Normally, MME informs PGW through SGW of the changes happened in ULI. This feature supports ULI that is s superset of ECGI.

The new field is called ULI. However, ULI is a complex IE composed of multiple identifiers and of variable length. For more details, refer the 3GPP TS 29.274.

Figure 2: User Location Information (ULI)



	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = 86 (decimal)							
2 to 3	Length = n							
4	Spare				Instance			
5	Spare		LAI	ECGI	TAI	RAI	SAI	CGI
a to a+6	CGI							
b to b+6	SAI							
c to c+6	RAI							
d to d+4	TAI							
e to e+6	ECGI							
f to f+4	LAI							
g to (n+4)	These octet(s) is/are present only if explicitly specified							

An ULI can be composed of one or more identifiers For example, there could be TAI and ECGI both in the ULI. Supporting such identifiers is problematic since the total length of ULI goes beyond 8 bytes and on per packet level, and have to pass an byte array and that has performance implications. In order, to overcome this issuse, ULI is formed as a combined type (for example, TAI AND ECGI together), then alone the ECGI part is shown in TODRs. This is done to ensure that identifier portion of ULI is accommodated in `uint64_t` (8 bytes). Specifically,

a. If TAI and ECGI both are present as a combined type, then only ECGI is shown.

b. If CGI and RAI both are present as a combined type, then only CGI is shown.

c. If both SAI and RAI both are present as a combined type, then only RAI is shown .

Every TODR can have multiple phases with a granularity of 2 seconds. ULI is added to the list of Phase attributes:

a. *ULI*: Newly introduced field.

ULI Details

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULI Type: ULI Value

ULI Type can be any one of these:

- 1–CGI
- 2–SAI
- 4–RAI
- 8–TAI
- 16–ECGI

ECGI is stored in ULI as given in the figure below. It needs to be printed in this format:

ULIType:ULIValue

An example is given below when ULI Type is ECGI:

16:0x21635401234567

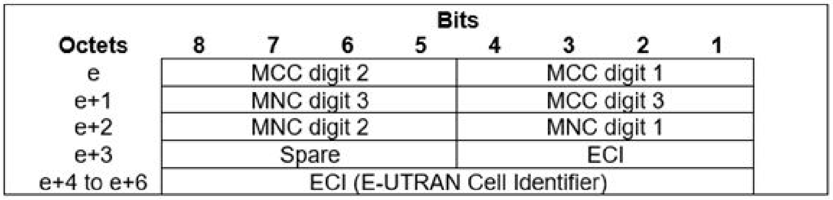
Here 16 represents that ULI Type is ECGI

0x21635401234567 is the hexadecimal representation of ECGI

MCC is ‘123’ i.e. the three digits of MCC are ‘1’, ‘2’ and ‘3’ MNC is ‘456’, that is. the three digits of MNC are ‘4’, ‘5’ and ‘6’

ECI is ‘19088743’ in decimal (‘1234567’ in hexadecimal)

Figure 3: ECGI Field



	Bits							
Octets	8	7	6	5	4	3	2	1
e	MCC digit 2				MCC digit 1			
e+1	MNC digit 3				MCC digit 3			
e+2	MNC digit 2				MNC digit 1			
e+3	Spare				ECI			
e+4 to e+6	ECI (E-UTRAN Cell Identifier)							

List of Attributes and File Format

All TODR attributes of traffic optimization is enabled by a single CLI command. The output is always comma separated, and in a rigid format.

Standard TODR

The following is the format of a Standard TODR:

```
instance_id,flow_type,srcIP,dstIP,policy_id, proto_type, dscp,
flow_first_pkt_rx_time_ms,flow_last_pkt_rx_time_ms,flow_cumulative_rx_bytes
```

Example:

```
1,0,173.39.13.38,192.168.3.106,0,1,0,
 1489131332693,1489131335924,342292
```

Where:

- *instance_id*: Instance ID.
- *flow_type*: Standard flow (0)
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.

- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.

Large TODR

The following is a sample output of a Large TODR.

```
19,1,404005123456789,22.22.0.1,1.1.1.8,custom1,2,0,1588858362158,1588858952986,16420806,1588858364162,419,351,7000,0,0,1,
19:2:15,2,0,0,2,1,1,16:0x12546300012345,
1588858364162,80396,1472,0,0,0,2,1,16:0x12546300012345,1588858366171,146942,1937,7000,0,0,2
```

Where:

- *instance_id*: Instance ID.
- *flow_type*: Large flow (1)
- *imsi_id*: Indicates the International Mobile Subscriber Identity.
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_name*: Identifies the name of the configured traffic optimization policy.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.
- *large_detection_time_ms*: Indicates the timestamp when the flow was detected as Large.
- *avg_burst_rate_kbps*: Indicates the average rate in Kbps of all the measured bursts.
- *avg_eff_rate_kbps*: Indicates the average effective rate in Kbps.
- *final_link_peak_kbps*: Indicates the highest detected link peak over the life of the Large flow.
- *recovered_capacity_bytes*: Indicates the recovered capacity in Kbps for this Large flow.
- *recovered_capacity_ms*: Indicates the timestamp of recovered capacity for this Large flow.
- *acs_flow_id_count*: Indicates the number of ACS Flow IDs present in this TODR. A maximum of 20 ACS Flow IDs is present.
- *acs_flow_id_list*: Indicates the list of individual ACS Flow IDs. For example, acs_flow_id1, acs_flow_id2, and so on.
- *phase_count*: Indicates the Large flow phase count.
- *min_gbr_kbps*: Indicates the Minimum Guaranteed Bit Rate (GBR) in Kbps.
- *max_gbr_kbps*: Indicates the Maximum Guaranteed Bit Rate (MBR) in Kbps.

- *phase_count_record*: Indicates the number of phases present in this record.
- *end_of_phases*: 0 (not end of phases) or 1 (end of phases).
- Large flow phase attributes:
  - *phase_type*: Indicates the type of the phase. This field represents that the flow was in one of the following three possible states where each state is represented by a numeric value:
    - 0 - Ramp-up Phase (if the Flow was previously idle)
    - 1 - Measurement Phase (required)
    - 2 - Flow Control Phase (if congestion detected during Measurement Phase)
  - *uli_type*: Indicates the type of ULI.
  - *phase_start_time_ms*: Indicates the timestamp for the start time of the phase.
  - *burst_bytes*: Indicates the burst size in bytes.
  - *burst_duration_ms*: Indicates the burst duration in milliseconds.
  - *link_peak_kbps*: Indicates the peak rate for the flow during its life.
  - *flow_control_rate_kbps*: Indicates the rate at which flow control was attempted (or 0 if non-flow control phase). This field is valid only when flow is in ‘Flow Control Phase’.
  - *max_num_queued_packets*: Identifies the maximum number of packets queued.
  - *policy_id*: Identifies the traffic optimization policy ID.

High Throughput Traffic Optimization Support

Cisco Ultra Traffic Optimization feature is enhanced to support the subscribers through the optimization of traffic. With High Throughput Traffic Optimization Support feature, support is added for optimization of traffic for 5G subscribers (high throughput). The feature also allows automatic switching of traffic optimization parameters depending on throughput characteristics (which is in turn based on 4G or 5G).

Note This is a licensed feature. Contact your Cisco Account representative for detailed information on specific licensing requirements.

The existing Cisco Ultra Traffic Optimization single flow logic is enhanced to dynamically toggle between algorithms depending on the profile packet pattern real time (for example, 4G LTE vs 5G mm and wave traffic pattern).

Cisco Ultra Traffic Optimization library is updated to introduce two separate sets of policy parameters under a traffic optimization policy:

- Base policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects normal throughput (for example, 4G throughput). They are called 'Base' policy parameters. These parameters are the same as the parameters that existed before the High Throughput Traffic Optimization Support feature was introduced.

- Extended policy parameters - these parameters are applied by the Cisco Ultra Traffic Optimization algorithm when it detects high throughput for a flow (for example, 5G throughput). They are called 'Extended' policy parameters.

The two separate policy parameters under the same policy quickly switch from one set to the other without requiring any intervention from session managers when there is a change in throughput.

Hence, having two separate sets of policy parameters in the same policy helps meet the requirement that the Cisco Ultra Traffic Optimization algorithm automatically, dynamically, and immediately adjusts to the change in throughput. This change in throughput could be due to a change in RAN characteristics, for example, when UE enters a 5G or high speed 4G coverage area.

How High Throughput Optimization Support Works

Cisco Ultra Traffic Optimization algorithm monitors the traffic and automatically transitions between Base and Extended policy parameters based on the following logic:

1. Start with base policy.
2. If measurement phase burst rate > extended link profile initial-rate then move to the extended policy.
3. If measurement phase burst rate < base link profile max-rate then move to the base policy.
4. Repeat steps 2,3 for every measurement phase.

.

Multi-Policy Support for Traffic Optimization

Cisco Ultra Traffic Optimization engine supports Traffic Optimization for multiple policies and provides Traffic Optimization for a desired location. It supports a maximum of 32 policies that include two pre-configured policies, by default. Operators can configure several parameters under each Traffic Optimization policy.

This feature includes the following functionalities:

- By default, Traffic Optimization is enabled for TCP and UDP data for a particular Subscriber, Bearer, or Flow that use the Service-Schema.

Important PORT 443 supports UDP or QUIC-based Traffic Optimization.

- Selection of a policy depends on the priority configured. A trigger-condition is used to prioritize a traffic optimization policy. The priority is configurable regardless of a specific location where the traffic optimization policy is applied. Based on the configured priorities, a traffic optimization policy can be overridden by another policy.
- A configuration to associate a traffic optimization policy with a Trigger Action, under the Service-Schema.
- A configuration to select a Traffic Optimization policy for a Location Trigger. Currently, only ECGI Change Detection is supported under the Local Policy Service Configuration mode.

Important Location Change Trigger is not supported with IPSG.

Important Policy ID for a flow is not recovered after a Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).

Important The Multi-Policy Support feature requires the same Cisco Ultra Traffic Optimization license key be installed. Contact your Cisco account representative for detailed information on specific licensing requirements.

How Multi-Policy Support Works

Policy Selection

Cisco's Ultra Traffic Optimization engine provides two default policies – Managed and Unmanaged. When Unmanaged policy is selected, traffic optimization is not performed.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

- Session Setup Trigger – If a Trigger Action is applied only for a Session Setup in a Service-Schema, then the trigger action is only applied to new sessions only.
- Bearer Setup Trigger – If a trigger action is applied only for a Bearer Setup, changes in the trigger action will be applicable to newly created bearers and its flows.
- Flow Creation Trigger – Under a trigger condition corresponding to a flow create, conditions can be added based on a rule-name, local-policy-rule or an IP protocol in addition to the trigger condition: any-match.

When traffic optimization on existing flows is disabled because of a trigger condition, then the traffic optimization engine will apply the default Unmanaged policy on them.

Deleting a Policy

Before deleting a Policy profile, all association to a traffic optimization policy should be removed.

For more information on deletion of a policy, refer to the *Traffic Optimization Policy Configuration* section.

Configuring Multi-Policy Support

The following sections describes the required configurations to support the Multi-Policy Support.

Configuring a Traffic Optimization Profile

Use the following CLI commands to configure a Traffic Optimization Profile.

```
configure
   require active-charging
   active-charging service service_name
```

```
      traffic-optimization-profile profile_name
         data-record[ large-flows-only | managed-large-flows-only ]
         no data record
         [ no ] efd-flow-cleanup-interval cleanup_interval
         [ no ] stats-interval stats_interval
         [ no ] stats-options { flow-analyst [ flow-trace ] | flow-trace [
  flow-analyst ] }
         end
```

NOTES:

- **require active-charging**: Enables the configuration requirement for an Active Charging service.

  Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- **data-record**: Enables the generation of traffic optimization data record.

  large-flows-only: Enables the traffic optimization data record generation for large flows.

  managed-large-flows-only: Enables the traffic optimization data record generation for managed large flows.

  The keywords - **large-flows-only** and **managed-large-flows-only** when configured along with **data-record** enables the CUTO library to stream the respective statistics as part of the **stats-options** command, to the external server. The operator can configure a combination of the **stats-options** keywords **flow-trace** and **flow-analyst** and the **data-record** command to notify the CUTO library accordingly.

  Note One of the above the two keywords can be configured as part of the data-record, which enables the CUTO library to stream the respective statistics.

  The default behavior of the **data-record** command is not affected with the above implementation . If configured without any of the options, then TODRs are generated for all standard and large flows, which is the existing behavior.

- **efd-flow-cleanup-interval**: Configures the EFD flow cleanup interval. The interval value is an integer that ranges 10–5000 milliseconds.

- **stats-interval**: Configures the flow statistics collection and reporting interval in seconds. The interval value is an integer that ranges 1–60 seconds.

- **stats-options**: Configures options to collect the flow statistics. It only specifies whether the stream must be a Flow Trace or a Flow Analyst or both, to an external server.

Note From Release 21.6 onwards, the **heavy-session** command is deprecated.

Configuring a Traffic Optimization Policy

Use the following CLI commands to configure a Traffic Optimization Policy.

```
configure
  require active-charging
  active-charging service service_name[extended]
    [ no ] traffic-optimization-policy policy_name[extended]
      bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [ [
backoff-profile [ managed | unmanaged ] [ min-effective-rate effective_rate
 ] | [ min-effective-rate effective_rate ] [ backoff-profile [ managed |
unmanaged ] ] }
      extended-bandwidth-mgmt { backoff-profile [ managed | unmanaged ]
 [ min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [ [
backoff-profile [ managed | unmanaged ] [ min-effective-rate effective_rate
 ] | [ min-effective-rate effective_rate ] [ backoff-profile [ managed |
unmanaged ] ] }
      [ no ] bandwidth-mgmt
      [ no ] extended-bandwidth-mgmt
      curbing-control { max-phases max_phase_value [ rate curbing_control_rate
 [ threshold-rate threshold_rate [ time curbing_control_duration ] ] ] | rate
curbing_control_rate [ max-phases [ threshold-rate threshold_rate [ time
curbing_control_duration ] ] ] | threshold-rate [ max-phases max_phase_value [
rate curbing_control_rate [ time curbing_control_duration ] ] ] | time [ max-phases
 max_phase_value [ rate curbing_control_rate [ threshold-rate threshold_rate] ] ]
}
      extended-curbing-control { max-phases max_phase_value [ rate
curbing_control_rate [ threshold-rate threshold_rate [ time curbing_control_duration
 ] ] ] | rate curbing_control_rate [ max-phases [ threshold-rate threshold_rate
 [ time curbing_control_duration ] ] ] | threshold-rate [ max-phases
max_phase_value [ rate curbing_control_rate [ time curbing_control_duration ] ] ] |
time [ max-phases max_phase_value [ rate curbing_control_rate [ threshold-rate
threshold_rate] ] ] }
      [ no ] curbing-control
      [ no ] extended-curbing-control
      heavy-session { standard-flow-timeout [ threshold threshold_value |
threshold threshold_value [ standard-flow-timeout timeout_value ] }
      extended-heavy-session { standard-flow-timeout [ threshold
threshold_value | threshold threshold_value [ standard-flow-timeout timeout_value
 ] }
      [ no ] heavy-session
      [ no ] extended-heavy-session
      link-profile { initial-rate initial_seed_value [ max-rate
max_peak_rate_value [ peak-lock ] ] | max-rate [ initial-rate initial_seed_value
 [ peak-lock ] ] | peak-lock [ initial-rate initial_seed_value [ max-rate
max_peak_rate_value ] ] }
       extended-link-profile { initial-rate initial_seed_value [ max-rate
max_peak_rate_value [ peak-lock ] ] | max-rate [ initial-rate initial_seed_value
 [ peak-lock ] ] | peak-lock [ initial-rate initial_seed_value [ max-rate
max_peak_rate_value ] ] }
       [ no ] link-profile
       [ no ] extended-link-profile
       session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
      extended-session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
 udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
       [ no ] session-params
       [ no ] extended-session-params
       end
```

NOTES:

- Only when **extended** keyword is used after the policy name, you will be able to see the '**extended-***' parameters, for example **extended-bandwidth-mgmt**.
- **no**: Overwrites the configured parameters with default values. The operator must remove all associated policies in a policy profile before deleting a policy profile. Otherwise, the following error message is displayed:

  ```
  Failure: traffic-optimization policy in use, cannot be deleted.
  ```

- **bandwidth-mgmt**: Configures Base bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **extended-bandwidth-mgmt**: Configures Extended bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **curbing-control**: Configures Base curbing flow control related parameters.

    - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. .
    - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate.
    - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing..
    - **time**: Configures the duration of a flow control phase in milliseconds.

- **extended-curbing-control**: Configures Extended curbing flow control related parameters.
    - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. The maximum phase value is an integer ranging 2–10 for extended parameter. The default value inherits base.
    - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate. The control rate value is an integer ranging 0-100000 kbps for extended parameter. The default value inherits base.
    - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing.The threshold rate is an integer ranging 100-100000 kbps for extended parameter. The default value inherits base.
    - **time**: Configures the duration of a flow control phase in milliseconds.

      The flow control duration value is an integer ranging 0–600000 for extended parameter. The default value inherits base.

- **heavy-session**: Configures parameters for Base heavy-session detection.
    - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows.
    - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed..

- **extended-heavy-session**: Configures parameters for Extended heavy-session detection.
    - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows. .
    - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed.

- **link-profile**: Configures Base link profile parameters.
    - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
    - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
    - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.

- **extended-link-profile**: Configures Extended link profile parameters.
    - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
    - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
    - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.

- **session-params**: Configures Base session parameters.
    - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
    - **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..
- **extended-session-params**: Configures Extended session parameters.
    - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
    - **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..

Important After you configure **require active-charging** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

The following table shows the parameter ranges for both Base and Extended set parameters, the default values of those parameters and, the validated Range/value for configuring the parameters for Cisco Ultra Traffic Optimization library.

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
bandwidth-mgmt /extended- bandwidth-mgmt	**backoff-profile**	**managed /unmanaged**	**managed**	**managed /unmanaged**	Inherits base	require match base	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	min-effective-rate	100-100000 kbps	600	100-500000 kbps	45000	allow full range	
	min- flow- control- rate	100-100000 kbps	250	100- 500000 kbps	1000	allow full range	
curbing-control / **extended-curbing- control**	**max-phases**	2-10	2	2-10	Inherits base	allow full range	
	rate	0-100000 kbps	0	0-100000 kbps	Inherits base	allow full range	
	threshold- rate	100-100000 kbps	600	100-100000 kbps	Inherits base	allow full range	
	time	0-600000 ms	0	0-600000 ms	Inherits base	allow full range	
heavy-session / **extended- heavy- session**	**standard- flow- time out**	100-10000 ms	500	100-10000 ms	Inherits base	allow full range	
	threshold	100000–100000000 bytes	3000000	100000–100000000 bytes	Inherits base	allow full range	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Com ment
link-profile / **extended-link-profile**	**initial-rate**	100-100000 kbps	7000	100-500000 kbps	50000	require greater than or equal to base max-rate	If you enter a value diff erent from Base, the value from Base para meter and an appro priate message will be disp layed.
	max- rate	100-100000 kbps	15000	100-500000 kbps	100000	require greater than or equal to base max-rate	If you enter a value diff erent from Base, the value from Base para meter and an appro priate message will be disp layed.
	peak-lock	enabled/disabled	disabled	enabled/disabled	disabled	allow either	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Com ment
session-params / **extended- session-params**	**tcp-ramp-up**	0-10000 ms	2000	0-10000 ms	2000	allow full range	
	udp-ramp-up	0-10000 ms	2000	0-10000 ms	2000	allow full range	

Traffic Optimization Policy - Default Values

```
Bandwidth-Mgmt:

   Backoff-Profile          : Managed
   Min-Effective-Rate       : 600 (kbps)
   Min-Flow-Control-Rate    : 250 (kbps)

Curbing-Control:

   Time                     : 0 (ms)
   Rate                     : 0 (kbps)
   Max-Phases               : 2
   Threshold-Rate           : 600 (kbps)

Heavy-Session:

   Threshold                : 3000000(bytes)
   Standard-Flow-Timeout    : 500 (ms)

Link-Profile:

   Initial-Rate             : 7000 (kbps)
   Max-Rate                 : 15000 (kbps)
   Peak-Lock                : Disabled

Session-Params:

   Tcp-Ramp-Up              : 2000 (ms)
   Udp-Ramp-Up              : 2000 (ms)
```

Associating a Trigger Action to a Traffic Optimization Policy

Use the following CLI commands to associate a Trigger Action to a Traffic Optimization Policy.

```
configure
   require active-charging
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization policy policy_name
         [ no ] traffic-optimization
         end
```

NOTES:

- **traffic-optimization policy**: Configures a traffic optimization policy.
- **no**: Removes the configured traffic optimization policy.

Enabling TCP and UDP

Use the following CLI commands to enable TCP and UDP protocol for Traffic Optimization:

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      [ no ] ip protocol = [ tcp | udp ]
      end
```

NOTES:

- **no**: Deletes the Active Charging Service related configuration.
- **ip**: Establishes an IP configuration.
- **protocol**: Indicates the protocol being transported by the IP packet.
- **tcp**: Indicates the TCP protocol to be transported by the IP packet.
- **udp**: Indicates the UDP protocol to be transported by the IP packet.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Service-Scheme Configuration for Multi-Policy Support

The service-schema framework enables traffic optimization at APN, rule base, QCI, and Rule level. In 21.6, with the Multi-Policy Support feature, traffic optimization in a service-schema framework allows the operator to configure multiple policies and to configure traffic optimization based on a desirable location.

The service-schema framework helps in associating actions based on trigger conditions, which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.

Session Setup Trigger

The **any-match = TRUE**, a wildcard configuration, is the only supported condition for this trigger and so this is applicable to all the flows of the subscriber.

Use the following configuration to setup a Session Trigger:

```
configure
    active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
trigger-action trigger_action_name
```

```
               exit
           subs-class sub_class_name
              apn = apn_name
              exit
           subscriber-base subscriber_base_name
              priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
              end
```

Sample Configuration

Following is a sample configuration for Session Setup Trigger:

```
 service-scheme SS1
      trigger sess-setup
        priority 1 trigger-condition sess-setup trigger-action sess-setup
      #exit
    trigger-condition sess-setup
      any-match = TRUE
    #exit
    trigger-action sess-setup
      traffic-optimization policy sess-setup
    #exit
```

Bearer Creation Trigger

The trigger conditions related to QCI can be used for this trigger, and so this is applicable to all the flows of specific bearers.

Use the following configuration to configure a Bearer Creation Trigger:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name2
            qci = qci_value
            exit
         trigger-action bearer-creation
            traffic-optimization policy bearer-creation
            exit
```

Sample Configuration

The following is a sample configuration for Bearer Creation Trigger:

```
service-scheme SS1
      trigger bearer-creation
        priority 1 trigger-condition bearer-creation trigger-action bearer-creation
      #exit
    trigger-condition bearer-creation
      qci = 1 to 2
    #exit
    trigger-action bearer-creation
    traffic-optimization policy bearer-creation
  #exit
```

Flow Creation Trigger

The trigger conditions related to rule-name and QCI can be used here, and so this is related to specific flow.

Use the following configuration to configure a flow creation trigger:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
            ip-protocol = protocol_type
            rule-name = rule_name
               **Multi-line or All-lines**
            exit
```

Sample Configuration

The following is a sample configuration for Flow Creation Trigger using the default Cisco Ultra Traffic Optimization policy:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC5 trigger-action TA4
    #exit
    trigger-condition TC5
      ip protocol = tcp
      ip protocol = udp
      multi-line-or all-lines
    #exit
    trigger-action TA4
      traffic-optimization
    #exit
```

Configuring: ecgi-change

The following demonstrates ecgi-change sample configuration:

Trigger Condition and Trigger Action in ACS Configuration

```
configure
active-charging-service ACS
   trigger-action TA1
      traffic-optimization policy flow-create-ecgi-change
    #exit
    trigger-condition TC4
      local-policy-rule = ruledef-ecgi
    #exit
 end
```

Service Schema Configuration

```
configure
active-charging-service ACS
```

```
    service-scheme SS1
      trigger flow-create
        priority 2 trigger-condition TC4 trigger-action TA1
      #exit
    subs-class SC1
      any-match = TRUE
    #exit
    subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
    #exit
end
```

Local Policy Configuration

```
local-policy-service LP
    ruledef anymatch
      condition priority 1 imsi match *
    #exit
    ruledef ecgi-1
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AE7F0A 1AE7F0B 1AE7F28 1AE7F29
1AE7F46 1AE7F47 1AEAC00 1AEAC01 1AEAC02 1AEAC0A 1AEAC0B 1AEAC0C 1AEAC14 1AEAC15 1AEAC16
1AEAC28 1AEAC29 1AEAC2A 1AEAC46 1AEAC47 1AEAC48 1AEAC50 1AEAC51 1AEAC52 1AEAC6E 1AEAC6F
1AEAC70 1AEAC78 1AEAC79 1AEAC7A
    #exit
    ruledef ecgi-10
      condition priority 1 ecgi mcc 300 mnc 235 eci match 1F36C52 1F36C6E 1F36C6F 1F36C70
1F36C78 1F36C79 1F36C7A
    #exit
    ruledef ecgi-2
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBE01 1AEBE02 1AEBE0B 1AEBE0C
1AEBE15 1AEBE16 1AEBE29 1AEBE2A 1AEBE47 1AEBE48 1AEBF00 1AEBF01 1AEBF02 1AEBF0A 1AEBF0B
1AEBF0C 1AEBF14 1AEBF15 1AEBF16 1AEBF1E 1AEBF1F 1AEBF20 1AEBF28 1AEBF29 1AEBF2A 1AEBF46
    #exit
    ruledef ecgi-3
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBF47 1AEBF48 1AEBF50 1AEBF51
1AEBF52 1AEBF6E 1AEBF6F 1AEBF70 1AEBF78 1AEBF79 1AEBF7A 1AF0E00 1AF0E01 1AF0E02 1AF0E0A
1AF0E0B 1AF0E0C 1AF0E14 1AF0E15 1AF0E16 1AF0E28 1AF0E29 1AF0E2A 1AF0E46
    #exit
    ruledef ecgi-4
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF0E47 1AF0E48 1AF4A0A 1AF4A0B
1AF4A14 1AF4A15 1AF4A28 1AF4A29 1AF4A46 1AF4A47 1AF4D00 1AF4D01 1AF4D0A 1AF4D0B 1AF4D14
1AF4D15 1AF4D28 1AF4D29 1AF4D46 1AF4D47 1AF4D50 1AF4D51 1AF4D6E 1AF4D6F
    #exit
    ruledef ecgi-5
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF4D78 1AF4D79 1AF7200 1AF7201
1AF7202 1AF720A 1AF720B 1AF720C 1AF7214 1AF7215 1AF7216 1AF721E 1AF721F 1AF7444 1AF7228
1AF7229 1AF722A 1AF7246 1AF7247 1AF7248 1AF7250 1AF7251 1AF7252 1AF726E
    #exit
    ruledef ecgi-6
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF726F 1AF7270 1B04C00 1B04C01
1B04C02 1B04C03 1B04C0A 1B04C0B 1B04C0C 1B04C0D 1B04C14 1B04C15 1B04C16 1B04C17 1B04C1E
1B04C1F 1B04C20 1B04C21 1B04C28 1B04C29 1B04C2A 1B04C2B 1B04C46 1B04C47
    #exit
    ruledef ecgi-7
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B04C48 1B04C49 1B04C50 1B04C51
1B04C52 1B04C53 1B04C6E 1B04C6F 1B04C70 1B04C71 1B04C78 1B04C79 1B04C7A 1B04C7B 1B05300
1B05301 1B05302 1B0530A 1B0530B 1B0530C 1B05314 1B05315 1B05316 1B05328 1B05329
    #exit
    ruledef ecgi-8
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B0532A 1B05346 1B05347 1B05348
1B32F00 1B32F01 1B32F02 1B32F0A 1B32F0B 1B32F0C 1B32F14 1B32F15 1B32F16 1B32F28 1B32F29
1B32F2A 1B32F46 1B32F47 1B32F48 1B76400 1B76401 1B76402 1B7640A 1B7640B 1B7640C 1B76428
    #exit
    ruledef ecgi-9
```

```
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B76429 1B7642A 1B76446 1B76447
1B76448 1F36C00 1F36C01 1F36C02 1F36C0A 1F36C0B 1F36C0C 1F36C14 1F36C15 1F36C16 1F36C1E
1F36C1F 1F36C20 1F36C28 1F36C29 1F36C2A 1F36C46 1F36C47 1F36C48 1F36C50 1F36C51
    #exit
    actiondef activate_lp_action
      action priority 1 activate-lp-rule name ruledef-tai
    #exit
    actiondef activate_lp_action1
      action priority 3 event-triggers ecgi-change
    #exit
    actiondef ecgi_change
      action priority 1 activate-lp-rule name ruledef-ecgi
    #exit
    eventbase default
     rule priority 1 event new-call ruledef anymatch actiondef activate_lp_action1 continue

      rule priority 11 event new-call ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 12 event new-call ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 13 event new-call ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 14 event new-call ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 15 event new-call ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 16 event new-call ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 17 event new-call ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 18 event new-call ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 19 event new-call ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 20 event new-call ruledef ecgi-10 actiondef ecgi_change continue
      rule priority 21 event ecgi-change ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 22 event ecgi-change ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 23 event ecgi-change ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 24 event ecgi-change ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 25 event ecgi-change ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 26 event ecgi-change ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 27 event ecgi-change ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 28 event ecgi-change ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 29 event ecgi-change ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 30 event ecgi-change ruledef ecgi-10 actiondef ecgi_change continue
    #exit
  #exit
end
```

Traffic Optimization Policy Configuration

```
configure
active-charging-service ACS
traffic-optimization-policy Config:
    traffic-optimization-policy flow-create-ecgi-change
      heavy-session threshold 400000
    #exit
end
```

Local Policy Configuration

Important Configuring Local Policy needs a Local Policy Decision Engine License. Contact your Cisco account representative for information on specific licensing requirements.

This section describes the traffic optimization policy configuration that is based on location.

Use the following sample configuration to enable a eCGI change rule:

```
configure
   active-charging service service_name
      local-policy-service service_name
        ruledef ruledef_name
          condition priority priority_value ecgi mccmcc_value mnc mnc_value eq
eq_value
          exit
        actiondef actiondef_name1
          action priority priority_value event-triggers actiondef_name2
          exit
        actiondef actiondef_name2
          action priority priority_value activate-lp-ruleruledef_name
          exit
        eventbase eventbase_name
          rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
          rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
          exit
```

Service-Scheme Configuration

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger flow-create
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger condition trigger_condition_name
            local-policy-rule = rule_name
            exit
         trigger action trigger_action_name
            traffic-optimization policy policy_name
            exit
```

Configuring L7 Rule

Important Configuring L7 Rule needs an Application Detection Control License. Contact your Cisco account representative for detailed information on specific licensing requirements.

Use the following CLI to configure an L7 rule:

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name
```

```
    rule-name = rule_name
    rule-name = rule_name
       **Multi-line or All-lines**
trigger-action trigger_action_name
    traffic-optimization policy policy_name
    exit
```

Sample Configuration

The following is a sample configuration for L7 Rules:

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC6 trigger-action TA6
    #exit
    trigger-condition TC6
      rule-name = whatsapp
      rule-name = http
      multi-line-or all-lines
    #exit
    trigger-action TA6
      traffic-optimization policy flow-create-L7-Rules
    #exit
```

Ookla Speedtest

Use the configuration information discussed in the section Configuring L7 Rule, on page 48.

Sample Configuration

The following is a sample configuration for Ookla Speedtest:

```
 service-scheme SS1
      trigger flow-create
        priority 1 trigger-condition ookla trigger-action ookla
      #exit
    trigger-condition ookla
      rule-name = speedtest
    #exit
    trigger-action ookla
      no traffic-optimization
    #exit
```

Location and App-based Configuration

Sample Configuration

```
 service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC3 trigger-action TA2
    #exit
    trigger-condition TC3
      local-policy-rule = ruledef-ecgi
      rule-name = youtube
      rule-name = whatsapp
      multi-line-or all-lines
    #exit
    trigger-action TA2
      traffic-optimization policy flow-create-ecgi-change
    #exi
```

Selective Configuration by Disabling TCP and UDP

Sample Configuration

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition tcponly trigger-action tcponly
      priority 2 trigger-condition udponly trigger-action udponly
    #exit
    trigger-condition tcponly
      ip protocol = tcp
    #exit
    trigger-condition udponly
      ip protocol = udp
    #exit
    trigger-action tcponly
      no traffic-optimization
    #exit
    trigger-action udponly
      no traffic-optimization
    #exit
```

L7/ADC and Location Trigger based Configuration

Sample Configuration

This sample configuration describes a scenario where an operator wants to always disable Traffic Optimization for Speedtest. The configuration disables traffic optimization regardless of the location. It applies a specific policy for a specific location (ECGI) (except for Speedtest) and overrides any other policy set by any trigger condition.

Also, for a specific policy optimization, for example: YouTube, the policy selection is prioritized as follows:

```
Service Scheme Configuration:
service-scheme SS1
trigger flow-create
  priority 1 trigger-condition speedtest-tc trigger-action speedtest-ta
  priority 2 trigger-condition location-tc trigger-action location-ta
  priority 3 trigger-condition youtube-tc trigger-action youtube-ta
  #exit
  trigger-condition location-tc
    local-policy-rule = ruledef-ecgi
  #exit
  trigger-action location-ta
    traffic-optimization policy flow-create-ecgi-change
  #exit
  trigger-condition speedtest-tc
    *rule-name = speedtest
  #exit
  trigger-action speedtest-ta
    no traffic-optimization
  #exit
  trigger-condition youtube-tc
    rule-name = youtube
  #exit
  trigger-action youtube-ta
    traffic-optimization policy youtube-policy
  #exit
* Provided rule-name = speedtest, is configured such that it always detects this traffic.
```

Configuring Cisco Ultra Traffic Optimization

This section provides information on enabling support for the Cisco Ultra Traffic Optimization solution.

Loading Traffic Optimization

Use the following configuration under the Global Configuration Mode to load the Cisco Ultra Traffic Optimization as a solution:

```
configure
   require active-charging traffic-optimization
   end
```

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important Enabling or disabling the traffic optimization can be done through the Service-scheme framework.

Important After you configure the **require active-charging traffic-optimization** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important In 21.3, and 21.5 and later releases, the dependency on the chassis reboot is not valid anymore. The Cisco Ultra Traffic Optimization engine is loaded by default. The Cisco Ultra Traffic Optimization configuration CLIs are available when the license is enabled. As such, the **traffic-optimization** keyword has been deprecated.

Enabling Cisco Ultra Traffic Optimization Configuration Profile

Use the following configuration under ACS Configuration Mode to enable the Cisco Ultra Traffic Optimization profile:

```
configure
   active-charging service service_name
      traffic-optimization-profile
      end
```

NOTES:

- The above CLI command enables the Traffic Optimization Profile Configuration, a new configuration mode.

Configuring the Operating Mode

Use the following CLI commands to configure the operating mode under Traffic Optimization Profile Configuration Mode for the Cisco Ultra Traffic Optimization engine:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         mode [ active | passive ]
         end
```

Notes:

- **mode**: Sets the mode of operation for traffic optimization.
- **active**: Active mode where both traffic optimization and flow monitoring is done on the packet.
- **passive**: Passive mode where no flow-control is performed but monitoring is done on the packet.

Enabling Cisco Ultra Traffic Optimization Configuration Profile Using Service-scheme Framework

The service-scheme framework is used to enable traffic optimization at APN, rule base, QCI, and Rule level. There are two main constructs for the service-scheme framework:

- **Subscriber-base** – This helps in associating subscribers with service-scheme based on the subs-class configuration.
  - **subs-class** – The conditions defined under subs-class enables in classifying the subscribers based on rule base, APN, v-APN name. The conditions can also be defined in combination, and both OR as well as AND operators are supported while evaluating them.
- **Service-scheme** – This helps in associating actions based on trigger conditions which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.
  - **trigger-condition** – For any trigger, the trigger-action application is based on conditions defined under the trigger-condition.
  - **trigger-actions** – Defines the actions to be taken on the classified flow. These actions can be traffic optimization, throttle-suppress, and so on.

Session Setup Trigger

The **any-match = TRUE**, a wildcard configuration, is the only supported condition for this trigger and so this is applicable to all the flows of the subscriber.

Following is a sample configuration:

```
configure
   active-charging service service_name
     service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
```

```
trigger-action trigger_action_name
            exit
         trigger-condition trigger_condition_name1
            any-match = TRUE
            exit
         trigger-action sess-setup
         traffic-optimization policy sess-setup
            exit
```

Bearer Creation Trigger

The trigger conditions related to QCI can be used for this trigger, and so this is applicable to all the flows of specific bearers.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
            exit
         exit
      subs-class sub_class_name
         apn = apn_name
         exit
      subscriber-base subscriber_base_name
         priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
         end
```

Flow Creation Trigger

The trigger conditions related to rule-name and QCI can be used here, and so this is related to specific flow.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
```

```
          exit
      trigger-condition trigger_condition_name2
          qci = qci_value
          exit
      trigger-condition trigger_condition_name3
          rule-name = rule_name
          exit
      service-scheme service_scheme_name
          trigger bearer-creation
             priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
             exit
          exit
      subs-class sub_class_name
          apn = apn_name
          exit
      subscriber-base subscriber_base_name
         priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
          end
```

Notes:

- *trigger_condition_name3* can have only rules, only QCI, both rule and QCI, or either of rule and QCI.

The following table illustrates the different levels of Traffic Optimization and their corresponding Subscriber Class configuration and Triggers.

Traffic Optimization Levels	Subscriber Class configuration and Triggers
Applicable to all the calls or flows	**subs-class** *sc1* **any-match = TRUE** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of a rulebase	**subs-class** *sc1* **rulebase = prepaid** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of an APN	**subs-class** *sc1* **apn = cisco.com** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all flows of a Bearer	**trigger-condition** *TC1* **qci = 1** **exit** Bearer creation trigger condition is TC1

Traffic Optimization Levels	Subscriber Class configuration and Triggers

Applicable to a particular flow	`trigger-condition TC1`
	`qci = 1`
	`rule-name = tcp`
	`multi-line-or all-lines`
	`exit`
	Flow creation trigger condition is TC1

Important In case of LTE to eHRPD handover, since QCI is not valid for eHRPD, it is recommended to configure rule-name as the trigger-condition under service-scheme.

Generating TODR

Use the following CLI commands under ACS Configuration Mode to enable Traffic Optimization Data Record (TODR) generation:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         data-record
         end
```

NOTES:

- If previously configured, use the **no data-record** command to disable generating TODR.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Cisco Ultra Traffic Optimization solution on the P-GW.

Cisco Ultra Traffic Optimization Show Commands and/or Outputs

This section provides information about show commands and the fields that are introduced in support of Cisco Ultra Traffic Optimization solution.

show active-charging traffic-optimization counters

The **show active-charging traffic-optimization counters sessmgr { all | instance** *number* **}** CLI command is introduced where:

- **counters** – Displays aggregate flow counters/statistics from Cisco Ultra Traffic Optimization engine.

Important This CLI command is license dependent and visible only if the license is loaded.

Following are the new field/counters:

- Traffic Optimization Flows:
    - Active Normal Flow Count
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
    - Base Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
    - Extended Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
    - Total Normal Flow Count
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
    - Base Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Extended Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Total IO Bytes
    - Total Large Flow Bytes

  - Total Recovered Capacity Bytes
  - Total Recovered Capacity ms

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

Important This CLI command is license dependent and visible only if the license is loaded.

- TCP Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
  - Extended Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count

    - Total IO Bytes
    - Total Large Flow Bytes
    - Total Recovered Capacity Bytes
    - Total Recovered Capacity ms

- UDP Traffic Optimization Flows:
    - Active Normal Flow Count
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
    - Base Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
    - Extended Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
-
    - Total Normal Flow Count
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
    - Base Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Extended Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Total IO Bytes:

  - Total Large Flow Bytes
  - Total Recovered Capacity Bytes
  - Total Recovered Capacity ms

show active-charging traffic-optimization info

This show command has been introduced in Exec Mode, where:

- **traffic-optimization** – Displays all traffic optimization options.
- **info** – Displays Cisco Ultra Traffic Optimization engine information.

The output of this CLI command displays the version, mode, and configuration values.

Following are the new fields/counters:

- Version:
- Mode:
- Configuration:
  - Data Records (TODR)
  - Statistics Options
  - EFD Flow Cleanup Interval
  - Statistics Interval

show active-charging traffic-optimization policy

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Extended-Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Curbing-Control
  - Time

  - Rate
  - Max-phases
  - Threshold-Rate
- Extended-Curbing-Control
  - Time
  - Rate
  - Max-phases
  - Threshold-Rate
- Heavy-Session
  - Threshold
  - Standard-Flow-Timeout
- Extended-Heavy-Session
  - Threshold
  - Standard-Flow-Timeout
- Link-Profile
  - Initial-Rate
  - Max-Rate
  - Peak-Lock
- Extended-Link-Profile
  - Initial-Rate
  - Max-Rate
  - Peak-Lock
- Session-Params
  - Tcp-Ramp-Up
  - Udp-Ramp-Up
- Extended-Session-Params
  - Tcp-Ramp-Up
  - Udp-Ramp-Up

Bulk Statistics

The following bulk statistics are added in the ECS schema to support Large and Managed flows:

Bulk Statistics	Description
tcp-active-base-large-flow-count	Indicates the number of TCP active-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-managed-large-flow-count	Indicates the number of TCP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-base-unmanaged-large-flow-count	Indicates the number of TCP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-large-flow-count	Indicates the number of TCP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-managed-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-ext-unmanaged-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-large-flow-count	Indicates the number of TCP total-base-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-managed-large-flow-count	Indicates the number of TCP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-base-unmanaged-large-flow-count	Indicates the number of TCP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-large-flow-count	Indicates the number of TCP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-managed-large-flow-count	Indicates the number of TCP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-ext-unmanaged-large-flow-count	Indicates the number of TCP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-large-flow-count	Indicates the number of UDP active-base-large-flow-count count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-active-base-managed-large-flow-count	Indicates the number of UDP active-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-base-unmanaged-large-flow-count	Indicates the number of UDP active-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-large-flow-count	Indicates the number of UDP active-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-managed-large-flow-count	Indicates the number of UDP active-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-ext-unmanaged-large-flow-count	Indicates the number of UDP active-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-large-flow-count	Indicates the number of UDP total-base-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-managed-large-flow-count	Indicates the number of UDP total-base-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-base-unmanaged-large-flow-count	Indicates the number of UDP total-base-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-large-flow-count	Indicates the number of UDP total-ext-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-managed-large-flow-count	Indicates the number of UDP total-ext-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-ext-unmanaged-large-flow-count	Indicates the number of UDP total-ext-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-normal-flow-count	Indicates the number of TCP active-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-active-large-flow-count	Indicates the number of TCP active-large-flow count for Cisco Ultra Traffic Optimization.
tcp-active-managed-large-flow-count	Indicates the number of TCP active-managed-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-active-unmanaged-large-flow-count	Indicates the number of TCP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-normal-flow-count	Indicates the number of TCP total-normal-flow count for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-count	Indicates the number of TCP total-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-managed-large-flow-count	Indicates the number of TCP total-managed-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-unmanaged-large-flow-count	Indicates the number of TCP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-io-bytes	Indicates the number of TCP total-IO bytes for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-bytes	Indicates the number of TCP total-large-flow bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-bytes	Indicates the number of TCP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-ms	Indicates the number of TCP total-recovered capacity ms for Cisco Ultra Traffic Optimization.
udp-active-normal-flow-count	Indicates the number of UDP active-normal-flow count for Cisco Ultra Traffic Optimization.
udp-active-large-flow-count	Indicates the number of UDP active-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-managed-large-flow-count	Indicates the number of UDP active-managed-large-flow count for Cisco Ultra Traffic Optimization.
udp-active-unmanaged-large-flow-count	Indicates the number of UDP active-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-normal-flow-count	Indicates the number of UDP total-normal-flow count for Cisco Ultra Traffic Optimization.
udp-total-large-flow-count	Indicates the number of UDP total-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-managed-large-flow-count	Indicates the number of UDP total-managed-large-flow count for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-total-unmanaged-large-flow-count	Indicates the number of UDP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
udp-total-io-bytes	Indicates the number of UDP total-IO bytes for Cisco Ultra Traffic Optimization.
udp-total-large-flow-bytes	Indicates the number of UDP total-large-flow bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-bytes	Indicates the number of UDP total-recovered capacity bytes for Cisco Ultra Traffic Optimization.
udp-total-recovered-capacity-ms	Indicates the number of UDP total-recovered capacity ms for Cisco Ultra Traffic Optimization.
tcp-uplink-drop	Indicates the number of TCP uplink-drop for Cisco Ultra Traffic Optimization.
tcp-uplink-hold	Indicates the number of TCP uplink-hold for Cisco Ultra Traffic Optimization.
tcp-uplink-forward	Indicates the number of TCP uplink-forward for Cisco Ultra Traffic Optimization.
tcp-uplink-forward-and-hold	Indicates the number of TCP uplink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-uplink-hold-failed	Indicates the number of TCP uplink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-uplink-bw-limit-flow-sent	Indicates the number of TCP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-drop	Indicates the number of TCP downlink-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold	Indicates the number of TCP downlink-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward	Indicates the number of TCP downlink-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward-and-hold	Indicates the number of TCP downlink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold-failed	Indicates the number of TCP downlink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-dnlink-bw-limit-flow-sent	Indicates the number of TCP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-dnlink-async-drop	Indicates the number of TCP downlink-async-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold	Indicates the number of TCP downlink-async-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward	Indicates the number of TCP downlink-async-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward-and-hold	Indicates the number of TCP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold-failed	Indicates the number of TCP downlink-async-hold-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-drop	Indicates the number of TCP process-packet-drop for Cisco Ultra Traffic Optimization.
tcp-process-packet-hold	Indicates the number of TCP process-packet-hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward	Indicates the number of TCP process-packet-forward for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-failed	Indicates the number of TCP process-packet-forward-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold	Indicates the number of TCP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
tcp-process-packet-forward-and-hold-failed	Indicates the number of TCP process-packet-forward and hold-failed for Cisco Ultra Traffic Optimization.
tcp-pkt-copy	Indicates the number of TCP packet-copy for Cisco Ultra Traffic Optimization.
tcp-pkt-Copy-failed	Indicates the number of TCP packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy	Indicates the number of TCP process-packet-copy for Cisco Ultra Traffic Optimization.
tcp-process-pkt-copy-failed	Indicates the number of TCP process-packet-copy-failed for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-action-forward	Indicates the number of TCP process packet, no packet found, and action forward for Cisco Ultra Traffic Optimization.
tcp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of TCP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
tcp-process-pkt-no-packet-found-action-drop	Indicates the number of TCP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
tcp-todrs-generated	Indicates the number of TCP TODRs generated for Cisco Ultra Traffic Optimization.
udp-uplink-drop	Indicates the number of UDP uplink-drop for Cisco Ultra Traffic Optimization.
udp-uplink-hold	Indicates the number of UDP uplink-hold for Cisco Ultra Traffic Optimization.
udp-uplink-forward	Indicates the number of UDP uplink-forward for Cisco Ultra Traffic Optimization.
udp-uplink-forward-and-hold	Indicates the number of UDP uplink-forward and hold for Cisco Ultra Traffic Optimization.
udp-uplink-hold-failed	Indicates the number of UDP uplink-hold failed for Cisco Ultra Traffic Optimization.
udp-uplink-bw-limit-flow-sent	Indicates the number of UDP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-drop	Indicates the number of UDP downlink-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-hold	Indicates the number of UDP downlink-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-forward	Indicates the number of UDP downlink-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-forward-and-hold	Indicates the number of UDP downlink-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-hold-failed	Indicates the number of UDP downlink-hold failed for Cisco Ultra Traffic Optimization.
udp-dnlink-bw-limit-flow-sent	Indicates the number of UDP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-async-drop	Indicates the number of UDP downlink-async-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold	Indicates the number of UDP downlink-async-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward	Indicates the number of UDP downlink-async-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward-and-hold	Indicates the number of UDP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.

Bulk Statistics	Description
udp-dnlink-async-hold-failed	Indicates the number of UDP downlink-async-hold failed for Cisco Ultra Traffic Optimization.
udp-process-packet-drop	Indicates the number of UDP process-packet-drop for Cisco Ultra Traffic Optimization.
udp-process-packet-hold	Indicates the number of UDP process-packet-hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward	Indicates the number of UDP process-packet-forward for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-failed	Indicates the number of UDP process-packet-forward failed for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold	Indicates the number of UDP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold-failed	Indicates the number of UDP process-packet-forward and hold failed for Cisco Ultra Traffic Optimization.
udp-pkt-copy	Indicates the number of UDP packet-copy for Cisco Ultra Traffic Optimization.
udp-pkt-Copy-failed	Indicates the number of UDP packet-copy-failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy	Indicates the number of UDP process-packet-copy for Cisco Ultra Traffic Optimization.
udp-process-pkt-copy-failed	Indicates the number of UDP process-packet-copy failed for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-forward	Indicates the number of UDP process packet, no packet found, action forward for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-forward-and-hold	Indicates the number of UDP process packet, no packet found, action forward and hold for Cisco Ultra Traffic Optimization.
udp-process-pkt-no-packet-found-action-drop	Indicates the number of UDP process packet, no packet found, action drop for Cisco Ultra Traffic Optimization.
udp-todrs-generated	Indicates the number of UDP TODRs generated for Cisco Ultra Traffic Optimization.

CHAPTER 8

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 9

Events Monitoring

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
This releae supports communicatation of monitoring information from MME to SCEF through Interworking(IWK) SCEF.	21.20
The Events Monitoring and External-Identifer features are fully qualified in this release.	2119.1
This release supports: • Monitoring Event configuration request and response over S6a and T6a interfaces. • External-identifier support on MME for Monitoring Events feature. **Important** Monitoring Events and External-identifier features are not fully qualified in this release and are available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19
First introduced.	21.18

Feature Description

The Event Monitoring functionality allows monitoring of specific events in the 3GPP system and makes the event information available through either Service Capability Exposure Function (SCEF) or Home Subscriber Server (HSS). Allows the identification of the 3GPP network elements that are suitable for configuring specific events, detecting events, and reporting events to the authorized users. MME supports Roaming functionality for monitoring events through Interworking (IWK) SCEF by communicating the monitoring information to SCEF.

The following example explains a specific use case for an individual subscriber.

A subscriber can track the following events:

- Loss of Connectivity
- UE Reachability
- Location Reporting
- Communication Failure
- Availability after DDN Failure
- Number of UEs Present in a Geographical Area

  Note This is a node level event unlike other events that are specific to a subscriber.

- UE Reachability and Idle Status Indication
- Availability after DDN Failure and Idle Status Indication

- PDN Connectivity Status

In StarOS 21.19 and later releases, MME supports monitoring events on s6a and t6a interfaces for monitoring the following events:

- **Loss of Connectivity**–Event is triggered when UE's radio connectivity is lost. HSS configures the Loss of Connectivity event through ULA/ISDR messages. Event reporting happens through RIR with event-specific parameters. The following AVPs are supported.

Table 3: Supported AVPs

AVPs	Parameters
Loss-Of-Connectivity-Reason - Identifies the reason of loss of connectivity	**UE_DETACHED_MME (0)** **UE_PURGED_MME (4)**

- **UE Reachability**–Monitoring Events reports when UE transitions to ECM-CONNECTED mode (for a UE using Power-Saving Mode or extended idle mode DRX) or when the UE reaches for paging (for a UE using extended idle mode DRX).

Table 4: Supported AVPs

AVPs	Parameters
UE-Reachability-Configuration	**[Reachability-Type]** **[Maximum-Response-Time** MME uses the Maximum Response Time as the Active Time for PSM UEs only if the configuration is enabled as part of Monitoring Events Profile.
Event Reporting	**Reachability-Information** **Maximum-UE-Availability-Time**

- **Location Reporting**–Monitoring Events sends report when the MME detects that the UE changed location with the granularity as requested by the monitoring event configuration. If there is Minimum Reporting Interval, while the timer is running, the MME suppresses sending consecutive Location Reporting notification. On timer expiry MME sends location information that was contained in the latest suppressed Location Reporting notification and restarts the timer. The supported Accuracy in the network is at either cell level (ECGI), eNodeB, or Tracking Area (TA) level.

  Location Reporting is supported for Current Location or the Last Known Location of a UE. One-time and Continuous Location Reportings are supported for the Current Location. The Location Reporting type allows:

  - One Time Reporting: If the requested location type is "Last known location", it is one time reporting only.
  - Continuous Location Reporting: If a Minimum Reporting Interval is not available, the serving node sends a notification every time it becomes aware of a location change. If periodic time was provided as part of the configuration, MME starts the periodic timer, after sending the first location report.

Table 5: Supported and Unsupported AVPs

AVPs	Parameters
Location-Information-Configuration	**[MONTE-Location-Type]** **[Accuracy]** **[Periodic-Time]**
MONTE-Location-Type	**CURRENT_LOCATION (0)** **LAST_KNOWN_LOCATION (1)** **Note** The default value, when this AVP is not included, is LAST_KNOWN_LOCATION (1).
Common Parameter	Maximum number of reports should not be greater than one if Monitoring-Type is **Location Reporting (2)** and MONTE-Location-Type is **Last Known Location (1)**
MME Location Information	**[E-UTRAN-Cell-Global-Identity]** **[Tracking-Area-Identity]** **[eNodeB-ID]**
Unsupported AVP	
MME Location Information	**[Geographical-Information]** **[Geodetic-Information]** **[Current-Location-Retrieved]** **[Age-Of-Location-Information]** **[User-CSG-Information]** **[Extended-eNodeB-ID]**

- **Communication Failure** –Event is triggered when the MME becomes aware of a RAN or NAS failure event. Event configuration by HSS through ULA/ISDR messages.

Table 6: Supported AVPs

AVPs	Parameters
Communication-Failure-Information	**[Cause-Type]** **[S1AP-Cause]**

- **Availability after DDN Failure**–MME triggers this event when the UE contacts the network, for example, to perform a TAU, or to execute a service request after DDN Failure.

Note Not every DDN failure triggers this event. This event is triggered only when DDN failure had occurred due to UE being in PSM or Extended idle mode DRX.

- Maximum number of Reports is not applicable for this event.

Table 7: Supported AVPs

AVPs	Parameters
Event configuration	**Monitoring -Type: AVAILABILITY_AFTER_DDN_FAILURE (6)**
Event Reporting	**Monitoring-Type set to AVAILABILITY_AFTER_DDN_FAILURE (6)**

- **Number of UEs Present in a Geographical Area**–This is triggered from SCEF to MME in the Configuration Information Request (CIR) message. MME responds with a Configuration Information Answer (CIA) message with the reports, status, and supported Attribute-Value Pair (AVPs). From SCEF, MME processes EUTRAN, TAI, enodeB as hex values based on the 3GPP specifications 29.272, and 29.274.

The following table describes the supported feature AVPs.

Table 8: Supported and Unsupported AVPs

AVPs	Parameters
Number-of-UE-Per-Location-Configuration	**{ EPS-Location-Information }** **[IMSI-Group-Id]** MME supports parsing of one Monitoring-Event-configuration with a maximum of three Number-of-UE-Per-Location-Configurations (in CIR). It responds with a CIA message with Monitoring-Event-Config-Status and one Monitoring-Event-Report.
MME-Location-Information	**[E-UTRAN-Cell-Global-Identity]** **[Tracking-Area-Identity]** **[User-CSG-Information]** **[eNodeB-ID]** For the above mentioned Location Information criteria, MME counts the number of UEs matching the criteria and sets the UE count in the CIA.

AVPs	Parameters

Number-of-UE-Per-Location-Report	**{ EPS-Location-Information }**
	{ UE-Count }
	IMSI-Group-Id
	{ Group-Service-Id }
	{ Group-PLMN-Id }
	{ Local-Group-Id }

IMSI-Group-Id	**{ Group-Service-Id }**
	{ Group-PLMN-Id }
	{ Local-Group-Id }

Unsupported AVP	
Location Information	**[Geographical-Information]** **[Geodetic-Information]** **[Current-Location-Retrieved]** **[Age-Of-Location-Information]** **[Extended-eNodeB-ID]** For the above mentioned criteria, MME sets UE count as 0 in the CIA.

Limitations: The Monitoring-Event-configuration AVPs have the following limitations:

- If the Number of UE events is unsupported, then MME responds with a Result-Code set to DIAMETER_UNABLE_TO_COMPLY.
- If the Monitoring Event type is other than seven (Number-of-UE-Per-Location-Configuration) or Number-of-UE-Per-Location-Configuration AVP is empty, then MME responds with a Result-Code set to DIAMETER_UNABLE_TO_COMPLY.
- If the TA/ECGI location requested by the SCEF is not served by the MME, then the MME sets UE count as 0 in the CIA.
- CIR sent from SCEF within three seconds from previous CIR gets queued in MME with the maximum queue size of five.

- **PDN Connectivity Status**–Supports the following AVPs.

Table 9: Supported AVPs

AVPs	Parameters
PDN-Connectivity-Status-Event configuration	HSS to MME: ULA / ISDRA Monitoring Event Type is set to PDN-Connectivity-Status-Configuration **[Service-Selection]** If the Service-Selection AVP is available, then the monitoring applies to that specific APN. If the Service-Selection is not available the monitoring request applies to all APNs.
PDN-Connectivity-Status-Report	**{ Service-Selection }** **{ PDN-Connectivity-Status-Type }** **[PDN-Type]** **[Non-IP-PDN-Type-Indicator]** **[Non-IP-Data-Delivery-Mechanism]** **[Served-Party-IP-Address]**

- **Idle Status Indication for Availability after DDN failure and UE reachability** – MME supports Idle Status Indication when the UE transitions into idle mode. The MME includes the time at which the UE transitioned into idle mode, the active time, and the periodic TAU/RAU time granted to the UE by the MME in the notification sent towards the SCEF, the eDRX cycle length, and the suggested number of downlink packets if a value is provided to the S-GW.

Table 10: Supported AVPs

AVPs	Parameters
Idle-Status-Indication	**[Idle-Status-Timestamp]**–Time at which the UE transitioned into idle mode. **[Active-Time] d**– The active time if PSM is enabled. **[Subscribed-Periodic-RAU-TAU-Timer]**–The periodic TAU/RAU time granted to the UE by the MME. **[eDRX-Cycle-Length]**–The eDRX cycle length if eDRX is enabled. **[DL-Buffering-Suggested-Packet-Count]** –The Suggested number of downlink packets sent to the S-GW.

- **External-identifier on MME for Monitoring Events**– The External-identifier feature is applicable for the ULR/ULA, DSR/DSA, and IDR/IDA command pairs over S6a (and S6d), when the MME supports the External-identifier.

  - MME includes the External-identifier or the MSISDN if present in the subscription data received from the HSS in the User Identifier AVP towards SCEF in RIR.

  Note If the MME does not support External-identifier, MME will not process the External-Identifier if received in the subscription data.

  - When you receive External Identifier AVP as part of Monitoring Event Configuration AVP, it has higher precedence than the same AVP received under Subscription Data AVP of ULA/ISDR.

- **Gtpv2 (S10 and S3 Interfaces)**–Monitoring Event information IE and Monitoring Event Extension Information IE are supported and filled as applicable.

- **Tracking Area Code in RIR**–MME includes the following AVP in every RIR Monitoring Event Report Message towards SCEF (except when the monitoring type is Location Reporting) to report UE location (TAC) when the event report is generated. MME supports enabling and disabling configuration at CallControlProfile level (Monte profile) and MME service (Monte profile). By default, it is disabled.

```
Monitoring-Event-Report
 [ EPS-Location-Information ]
         [MME-Location-Information]
              [ Tracking-Area-Identity ]
```

Rat-Type and IMSI-Group-Id Filters

The following method describes how to configure Rat-Type and IMSI-Group-Id filters for the operators:

- By default the Rat-Type Filter is configured to all.
- For the Number of UEs requested location criterion, MME matches the requested location criteria for each UE.
  - If IMSI-Group filtering is requested, then the exact count of the number of UEs belonging to the provided IMSI Group that are known to be at the requested location is included in the CIA.
  - If IMSI-Group filtering is not requested, then the exact count of the number of UEs belonging to the provided requested location is calculated and included in the CIA.

To calculate the number of UEs count belonging to a requested location, MME does number of UEs filtering based on the Rat-Type and IMSI-Group-ID:

By default, the Rat-Type Filter is configured to access type 'all' for number of UE events under *monitoring-event* profile.

- MME checks if a subscriber Rat-Type matches with the configured RAT-Type.
- If the Rat-Type configured does not match, MME will not do further location search for that subscriber.
- If Rat-Type matches, it proceeds to check if the IMSI-Group-Id is present in CIR request message.

If the IMSI-Group-Id filtering is requested:

- MME checks to match with any of the subscribers configured IMSI-Group-Id (each subscriber can have maximum of five IMSI-Group-ID configured). If a match is found, then the UE/subscriber location is matched with the requested location criteria and only then number of UEs count is incremented.

If the IMSI-Group-Id filtering is not requested:

- UE location is matched with the requested location criteria. If match is found only, then number of UEs count is incremented. This is performed for all the UEs located at MME.

Session Recovery Support

MME supports the recovery of monitoring events configurations when there is a session manager task failure. Following are the post recovery functions:

- If the periodic time is present as part of the location reporting configuration, the same gets restarted only after sending the report for first location change.
- UE reachability reporting related to paging occasions for UEs in idle mode gets resumed only when the UE moves again to the idle state.

Note Monitoring events-related statistics are not recovered as part of recovery mechanism.

How it Works

This section describes how monitoring events work for the following events:

- **Number of UEs Present in a Geographical Area** –MME and SCEF exchanges the UE information based on the location information through Configuration Information Request (CIR) and Configuration Information Answer (CIA) messages
- **Communication Failure**–The communication failure events that happen between MME and HSS can be monitored, when HSS sends a communication failure message in the monitoring event configuration. MME receives the message through Insert Subscriber Data Request (ISDR) or Update Location Answer (ULA) on s6a interface. The MME sends the Monitoring Event Report for the communication failure event to SCEF over t6a interface through RIR (Reporting-Information-Request) messages.
- **External-identifier**–MME supports the following External-identifier functions:
  - If enabled in CLI, updates HSS on External-identifier support.
  - If MME receives external identifier as part of Monitoring Event Configuration Grouped AVP, this external identifier is sent in RIR to SCEF.
  - If external identifier AVP is NOT received as part of Monitoring Event Configuration AVP but, received in Subscription Data AVP, the same is updated in RIR to SCEF.
- **IMSI-Group**–MME supports following IMSI-Group-Id functions:
  - Updates HSS through ULA, ISDR, and DSDR.
  - MME replaces stored IMSI-Group Ids, if any, with the received information on receiving IMSI-Group-Id AVP(s) within the Subscription-Data AVP.
  - Supports maximum of five IMSI-Group-ID for each UE.

- **UE Reachability**–MME uses the timer values sent by HSS for PSM enabled UEs when configured through cli. By default, it is disabled.

Table 11: MME behavior when PSM or eDRX or both are enabled

If Only PSM is Enabled	If Only eDRX is Enabled	If Both PSM and eDRX is Enabled
• RIR is sent when UE gets connected without Maximum-UE-Availability-Time. • If idle indication is enabled, RIR is sent when UE moves to idle.	• RIR is sent when UE gets connected without Maximum-UE-Availability-Time. • RIR is sent before every paging occasion with PTW as Maximum-UE-Availability-Time. • If idle indication is enabled, RIR is sent when UE moves to idle.	• RIR is sent when UE gets connected without Maximum-UE-Availability-Time. • If idle indication is enabled, RIR is sent when UE moves to idle. • RIR is sent before every paging occasion with PTW as Maximum-UE-Availability-Time.

Monitoring Events WorkFlow

This section describes the call flows in which the monitoring events procedures are performed.

Figure 4: Call Flow from SCEF to MME

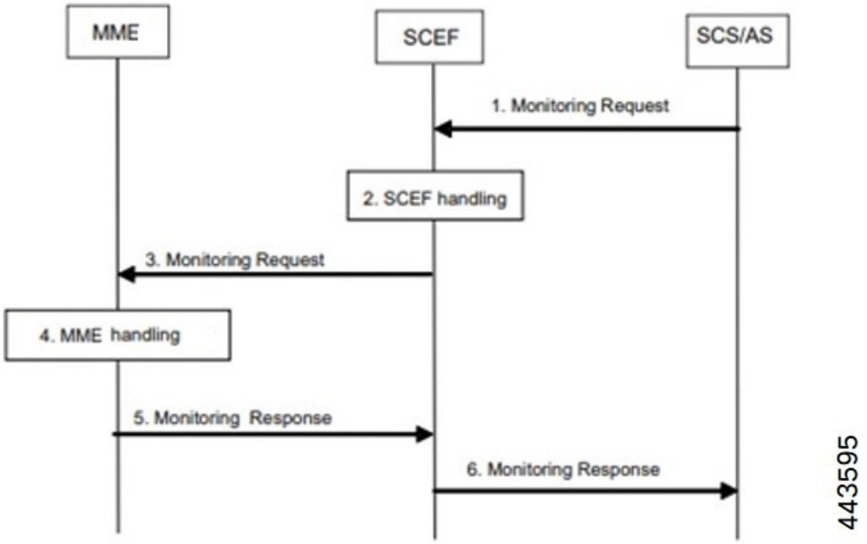


Figure 5: Call Flow from SCEF to MME

Table 12: Monitoring Event Configuration and Deletion through MME Procedure

Step	Description
1	The SCS/AS sends a Monitoring Request (SCS/AS Identifier, Monitoring Type, Monitoring Duration, Maximum Number of Reports, T8 Destination Address, T8 Long-Term Transaction Reference ID (TLTRI) for Deletion message to the SCEF. The SCEF assigns a TLTRI that identifies the Monitoring Request.
2	The SCEF stores the TLTRI, and also assigns it to an SCEF Reference ID.
3	The SCEF sends Monitoring Request such as SCEF ID, SCEF Reference ID, Monitoring Type, Monitoring Duration, Maximum Number of Reports and SCEF Reference ID for Deletion message to the MME.
4	• The MME examines whether to accept the request from the SCEF based on operator configuration or whether it serves the SCEF Reference ID for Deletion and can delete it. • If acceptable, the MME stores SCEF ID, SCEF Reference ID, Monitoring Duration, Maximum Number of Reports and other relevant parameters, unless it is a One-time request, and the Monitoring Event is available to the MME currently. • The MME deletes the monitoring configuration identified by the SCEF Reference ID for Deletion, if provided.
5	The MME sends a Monitoring Response (SCEF Reference ID, Cause) message to the SCEF to acknowledge acceptance of the Monitoring Request and to provide the requested monitoring information or to acknowledge the deletion of the identified monitoring event configuration, if it was requested.
6	The SCEF sends a Monitoring Response (TLTRI, Cause, Monitoring Event Report) message to the SCS/AS to acknowledge acceptance of the Monitoring Request and to provide the requested monitoring information in Monitoring Event Report parameter or to acknowledge the deletion of the identified monitoring event configuration at the time of request.

Figure 6: Monitoring Event Configuration and Deletion through HSS Call Flow

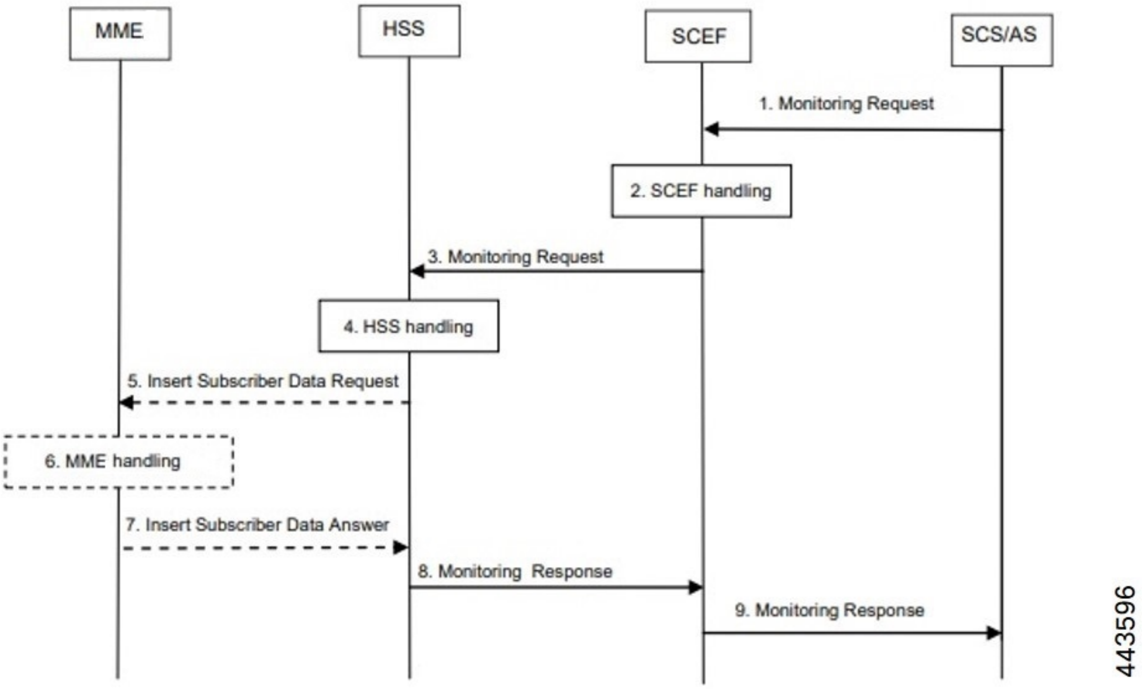


Table 13: Monitoring Event Configuration and Deletion through HSS Procedure

Step	Description
1	The SCS/AS sends a Monitoring Request message to the SCEF with necessary parameters. The request can be for both configuring and deleting any existing configuration..
2	The SCEF stores parameters provided and takes actions based on operator policies. The SCEF stores the T8 Long-Term Transaction Reference ID (TLTRI) and also assigns to an SCEF Reference ID.
3	The SCEF sends a Monitoring Request message to the HSS to configure the given Monitoring Event on the HSS/MME.
4	The HSS examines the Monitoring Request message, stores the parameter, and takes action based on operator policies.
5	HSS sends an Insert Subscriber Data Request (Monitoring Type, SCEF ID, SCEF Reference ID, Maximum Number of Reports, Monitoring Duration, SCEF Reference ID for Deletion, and so on) message to the MME for each individual UE. **Note** Monitoring Event Configuration can also be sent over ULA.

Step	Description
6	The MME stores the received parameters and starts to watch for the indicated Monitoring Event unless, it is a One-time request, and the Monitoring Event is available to the MME at the time of sending Insert Subscriber Data Answer. The MME deletes the monitoring configuration identified by the SCEF Reference ID for Deletion, if provided. MME does not perform any duplication checks regarding SCEF-Ref-id. To know more about MME handling refer the *MME Handling of Configuration and Deletion* section.
7	If the monitoring configuration is successful, the MME sends an Insert Subscriber Data Answer (Cause) message to the HSS. If the requested Monitoring Event is available to the MME at the time of sending Insert Subscriber Data Answer, then the MME includes the Monitoring Event Report in the Insert Subscriber Data Answer message. **Note** If configuration was received over ULA, reports will be sent over RIR towards SCEF
8	HSS sends a Monitoring Response message to the SCEF to acknowledge acceptance of the Monitoring Request.
9	SCEF sends a Monitoring Response message to the SCS/AS to acknowledge acceptance of the Monitoring Request.

MME Handling of Configuration and Deletion:

- The Diamproxy client, which is running on the StarOS device receives Monitoring Event Configuration Requests from the HSS through s6a interface under Subscription data grouped AVP or from the SCEF through t6a in Configuration Information Request message.
- AVP information received from the device is parsed and the message is sent to corresponding Session Manager for further handling.
- The Session Manager parses the event message and decodes the appropriate event.

  Important MME running as part of Session Manager identifies if the message is synchronous and responds immediately or asynchronously. Requests from HSS are received in the Update Location Answer(ULA)/Insert Subscriber Data Request(ISDR).

  If the response is determined as asynchronous, then the response is notified through t6a to SCEF directly.
- Event handling routine invokes handler for appropriate events.
- After the event handling, the report is sent through Monitoring Event Report message on s6a and t6a interface. Based on the event type, MME chooses to dispatch the report on S6a interface.
- If available, the HSS S6a Insert Subscriber Data Answer can contain the report for the Monitoring event (s). Configuration Information Answer and Reporting Information Request message can contain the report on t6a interface.

Limitation: After session manager recovery the Diamproxy client continues to send CIR to the same cached session manager instance until the next CMR is triggered from any of the active session manager instances. During this period MME will not handle the CIR message.

Figure 7: Monitoring Events Call Flow through Interworking (IWK) SCEF

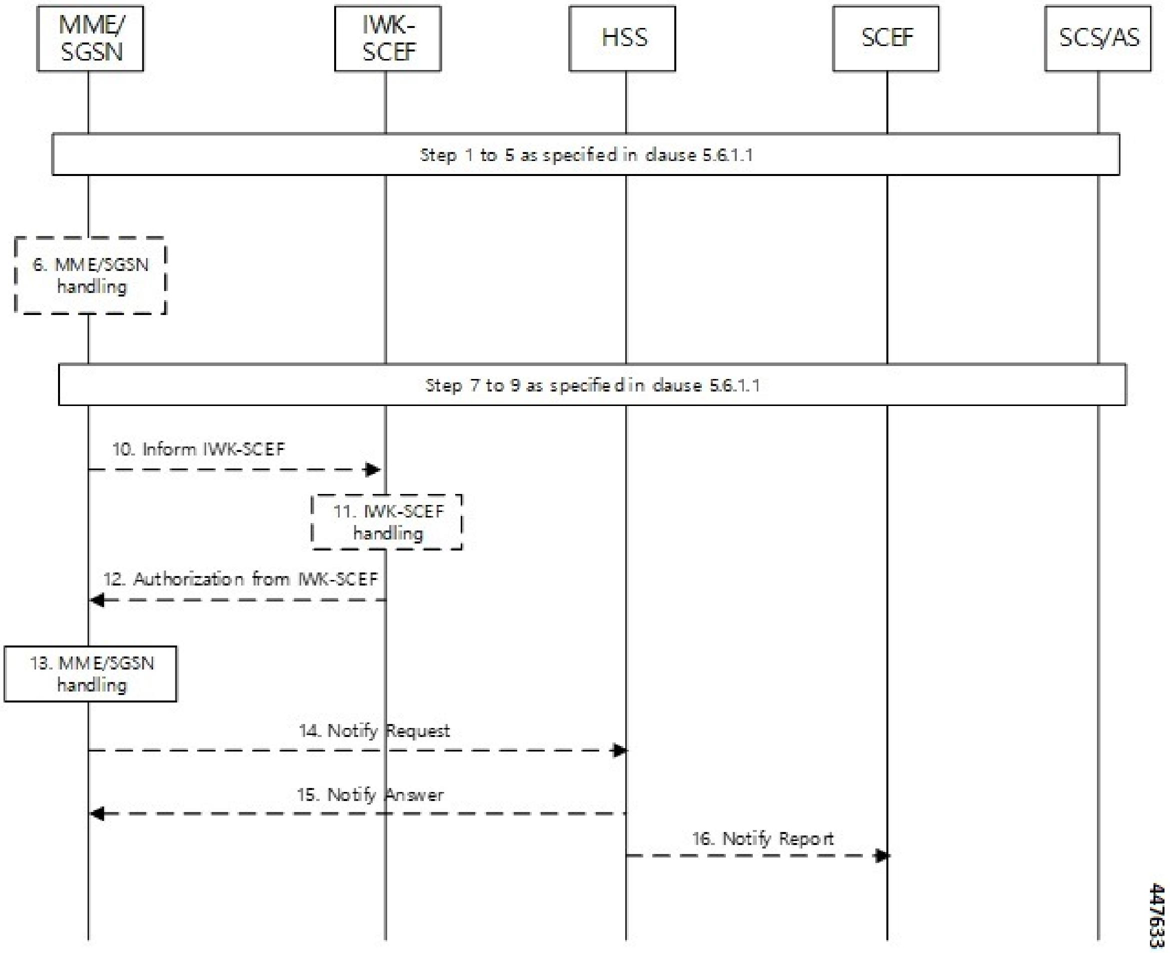


Table 14: Monitoring Event Configuration through IWK-SCEF Procedure

Step	Description
1 through 9	MME establishes a UE connection and learns the monitoring event configuration parameters from HSS through S6a interface. **Note** HSS S6a subscription data contains Monitoring event configuration AVPs that MME need to parse to learn the event.

Step	Description
10	MME checks: • for the roaming subscribers who have received monitoring event configuration in ULA/ISDR from HSS • whether roaming support and IWK SCEF details are configured as part of monitoring event profile. MME then constructs a Configuration Information Request message (CIR), which includes monitoring event configuration as received from HSS and Supported Features AVP. MME starts a timer for 6 seconds after sending CIR. When DSDR / ISDR with 'scef ref id for deletion' is received, MME deletes the respective config locally and also sends CIR with details of events to be deleted, with corresponding scef reference id filled as part of "SCEF-Reference-ID-for-Deletion" AVP.
11	IWK-SCEF either accepts or rejects events.

Step	Description
12 through 15	

Step	Description

	• If there is no response, MME considers timeout as failures and does not apply new monitoring configurations and for each rejected events MME sends NOR towards HSS separately.
	• If CIA is received from MME, MME passes through the message and checks if IWK-SCEF has sent any of the below failure causes and it takes necessary action accordingly.
	`At Message level ,`
	`Experimental code AVP :`
	`DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510)`
	`DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511)`
	• If Experimental code AVP is not present, MME checks for Result code AVP.
	• If MME receives any of the above failure causes or result code is not success, MME does not apply any of the new monitoring events configuration sent in CIR and for each rejected events MME sends NOR towards HSS separately.
	• If message level IWK SCEF responds as success, MME checks for contents filled with Service-result-code AVP for every configuration sent.
	• If **Service-result-code** AVP is filled with Experimental Result Code values, MME checks for below causes, else MME considers it as Result-code values and takes action accordingly:
	`Experimental code values checked by MME:`
	`DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510)`
	`DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511)`
	`DIAMETER_ERROR_CONFIGURATION_EVENT_STORAGE_NOT_SUCCESSFUL (5513)`
	`DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT (5514)`
	• If MME receives any of the above failure causes or result code is not success, MME does not apply those failed monitoring events configuration and for each rejected events MME sends NOR towards HSS separately. MME applies for the monitoring configurations which IWK SCEF had returned success and start reporting.
	• MME applies the monitoring events configuration that is accepted by IWK-SCEF.
	• MME continues to monitor for the events, triggers events, and sends the report to IWK-SCEF through Reporting Information Request (RIR).
	Important Unless IWK-SCEF rejects with any of the above failure causes,

Step	Description
	MME considers the same as success and monitoring events configuration are applied for subscribers.

Note

- MME does not include Monitoring Event Report as part of CIR to IWK SCEF. Instead, MME sends the available reports as part of RIR No reports are filled in ISDA for roaming subscribers.
- When current location is requested in ISDR as part of monitoring events configuration, paging or location reporting control gets triggered based on UE state. RIR with location report is sent only after receiving response for paging or location reporting and CIA from IWK SCEF.
- Number of UEs in geographical area is a node level messages and behavior will be the same for both roaming and home subscribers.

Monitoring Events Report Call Flow and Procedure

The following section describes call flows and procedures of monitoring events report.

Figure 8: Call Flow

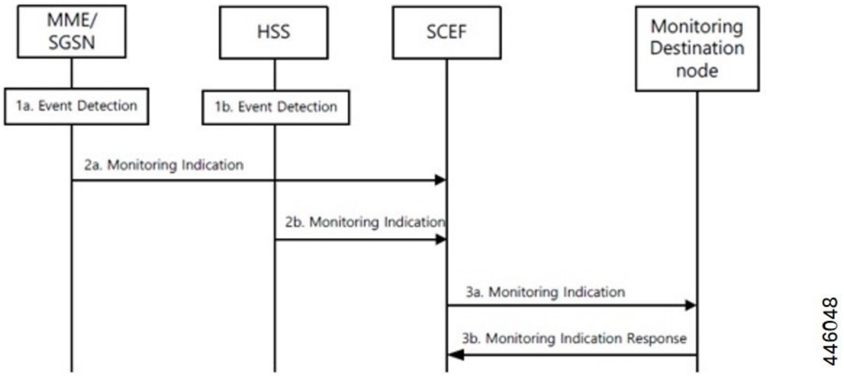

MME/
SGSN
HSS
SCEF
Monitoring
Destination
node
1a. Event Detection
1b. Event Detection
2a. Monitoring Indication
2b. Monitoring Indication
3a. Monitoring Indication
3b. Monitoring Indication Response
446048

Table 15: Monitoring Event Report Procedure

Step	Description
1	MME detects events.
2	Report is sent through Monitoring Event Report message on s6a and t6a interface. For roaming subscribers, the report is sent through t6ai interface.

Configuring, monitoring, and reporting of new messages and AVPs for subscribers are supported by following mechanisms:

- Monitoring Event Configuration AVP in CIR message from SCEF over t6a interface.

- Monitoring Event Configuration in ULA/ISDR from HSS over s6a interface.
- Monitoring Event Report AVP from MME over t6a interface through CIA for the number of UE in a geographical area event.
- Monitoring Event Report AVP to HSS over S6a interface through ISDA message.
- Monitoring Event Report AVP to SCEF over t6a interface through RIR message.

Limitations

Following limitations are applicable for monitoring events functionality:

- Maximum of one Monitoring Event Configuration for each event for the UE is supported in MME. If MME receives same monitoring event configuration for same UE and Type, MME replaces the existing configuration and starts monitoring event reporting based on the new configuration.

  For Number of UEs in Geographic area, maximum of one Monitoring-Event-Configuration for each CIR message is supported.
- We recommend limiting the maximum number of UE with monitoring events enabled and active up to 50 percent of the maximum sessions for each session manager instance. Beyond this limit, there might be an impact on memory and CPU resources. There are no hard limits restricted within MME.
- Maximum of five IMSI-Group-Ids for each UE or subscriber is configured and maintained.
- If SCEF does not respond, MME does not retry the Reporting Information Request.
- Maximum range of Monitoring-Duration supported is limited to 30 days.
- The maximum length of SCEF-Id, SCEF-Realm, External-Identifier, Service-Selection AVP, and Local_Group_id AVP is 128 characters.

Supported Standards

The Monitoring Events feature complies with the following 3GPP Release 16.0.0 specification standards:

- 3GPP TS 23.682
- 3GPP TS 29.128
- 3GPP TS 29.272
- 3GPP TS 29.274
- 3GPP TS 29.128
- 3GPP 23.401

Common Procedures and Parameters for Monitoring Events

Following procedures, messages and common parameters are supported for Monitoring Events.

Table 16: Supported Interfaces and Procedures

Interface	Description
S6a	Update Location Request Update Location Answer Insert Subscriber Data Request Insert Subscriber Data Answer Delete Subscriber Data Request Delete Subscriber Data Answer Notification Request Notification Answer
T6a	Reporting Information Request Reporting Information Answer Configuration Information Request Configuration Information Answer

Following table lists common AVPs on T6a and S6a interfaces.

Table 17: Common Procedures and AVPs

Procedure	Common AVPs
Monitoring-Event-Configuration	**[SCEF-Reference-ID]** **{ SCEF-ID }** **{ Monitoring-Type }** **[SCEF-Reference-ID-for-Deletion]** **[Maximum-Number-of-Reports]** **[Monitoring-Duration]** **[UE-Reachability-Configuration]** **[Location-Information-Configuration]** **[Number-Of-UE-Per-Location-Configuration]** **Note** Allows Maximum of 3 AVPs for each MONTE configuration. **PDN-Connectivity-Status-Configuration**
Monitoring-Event-Status	**[Service-Report],{ SCEF-Reference-ID }, [SCEF-ID]**

Procedure	Common AVPs
Monitoring-Event-Report	**SCEF-Reference-ID },[SCEF-ID], [Monitoring-Type], [Reachability-Information], [EPS-Location-Information],[Communication-Failure-Information],[Number-Of-UE-Per-Location-Report] , [Loss-Of-Connectivity-Reason], [Idle-Status-Indication], [Reporting-Time-Stamp], [Maximum-UE-Availability-Time], Maximum-UE-Availability-Time], [PDN-Connectivity-Status-Report]**

Following lists of GTPv2 IEs (S10 and S3) are supported for monitoring events:

- Monitoring Event Information
- Monitoring Event Extension Information

Configuring MME Services and Call Control Profiles

This section describes how to configure monitoring events for a call control profile.

Important When you configure MME service for users, monitoring-events is disabled by default. Whenever the operator enables the **MONTE** feature in a call control profile or mme-service, it is mandatory to associate a monitoring-event-profile.

Enabling the CLI monitoring-events in a Call Control Profile

Use the following configuration to enable CLI monitoring-events for all users in a call control profile.

```
configure
  call-control-profile  profile_name
    [ no | remove ] monitoring-events
    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 and must be a string of 1-64 characters.

- **monitoring-events**: Enables the monitoring events under the call control profile mode.
- **no**: Disables CLI monitoring events in a call-control-profile for an MME service.
- **remove**: Removes the event configuration from the call-control-profile.

  :

Associating Monitoring Events Profile under Call Control Profile

Use the following configuration to associate a monitoring-event-profile CLI for all users in a call control profile. For the number-of-ue-events profile, the operator should enable the CLI and must associate at mme-service level. If the operator enables it at CCP level, then there will not be any effect as the configuration is a node-level message.

```
configure
   call-control-profile  profile_name
      associate monitoring-event-profile profile_monte
      end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the call control profile name, and must be an alphanumeric string of 1-64 characters.
- **associate monitoring-event-profile** *profile_monte*: Associates monitoring profiles in a call control profile whenever MONTE feature is enabled.

Configuring Monitoring Events for an MME Service

Use the following configuration to monitor events for an MME service:

```
configure
   context context_name
      mme-service service_name
         [ no ] monitoring-events
         end
```

NOTES:

- **mme-service** *service_name*: Specifies the name of the MME service and and must be a string of 1-63 characters.
- **monitoring-events**: Enables monitoring events for MME service users.
- **no**: Disables CLI monitoring-events in an MME Service.

Associating Monitoring Events Profile under MME Service

Use the following configuration to associate a monitoring-event-profile CLI for all users in an MME service.

Important monitoring-event-profile is mandatory for MME to start event monitoring.

```
configure
   context context_name
      mme-service service_name
         associate monitoring-event-profile  profile_monte
         end
```

NOTES:

- **mme-service** *service_name*: *service_name* specifies the MME service name, and must be a string of 1 to 63 characters.
- **monitoring-events**: Configures monitoring events for MME service users.
- **associate monitoring-event-profile** *profile_monte*: Associates monitoing profiles in an mme-service whenever MONTE feature is enabled.

Verifying the CLI monitoring-events in an MME Service

The following command is used to verify the parameters for Event Monitoring in an MME service:

- **show mme-service all | grep Monitor**

Sample Output Configuration:

```
[ingress]asr5500# show mme-service all | grep Moni
Tuesday April 28 20:31:23 IST 2020
Monitoring Event Profile : test
Monitoring Events : Enabled
```

Configuring Monitoring Events Profile

This section describes how to configure monitoring events profile in a lte-policy mode.

Configuring monitoring-event-profiles

Use the following command to configure monitoring event profiles to enable list of event types that MME can support.

```
configure
  lte-policy
    monitoring-event-profile  profile_monte
      events
      end
```

NOTES:

- **lte-policy** *profile_name*: Creates an instance of the lte-policy for monitoring events configuration.
- **monitoring-event-profile** *profile_monte profile_name*: Creates a monitoring events profile name under the lte-policy mode.
- **events** : Specifies the event types that MME supports. Options include:
  - loss-of-connectivity
  - ue-reachability
  - location-reporting
  - communication-failure
  - availability-after-ddn-failure

- idle-status-indication
- pdn-connectivity-status
- number-of-ue-in-geo-area
- Roaming Support

Note If the user configures with Idle Status Indication under the monitoring event profile, then it allows enabling of the following events:

- If UE Reachability (1) is configured, enables UE Reachability and Idle Status Indication(8) events.
- If Availability after DDN failure (6) is configured, enables Availability after DDN Failure and Idle Status Indication (9) events.

Enabling Additional CLI Parameters under number-of-ue-in-geo-area

Use the following CLI configuration to enable or disable SCEF IDs to list authorized SCEFs that can request number of UEs present in a geographical area:

Note Since this a node-level message, ensure to enable this CLI command and associate at mme-service level as number of UE events.

```
configure
  lte-policy
    monitoring-event-profile profile_monte
      [ no ] events number-of-ue-in-geo-area  authorized-scef-id  scef_id

      end
```

NOTES:

- **lte-policy** : Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile** *profile_monte* : Creates a monitoring events profile name under the lte-policy mode.
- **events number-of-ue-in-geo-area** : Lists the event type instance to enable the authorized SCEFs.
- **authorized-scef-id**: Enables SCEF IDs to list authorized SCEFs who can request this events.
- **[no]**: Disables authorized SCEF ID.

Configure RAT-Type Filter

Use the following CLI configuration to list number of UEs that are calculated based on access types.

```
configure
  lte-policy
```

```
      monitoring-event-profile profile_monte
         events number-of-ue-in-geo-area { nb-iot | wb-eutran }
         default events number-of-ue-in-geo-area
         end
```

NOTES:

- **lte-policy** : Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile***profile_monte* : Creates a monitoring events profile name under the lte-policy mode.
- **events number-of-ue-in-geo-area** : Lists the event type instance to enable the access type.
- **nb-iot**: Counts only UEs with Access type as NB-IOT.
- **wb-eutran**: Counts only UEs with Access type as EUTRAN.

Enabling Additional CLI Parameters under ue-reachability

Use the following CLI configuration to enable or disable the HSS provided values for active timer t3224 and subscribed periodic time t3412_E.

```
configure
   lte-policy
      monitoring-event-profile profile_monte
         [ no ] events ue-reachability hss-requested-psm-timers
         end
```

NOTES:

- **lte-policy** *profile_name*: Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile***profile_monte* : Creates a monitoring events profile name under the lte-policy mode.
- **no events ue-reachability**: Disables UE reachability events.
- **hss-requested-psm-timers**: MME applies t3324 and t3412_e timers from subscription data received from HSS. Overrides values defined in PSM policy.

edrx-reporting-occasions

Use the following LTE policy configuration to send the UE Reachability report on every paging occasions.

```
configure
   lte-policy
      monitoring-event-profile profile_monte
         events ue-reachability edrx-reporting-occasions
         minimum-cycle-value value reporting-offsetvalue
         end
```

NOTES:

- **lte-policy** *profile_name*: Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile***profile_monte* : Creates a monitoring events profile name under the lte-policy mode.

- **events ue-reachability** : Creates an instance of ue-reachability events.
- **edrx-reporting-occasions**: Triggers report on paging occasion for eDRX enabled UEs.

  Note By default, the minimum-edrx-value is 13 and the reporting offset is 2 seconds.

- **minimum-cycle-value**: The minimum eDRX cycle value, above which the UE reachability reporting on paging occasions gets triggered.
- **reporting-offset**: Indicates how early the report will be sent before eDRX paging window occurs in seconds.

Track Area Code in Reporting Information Request

Use the following command to fill the Tracking Area Code (tac) value in every event reporting (RIR message) that is sent to SCEF. By default, the TAC in RIR feature is disabled..

```
configure
  lte-policy
    monitoring-event-profile profile_monte
      no events tac-in-rir
      end
```

NOTES:

- **lte-policy** *profile_name*: Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile***profile_monte* : Creates a monitoring events profile name under the lte-policy mode.
- **no events tac-in-rir**: Disables or fills TAC in all RIR messages sent to SCEF.

Enabling Roaming Support

Use the following CLI configuration to enable Roaming support:

Note It is mandatory to configure both host and realm of IWK-SCEF for roaming subscribers. Otherwise, MME considers roaming subscribers as home subsribers and routing of messages will happen accordingly.

```
configure
  lte-policy
    monitoring-event-profile map
      [no]roaming-support  dest host  scef_id
      [no]roaming-support   dest realm realm.com
      end
```

NOTES:

- **lte-policy** : Creates an instance of a lte-policy for monitoring events configuration.
- **monitoring-event-profile** *map* : Creates a monitoring events profile name under the lte-policy mode.

- **[no]roaming-support dest host** : Enables roaming support destination host name to communicate to SCEF through Interworking (IWK).
- **[no]roaming-support dest realm**: Enables roaming support destination realm name to communicate to SCEF through Interworking (IWK).
- **no** : Removes roaming support destination host or destination realm.

Note Make sure to configure both the parameters for roaming subscribers. Otherwise, routing happens like home subscribers.

Configuring External-identifier in lte-policy

This section describes how to configure External-identifiers in a lte-policy CLI.

Enabling external-identifier

Use the following configuration to enable the external-identier CLI in the LTE policy mode.

```
configure
     lte-policy
     monitoring-event-profile  profile_monte  profile_name
     external-identifier
       end
```

NOTES:

- **lte-policy** *profile_name*: Creates an instance of an lte-policy for monitoring events configuration.
- **monitoring-event-profile** *profile_monte profile_name*: Creates a monitoring events profile name under the lte-policy mode.
- **external-identifier**: Enables external-identifier feature support for monitoring-events.

Configuring congestion-action-profile for Monitoring Events

This section describes how to configure congestion action profile for monitoring events.

Enabling a congestion-action-profile Condition for Monitoring Events

Use the following configuration to enable CLI for congestion condition to drop or reject the monitoring-event-config requests in the LTE policy mode.

```
configure
     lte-policy
        [ no ] congestion-action-profile profile_name
```

```
{drop | reject  monitoring-event-config-request}
 end
```

NOTES:

- **lte-policy** : Creates an instance of an lte-policy for monitoring events configuration.
- **[no] congestion-action-profile** : Removes the specified profile from the system.
- **congestion-action-profile** *profile_name* : Creates an instance of congestion profile for monitoring-events.
- **drop | reject monitoring-event-config-request** : Drops or rejects every new incoming Monitoring Event configuration without any reply.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the Monitoring Events feature.

Show Commands and Outputs

show mme-service statistics

show mme-service statistics

The output of this command includes the following fields:

- Loss of connectivity—Indicates the current session statistics of Loss of connectivity event configuration.
- UE Reachability—Indicates the current session statistics of UE Reachability event configurations.
- Location Reporting—Indicates the current session statistics of reporting location event configurations.
- Communication Failure—Indicates the current session statistics of Radio connection status failure events.
- Availability after DDN Failure—Indicates the current session statistics of Availability after DDN Failure event configuration.
- UE Reachability and Idle status indication—Indicates the current session statistics of UE Reachability and Idle status indication event configurations.
-
- Availability after DDN Failure and Idle Status indication—Indicates the current session statistics of Availability after DDN Failure and Idle Status indication event configuration.
- PDN connectivity status—Indicates that the current session statistics of PDN connectivity status event configuration.

show mme-service statistics-monte

The output of this command includes the following fields:

Monitoring Report Config Rx Count

- Loss of connectivity—Indicates that the number of Loss of connectivity event configuration received.
- UE Reachability—Indicates that the number of UE reachability event configurations received
- Location Reporting—Indicates that the number of reporting location event configurations received.
- Communication Failure—Indicates that the number of Radio connection status failure events received.
- Availability after DDN Failure—Indicates that the number of Availability after DDN Failure event configuration received.
- Number of UE in a geographic area—Indicates the received Number of UEs present in a geographic area event configuration.
  - Progress—Indicates the number of 'Number of UE in a geographic area' events under progress.
  - Pending—Indicates the number of 'Number of UE in a geographic area' events queued.
  - Drop— Indicates the number of 'Number of UE in a geographic area' events dropped.
- Idle status indication—Indicates that the number of Idle status event configurations received.
- PDN connectivity status—Indicates that the PDN connectivity status event configuration received.

Monitoring Report Config Tx Count: The output includes the following fields:

- Loss of connectivity—Indicates the number of loss of connectivity reports sent.
- UE Reachability—Indicates the number of UE reachability reports sent.
- Location Reporting—Indicates that the number of Location reports sent.
- Communication Failure—Indicates that the number of communication failure reports sent.
- Availability after DDN Failure—Indicates that the number of Availability after DDN Failure reports sent.
- Number of UE in a geographic area—Indicates that the number of UE in a geographical area report responded.
  - Success—Indicates the number of Number of UE in a geographic area event success responses.
  - Failure—Indicates the number of Number of UE in a geographic area event failure responses.
  - Drops—Indicates the number of 'Number of UE in a geographic area' event responses dropped
- UE Reachability and idle status indication—Indicates that the number of UE Reachability and idle status indication report sent.
- Availability after DDN Failure and idle status indication—Indicates that the Availability after DDN Failure and idle status indication report sent.
- PDN connectivity status—Indicates that the number of PDN connectivity statuses report sent.

Monitoring Event Configuration Deleted Count: The output includes the following fields:

- Loss of connectivity—Indicates the number of deleted loss of connectivity monitoring events.
- UE Reachability—Indicates the number of deleted UE Reachability monitoring events.

- Location Reporting—Indicates the number of deleted location reporting monitoring events.
- Communication Failure—Indicates the number of deleted communication failure monitoring events.
- Availability after DDN Failure—Indicates number of deleted availability after DDN failure monitoring events.
- UE Reachability and idle status indication—Indicates the number of deleted UE reachability and idle status indication monitoring events.
- PDN connectivity status—Indicates the number of deleted pdn connectivity status monitoring events.
- ULA received without monte cfg—Indicates the number of deleted monitoring events configurations when ULA received with updated set of configurations.
- HSS update received with different scef ref id—Indicates the number of deleted monitoring events with HSS update received with different SCEF Reference Id.
- HSS update received with same scef ref id—Indicates the number of deleted monitoring events with HSS update received with same SCEF Reference Id.

Monitoring Event Roaming statistics: The output includes the following fields:

- CIR sent —Indicates the number of CIR messages sent for roaming subscribers.
- CIA received—Indicates the number of CIA message received from roaming subscribers.
- CIR timeout—Indicates the CIR timeout value if there is no response for the CIR messages sent.
- RIR sent—Indicates the number of RIR messages sent for roaming subscribers.
- CIR denied by IWK-SCEF—Indicates the number of CIR messages denied through IWK-SCEF.

show lte-policy monitoring-event-profile

Monitoring Event Profile mon

The output of this command includes the following fields:

- Loss of connectivity—Indicates the enabled events of Loss of connectivity event configuration.
- UE Reachability—Indicates the enabled events of UE Reachability event configurations.
- Location Reporting—Indicates the enabled events of reporting location event configurations.
- Communication Failure—Indicates the current session statistics of Radio connection status failure events.
- Availability after DDN Failure—Indicates the current session statistics of Availability after DDN Failure event configuration.
- Idle Status Indication Failure—Indicates the enabled events of Idle status indication event configurations.
- PDN Connectivity Status Report—Indicates that the enabled events of PDN connectivity status event configuration.
- Number Of UE's in Geo Area—Indicates the received Number of UEs present in a geographic area event configuration

- Roaming Support—Indicates whether roaming support is enabled or disabled for Interworking SCEF destination host or realm.

Bulk Statistics

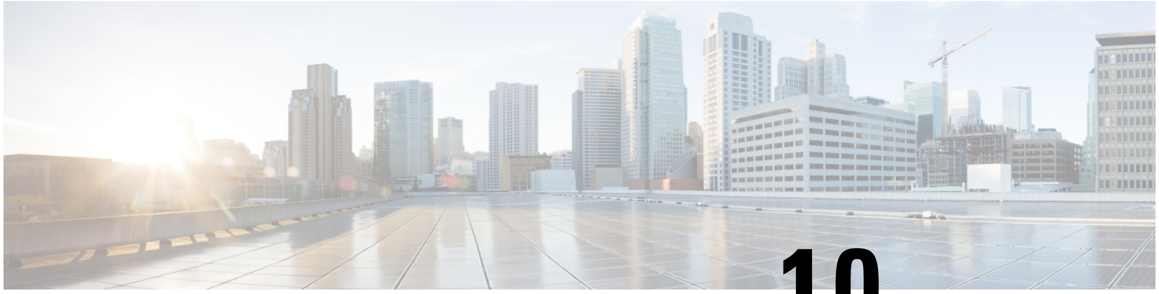
This section provides information on the bulk statistics for the Monitoring Events feature on MME.

MME Schema

The following bulk statistics are included in the MME Schema to track overall statistics:

Counters	Description
monitored-subscribers	The current total number of monitored subscribers for monitoring events.
monitored-loss-of-connectivity	The current total number of loss of connectivity events configured.
monitored-ue-reachability	The current total number of UE reachability events configured.
monitored-location-reporting	The current total number of location reporting events configured.
monitored-communication-failure	The current total number of communication failure events configured.
monitored-availability-after-ddn-failure	The current total number of availability after DDN failure events configured.
monitored-availability-after-ddn-failure-idleind	The current total number of availability after DDN failure and idle status indication events configured.
monitored-ue-reachability-idleind	The current total number of UE reachability and idle status indication events configured.
monitored-pdn-connecitivty-status	The current total number of PDN connectivity status events configured.
monte-rx-loss-of-connectivity	The total number of loss of connectivity monitoring events configured.
monte-rx-ue-reachability	The total number of UE reachability monitoring events configured.
monte-rx-location-reporting	The total number of location reporting monitoring events configured.
monte-rx-communication-failure	The total number of communication failure monitoring events configured.
monte-rx-availability-after-ddnfailure	The total number of availability after DDN failure monitoring events configured.
monte-rx-number-of-ue-geoarea	The total number of UEs present in a geographical area monitoring events configured.
monte-rx-uereachability-idleind	The total number of UE reachability and idle status indication monitoring events configured.

Counters	Description
monte-rx-availability-ddnfailure-idleind	The total number of availability after DDN failure and idle status indication monitoring events configured.
monte-rx-pdn-connectivity-status	The total number of PDN connectivity status monitoring events configured.
monte-tx-loss-of-connectivity	The total number of loss of connectivity monitoring reports sent.
monte-tx-ue-reachability	The total number of UE Reachability monitoring reports sent.
monte-tx-location-reporting	The total number of location reporting monitoring reports sent.
monte-tx-communication-failure	The total number of communication failure monitoring reports sent.
monte-tx-availability-after-ddnfailure	The total number of availability after DDN failure monitoring reports sent.
monte-tx-number-of-ue-geoarea	The total number of number of UEs present in a geographical area monitoring reports sent.
monte-tx-uereachability-idleind	The total number of UE reachability and idle status indication monitoring reports sent.
monte-tx-availability-ddnfailure-idleind	The total number of availability after DDN failure and idle status indication monitoring reports sent.
monte-tx-pdn-connectivity-status	The total number of PDN connectivity status monitoring reports sent.
monte-del-ue-reachability	The total number of deleted UE Reachability monitoring events.
monte-del-location-reporting	The total number of deleted location reporting monitoring events.
monte-del-communication-failure	The total number of deleted communication failure monitoring events.
monte-del-availability-after-ddn-failure	The total number of deleted availability after DDN failure monitoring events.
monte-del-uereachability-idleind	The total number of deleted UE reachability and idle status indication monitoring events.
monte-del-availability-ddnfailure-idleind	The total number of deleted availability after DDN failure and idle status indication monitoring events.
monte-del-pdn-connectivity-status	The total number of deleted PDN connectivity status monitoring events.
monte-del-loss-of-connectivity	The total number of deleted loss of connectivity monitoring events.



CHAPTER 10

HSS and AuC Interworking Configuration Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. This feature is fully qualified in this release.	21.20
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19
The maximum number of HSS Peer Services that can be created and configured has been increased from 64 to 96.	21.15
First introduced.	Pre 17.0

Feature Description

The maximum number of HSS Peer services that can be configured per MME chassis has been increased from 96 to 128.

Note

- In StarOS 21.15 and later releases, the maximum memory for diamproxy proclet allocated is increased by 250 MB. The increase is only for SCALE_LARGE platform (qvpc-di-large).
- The maximum number of configurable Diameter endpoint is limited to 96.
- This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.

CHAPTER 11

Ignoring SAI, RAI, or CGI in Change Notification Request Messages

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *S-GW Administration Guide* • *Command Line Interface Reference, Modes I - Q* • *Command Line Interface Reference, Modes R - Z* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
With this release, a new CLI **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** is added to control the RAI/SAI/CGI in Change Notification Request message for P-GW and S-GW services.	21.19.11

Feature Changes

Previous Behavior: P-GW and S-GW received RAI/SAI/CGI in the CHANGE NOTIFICATION REQUEST message under 4G CALL FLOW (RAT TYPE as EUTRAN), detected ULI changes, and generated ULI change CDRs based on the Change Notification Request message.

New Behavior: To ignore RAI/SAI/CGI under 4G CALL FLOW, a new CLI **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** is added to the P-GW and S-GW and its functions are.

- If the **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI is enabled under P-GW and S-GW services, then, detection of User Location Information (ULI) change and generation of ULI change CDR based on CHANGE NOTIFICATION REQUEST messages are ignored
- If this **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi**CLI is enabled either in P-GW or S-GW service or enabled in both the services, then, ULI IE containing any of SAI/CGI/RAI or its combination in Change notification request for RAT Type EUTRAN is ignored for that service type.

  For example, if the **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI is enabled only under S-GW service, then ULI IE is ignored only for S-GW. If the CLI is configured only under P-GW service, then ULI IE is ignored only for P-GW. This results in ULI change CDR not getting generated for such messages even if TAI/ECGI or its combination changes in same message

Note The **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI is applicable only for Change Notification Request message. Other 3GPP GTPV2 messages having ULI IE includes RAI/SAI/CGI and generates ULI change CDR based on RAI/SAI/CGI.

Command Changes

Note

- Enabling the **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI applies to GTPP CUSTOM dictionaries having secondary RAT usage reports in CDR. Dictionaries having secondary RAT usage reports are CUSTOM38,CUSTOM24 and CUSTOM44.
- CLI not mandatory if based on the requirement CUSTOMER can enable/disable the CLI.

To ignore RAI/SAI/CGI in the Change Notification Request messages for S-GW services, use the following configuration to enable or disable the **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI under **egtp** command mode.

```
configure
   context context_name
     sgw-service sgw-service_name
       [no | default] egtp change-notification-req rat-type eutran
ignore-uli-with-rai-sai-cgi
       Exit
```

To ignore RAI/SAI/CGI in the Change Notification Request message for P-GW services, use the following configuration to enable or disable the **egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** CLI under **egtp** command mode.

```
configure
   context context_name
     pgw-service pgw-service_name
      [no | default] egtp change-notification-req rat-type eutran
ignore-uli-with-rai-sai-cgi
      Exit
```

NOTES:

- **default egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi**: Applies the default value "false" to the CLI.

  The P-GW/S-GW detects ULI changes even RAI/SAI/CGI received in Change notification Request message under 4G call flow.

- **no egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi** : Disables the CLI, where P-GW/S-GW can detect ULI changes even RAI/CGI/SAI received in Change notification Request message under 4G call flow.

Performance Indicator Changes

show config

This command is modified to display the following output for sgw-service

```
sgw-service sgw-service
      associate ingress egtp-service sgw_ingress_egtp
      associate egress-proto gtp egress-context ingress egtp-service sgw_egress_egtp
      plmn id mcc 123 mnc 765 primary
      no reporting-action event-record
      egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi
```

This command is modified to display the following output for pgw-service

```
pgw-service pgw_service
      associate ggsn-service ggsn-service
      associate egtp-service egtp_service
      associate peer-map map_pgw
      egtp create-session-rsp apn-ambr-always-include
      egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi
```

show sgw service name

This command has been modified to display the following output

```
show sgw-service name sgw-svc
   EGTP Modify bearer cmd negotiate qos : Disabled
  EGTP GnGp Modify bearer res with APN-AMBR : Disabled
  EGTP Modify bearer res with CHARGING-ID   : Disabled
  EGTP Modify bearer res with CHARGING-FQDN or CHARGING-GW-ADDRESS : Disabled
  EGTP Modify bearer res with MSISDN        : Disabled
  EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch : Enabled

  EGTP Bearer Request with Context Not Found cause if ULI mismatch : Disabled
  EGTP Bit Rate in Rounded Down Kbps : Disabled
  EGTP Suppress Update Bearer Request (no bitrate change) : Disabled
  EGTP Create Session Response with APN-AMBR IE : Enabled
  EGTP Ignore ULI IE with SAI/RAI/CGI in Change Notification Req for EUTRAN: Disabled
```

show pgw service name

This command has been modified to display the following output

```
show pgw-service name pgw-svc
   EGTP Modify bearer cmd negotiate qos : Disabled
  EGTP GnGp Modify bearer res with APN-AMBR : Disabled
  EGTP Modify bearer res with CHARGING-ID   : Disabled
  EGTP Modify bearer res with CHARGING-FQDN or CHARGING-GW-ADDRESS : Disabled
  EGTP Modify bearer res with MSISDN        : Disabled
  EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch : Enabled

  EGTP Bearer Request with Context Not Found cause if ULI mismatch : Disabled
  EGTP Bit Rate in Rounded Down Kbps : Disabled
  EGTP Suppress Update Bearer Request (no bitrate change) : Disabled
  EGTP Create Session Response with APN-AMBR IE : Enabled
EGTP Ignore ULI IE with SAI/RAI/CGI in Change Notification Req for EUTRAN: Disabled
```

CHAPTER 12

Migrating 3G to 4G Context

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 - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

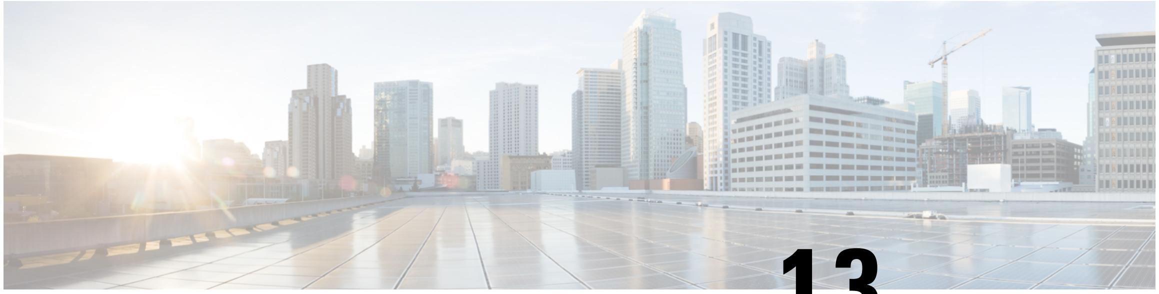
Revision History

Revision Details	Release
First Introduced	**21.15.51**

Feature Changes

Previous Behavior: When there is a low number of session manager the chance of existence of transaction record is high, when a new Modifiy bearer request comes in. During 3G to 4G Hand Over (HO), Modify Bearer Request is rejected due to context not found, even when active transmission is found and it is not a retransmitted message.

New Behavior: P-GW supports migrating the 3G context to 4G context even if an active transmission is found and it is not a retransmitted message.



CHAPTER 13

Non-IP Data Over SCEF

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* • *Ultra IoT C-SGN Administration Guide*

Revision History

Revision Details	Release
This release supports: • Connection Management by SCEF Procedure to release a T6a connection between MME and SCEF. • This release supports PDN disconnect and detach procedure towards the UE when it receives a MO Data Answer message with Permanent Failure from SCEF.	21.19
The feature is tested and qualified on the ASR 5500 platform. This release supports temporary buffering of single MT Data Request received from SCEF while UE is in idle mode.	21.3
First introduced.	N5.1 (21.1.V0)

Packet Data Network Disconnect or Detach Procedure

Before the implementation of Packet Data Network (PDN) Disconnect or Detach procedure in a network, MME followed the below process after receiving the permanent failure code:

1. The User Equipment (UE) connects to the network with Non-IP Data Delivery (NIDD) option and establishes T6a connection.
2. UE tries Mobile Originated (MO) NIDD whenever a Session DB on the SCEF gets cleared.
3. UE sends Non-Access Stratum (NAS) “MO REQUEST” with the data and receives NAS_SERVICE_ACCEPT.
4. The MME sends Diameter “MO-Data-Request” over T6A and receives “DIAMETER_ERROR_INVALID_EPS_BEARER (5651)” or “DIAMETER_ERROR_USER_UNKNOWN”.

However, there was data loss. This data loss was because of the lack of PDN Disconnect or Detach procedure initiation from MME towards the UE. UE may assume that it is T6a connected and retry MO NIDD indefinitely.

In StarOS 21.19 and later releases, the MME supports PDN Disconnect or Detach procedure towards the UE when it receives a MO Data Answer message with Permanent Failure Result-Code/Experimental-Result from SCEF. If the permanent failure is different from DIAMETER_ERROR_ INVALID_EPS_BEARER and from DIAMETER_ERROR_USER_UNKNOWN, then MME also initiates the "Connection Management by MME/SGSN" procedure to release the T6a connection between the MME and the SCEF.

How it Works

This section covers SCEF Initiated T6a Connection Release and Packet Data Network (PDN) Disconnect and Detach procedures.

Connection Release

MME allows Service Capability Exposure Function (SCEF) to initiate T6a connections release procedure in compliance with the 3GPP specifications 23.682 Release 15, Section 5.13.5.3 and 29.128 Release 15, Section 5.8.

Using one of the following procedures, the MME releases the T6a connection towards the SCEF(s) corresponding to the SCEF ID indicator for an APN:

- User Equipment (UE)-initiated Detach procedure for E-UTRAN
- MME-initiated Detach procedure
- HSS-initiated Detach procedure
- UE or MME requested PDN disconnection procedure.

In one of the following scenarios, the SCEF releases the T6a connection towards the MME corresponding to PDN connections:

- When an NIDD Authorization Update request from the HSS indicates that the user is no longer authorized for NIDD.
- Failure of SCEF or failure of SCS/AS connection
- Based on a request from the SCS/AS
- Based on removal of the APN associated with the T6a connection from the SCEF

SCEF Initiated T6a Connection Release Procedure

SCEF invokes Connection Management by SCEF procedure to release a T6a connection between MME and SCEF. This procedure is mapped to the commands Connection-Management-Request/Answer (CMR/CMA) in the Diameter application along with IEs.

The following table describes Connection Request management IE from SCEF.

Table 18: Connection Management SCEF Request

Information Element Name	Mapping to Diameter AVP	Category	Description
User Identity	User-Identifier	M	This information element contains the identity of the UE. This is a grouped AVP which contains the IMSI.
EPS Bearer Identity	Bearer-Identifier	M	This information element contains the identity of the EPS bearer, identifying the T6a connection to the applicable request.

Information Element Name	Mapping to Diameter AVP	Category	Description
T6a/b Connection Action	Connection Action	M	This information element contains T6a connection management action indicating a T6a connection establishment, a T6a connection release, or a T6a connection update.
Extended PCO	Extended- PCO	C	This information element contains Extended-Protocol Configuration Options (PCO), indicating that the SCEF needs to send updated extended PCO information (for example, APN Rate Control information) to the UE.
Supported Features	Supported-Features	O	Lists the features supported by the origin host.

SCEF sets the Connection-Action to CONNECTION_RELEASE (1) for a T6a Connection Release.

The following table describes SCEF Answer management from MME.

Table 19: Connection Management SCEF Answer

Information Element Name	Mapping to Diameter AVP	Category	Description
Result	Result-Code/Experimental-Result	M	This information element provides the result of the request. Result-Code AVP is used for errors defined in the Diameter Base Protocol. Experimental-Result AVP is used for T6a/b errors. This is a grouped AVP, which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Information Element Name	Mapping to Diameter AVP	Category	Description
Supported Features	Supported-Features	O	This information element contains the list of features supported by the origin host.

After MME receives the Connection Management Request with Connection-Action set to 1 in t6a interface, MME does the following.

Table 20: T6a Connection Release Procedure by SCEF

Step	Description
1	Checks if the User Identity exists in the MME. If the User Identity does not exist, sets the Experimental-Result to **DIAMETER_ERROR_USER_UNKNOWN** in the Connection Management SCEF Answer.
2	Checks whether the T6a connection action indicates a T6a connection update or T6a connection release. If the T6a connection acttion is not update or release, then sets the Experimental-Result to **DIAMETER_ERROR_OPERATION_NOT_ALLOWED** in the Connection Management SCEF Answer.
3	Checks whether a T6a connection context exists for a user and the received EPS Bearer Identity. If T6a conection context does not exist, then sets the Experimental-Result to **DIAMETER_ERROR_ INVALID_EPS_BEARER** in the Connection Management SCEF Answer.
4	If the T6a connection action indicates T6a connection release, delete the T6a connection context at the MME. If successful, sets the Result code to DIAMETER_SUCCESS in the Connection Management SCEF Answer.
5	The MME performs the MME initiated Detach procedure.

Initiating Packet Data Network Disconnect or Detach Procedure

MME triggers the PDN Disconnect or Detach procedure based on the following conditions:

- MME checks whether to trigger PDN Disconnect procedure or Detach procedure based on the PDN Count.
- If the last PDN and Attach without PDN connectivity is supported by UE, then MME triggers the PDN Disconnect procedure.
- If UE has more than one PDN, and UE sends MO Data Request procedure towards SCEF-specific PDN, and if MME receives MO Data answer with any permanent failure cause, MME triggers PDN disconnect procedure towards UE. MME initiates Connection release procedure towards SCEF except when the error is other than “DIAMETER_ERROR_USER_UNKNOW” and “DIAMETER_ERROR_INVALID_EPS_BEARER” .

- If UE has only one PDN and Attach without PDN is not supported, then MME triggers Detach procedure. If permanent failure is different than Diameter_Error_User_Unknown and Invalid EPS Bearer ID, MME initiates a Connection Management procedure to release the T6a connection.
- If UE has one PDN or more than one PDN and UE sends MO Data Request procedure towards SCEF-specific PDN, and if MME receives MO Data answer with failure cause as User-Unknown, MME triggers Detach procedure.

The following table describes error scenarios when MME initiates Detach/PDN disconnect towards UE and release of T6a connection towards SCEF .

Table 21: Detach/PDN disconnect Errors

DIAMETER_ERROR/No of PDNs	1 PDN & Attach without PDN Support by UE	>1 PDN	1 PDN & Attach without PDN not Support by UE
USER_UNKNOWN	Detach towards UE and no T6a Connection release towards SCEF	Detach towards UE and no T6a Connection release towards SCEF	Detach towards UE and no T6a Connection release towards SCEF
INVALID_EPS_BEARER	PDN Disconnect towards UE and no T6a Connection release towards SCEF	PDN Disconnect towards UE and no T6a Connection release towards SCEF	Detach towards UE and no T6a Connection release towards SCEF
OPERATION_NOT_ALLOWED	PDN Disconnect towards UE and T6a Connection release towards SCEF	PDN Disconnect towards UE and T6a Connection release towards SCEF	Detach towards UE and T6a Connection release towards SCEF
NIDD_CONFIGURATION_NOT_AVAILABLE	PDN Disconnect towards UE and T6a Connection release towards SCEF	PDN Disconnect towards UE and T6a Connection release towards SCEF	Detach towards UE and T6a Connection release towards SCEF

DIAMETER_ERROR/No of PDNs	1 PDN & Attach without PDN Support by UE	>1 PDN	1 PDN & Attach without PDN not Support by UE
SCEF_REFERENCE_ID_UNKNOWN	PDN Disconnect towards UE and T6a Connection release towards SCEF	PDN Disconnect towards UE and T6a Connection release towards SCEF	Detach towards UE and T6a Connection release towards SCEF

Monitoring and Troubleshooting

This section provides information regarding show commands of data over T6A (SCEF) statistics for this feature.

show mme-service statistics

The ESM procedure statistics counters are added for the following:

- Non-IP PDN Connections over SCEF (T6a)
- Non-IP PDN Disconnects over SCEF (T6a)

The statistics added are as follows:

```
ESM Statistics:
.
.
PDN Connections With PDN Type Override to ipv6:
   Attempted:          0   Success:         0
   Failures:           0
NON-IP PDN Connections With SCEF:
   Attempted:          0   Success:         0
   Failures:           0
NON-IP PDN Connections With SGI:
   Attempted:          0   Success:         0
   Failures:           0
PDN Disconnections With SCEF:
   Attempted:          0   Success:         0
   Failures:           0
```

For PDN statistics, the following is displayed:

```
.
.
PDN Statistics:
  All PDNs:            0   Connected PDNs:      0
  Idle PDNs:           0
NON-IP PDN Statistics:
...
...
```

```
Data Over T6A (SCEF) Statistics:
   Rx Packets:         0   Rx Bytes:            0
   Tx Packets:         4   Tx Bytes:            84
   Rx Drop Packets:    0   Rx Drop Bytes:       0
   Tx Drop Packets:    0   Tx Drop Bytes:       0
```

show mme-service statistics monte

Following statistics are displayed for Monitoring events in MME:

```
Session Statistics:
Monitoring Events Statistics:
     Current number of UEs being monitored:             0

     Current number of reports configured:
     Loss of connectivity                                        :            0
     UE Reachability                                             :            0
     Location Reporting                                          :            0
     Communication Failure                                       :            0
     Availability after DDN Failure                              :            0
     UE Reachability and idle status indication                  :            0
     Availability after DDN Failure and idle status indication   :            0
     PDN connectivity status                                     :            0
Monitoring Events Statistics:

Monitoring Report Config Rx Count:
  Loss of connectivity                                        :            0
  UE Reachability                                             :            0
  Location Reporting                                          :            0
  Communication Failure                                       :            0
  Availability after DDN Failure                              :            0
   UE Reachability and idle status indication                  :            0
  Availability after DDN Failure and idle status indication   :            0
  PDN connectivity status                                     :            0

Monitoring Reports Tx Count:
  Loss of connectivity                                        :            0
  UE Reachability                                             :            0
  Location Reporting                                          :            0
  Communication Failure                                       :            0
  Availability after DDN Failure                              :            0
    UE Reachability and idle status indication                  :            0
  Availability after DDN Failure and idle status indication   :            0
```

show bulkstats variables mme | grep moni

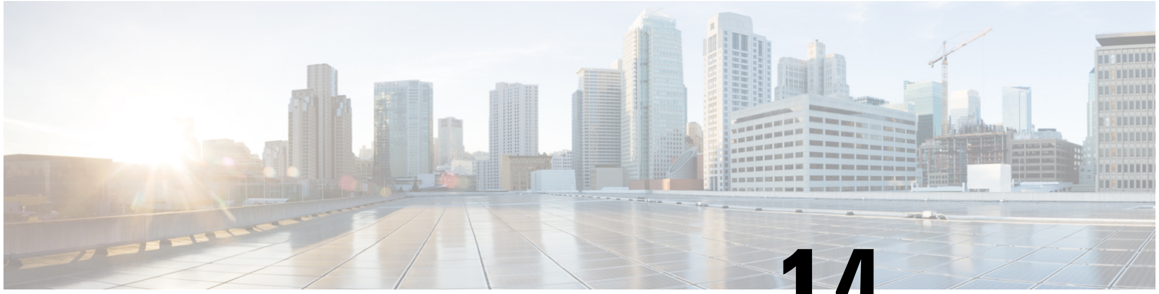
On running the above command, the following session statistics is displayed:

```
%monitored-subscribers%                                     Int32     0   Gauge
         %monitored-loss-of-connectivity%                             Int32     0   Gauge
         %monitored-ue-reachability%                                  Int32     0   Gauge
         %monitored-location-reporting%                               Int32     0   Gauge
         %monitored-communication-failure%                            Int32     0   Gauge
         monitored-availability-after-ddn-failure%                    Int32     0   Gauge
         monitored-number-of-ue-geoarea%                              Int32     0   Gauge
         %monitored-uereachability-idleind%                            Int32     0   Gauge
         %monitored-availability-after-ddn-failure-idleind%            Int32     0   Gauge
         %monitored-pdn-connecitivty-status%                           Int32     0   Gauge
```

show bulkstats variables mme | grep monte

On running the above command , the following overall statistics is displayed:

```
%mme-monte-rx-loss-of-cnnectivity%                            Int32     0   Counter
%mme-monte-rx-ue-reachability%                                Int32     0   Counter
 %mme-monte-rx-location-reporting%                             Int32     0   Counter
 %mme-monte-rx-communication-failure%                          Int32     0   Counter
%mme-monte-rx-availability-after-ddnfailure%                  Int32     0   Counter
%mme-monte-rx-number-of-ue-geoarea%                           Int32     0   Counter
%mme-monte-rx-uereachability-idleind%                         Int32     0   Counter
%mme-monte-rx-availability-ddnfailure-idleind%                Int32     0   Counter
%mme-monte-rx-pdn-connectivity-status%                        Int32     0   Counter
 %mme-monte-tx-loss-of-connectivity%                           Int32     0   Counter
%mme-monte-tx-ue-reachability%                                Int32     0   Counter
%mme-monte-tx-location-reporting%                             Int32     0   Counter
%mme-monte-tx-communication-failure%                          Int32     0   Counter
 %mme-monte-tx-availability-ddn-failure%                       Int32     0   Counter
%mme-monte-tx-number-of-ue-geoarea%                           Int32     0   Counter
 %mme-monte-tx-uereachability-idleind%                         Int32     0   Counter
%mme-monte-tx-availability-ddnfailure-idleind%                Int32     0   Counter
%mme-monte-tx-pdn-connectivity-status%                        Int32     0   Counter
[
```



CHAPTER 14

NR UE Security Capability IE for 5G Security Support on MME

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 - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	**Release**
This feature is fully qualified for this release.	21.14.19

Revision Details	Release
First Introduced. **Note** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19

Feature Changes

Previous Behavior:

- When MME receives UE Additional Security Capability from Attach/TAU, MME parses the UE Additional Security Capability and replays the same in the Security Mode command.
- MME includes or sends the NR UE Security Capability IE over S1AP interface as part of the following messages:
    - INITIAL-CONTEXT-SETUP-REQUEST
    - PATH-SWITCH-REQ-ACK

      If MME receives *NR UE Security Capability* in PATH SWITCH REQUEST from eNodeB, it uses the same in PATH SWITCH ACK else, it uses by parsing the *UE Additional Security Capability* received in Attach/TAU request such as, UE-CONTEXT-MODIFICATION-REQUEST, HANDOVER-REQUEST, DOWNLINK-NAS-TRANSPORT.

      .
- MME includes the *UE Additional Security Capability IE* over S10 interface as part of the following messages:
    - FORWARD RELOCATION REQUEST
    - CONTEXT RESPONSE
    - IDENTIFICATION RESPONSE

New Behavior: After configuring the CLI as **no nr-ue-security-capability-ie**

- MME ignores the *UE Additional Security Capability* IE received in Attach/TAU request.
- MME does not include *Replayed UE Additional Security Capability* in the Security Mode command.
- MME does not include *NR UE Security Capability* over S1AP interface as part of following messages:
    - Initial Context Setup Request
    - MME ignores *NR UE Security Capability* IE received in PATH SWITCH REQUEST from eNodeB and also thereby won't include in PATH SWITCH ACK
    - Downlink NAS messages
    - UE Context Modification Request
    - S1 Handover Request

- MME does not include *UE Additional Security Capability* in MM Context over S10 interface as part of following messages:
  - Forward Relocation Request
  - EGTP Context Response for the Context Received from another MME
  - Identification Response

Command Changes

NR UE Security Capability IE

Use the following configuration to configure NR UE Security Capability IE in messages over S1AP and S10 Interfaces to the peer.

```
configure
   context context_name
      mme-service nr-ue-security-capability-ie service_name
         [ no ] nr-ue-security-capability-ie
         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 must be a string 1–63 characters.
- **nr-ue-security-capability-ie**: Configures NR UE Security Capability IE for MME service users.
- **no**: Disables CLI **NR UE Security Capability IE** in an MME Service.

CHAPTER 15

N26 Interface Support

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**
The N26 interface for interworking with 5GS functionality is fully qualified in this release.	21.20.3

Revision Details	Release
MME supports N26 interface between AMF in 5GC and MME in Evoloved Packet Core (EPC) to provide seamless session continuity for single registration mode UE. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20
First introduced. This release supports N26 Interface for interworking with 5GS functionality. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.19

Feature Description

MME supports 5GS interworking with N26 interface in compliance with 3GPP 5GS standards. Interworking procedures using the N26 interface, enables the exchange of Mobilty Management (MM) and Session Management (SM) states between the source and target network.

With the 5GS interworking with N26 interface, the User Equipment (UE) operates in single-registration mode. MME supports N26 interface between Access and Mobility Management Function (AMF) in 5GC and MME in EPC to provide seamless session continuity (for example, for voice services) for single registration mode UE. For the 3GPP access, the network keeps only one valid MM state for the UE either in the AMF or Mobility Management Entity (MME).

MME supports the following Interworking procedures with N26 interface:

- Attach procedure
- EPS to 5GS Mobility Registration procedure
- 5GS to EPS Idle mode mobility procedure
- 5GS to EPS Handover
- EPS to 5GS Handover
- 5GS to EPS Handover Cancel
- EPS to 5GS Handover Cancel

Supported IEs and AVPs

MME supports the following IEs for this N26 interface with interworking 5Gs feature:

S1AP (eNodeB) Interface

- **GUMMEI Type**–The S1-AP interface supports **mappedFrom5G** in the Globally Unique Mobility Management Entity Identifier (GUMMEI) type IE. If the UE was previously registered in 5GS, the UE provides in Access Stratum signalling a GUMMEI mapped from the 5G-GUTI and in additional indicates as **Mapped from 5G-GUTI**.

- **Handover Type**–This Handover type IE indicates, which kind of handover was triggered in the source side. The Handover type IE currently supports **EPSto5GS** and 5GStoEPS type.
- **Handover Restriction List**–The Handover Restriction list IE is enhanced to support **Core Network Type Restrictions**, **NR Restriction in 5GS** and **Last NG-RAN PLMN Identity**.

Note MME currently includes only one serving PLMN in Core Network Restrictions Type IE.

- **Target ID**–The Target ID IE is enhanced to support **Global RAN Node ID** and **Selected TAI(5GS TAI)**.

Note Global ng-eNB under Global RAN Node ID is currently not supported.

NAS (UE) Interface

- **UE Network Capability (N1-mode)** – MME supports N1-mode handling in UE Network Capability IE. For UE that supports N1 mode, the UE sets the N1 mode bit to **N1 mode supported** in the UE network capability IE of the ATTACH REQUEST/TRACKING AREA UPDATE REQUEST message.
- **UE Status IE** – MME supports UE Status IE in the ATTACH REQUEST/TRACKING AREA UPDATE REQUEST message and provides the network with information related to the current UE registration status that is used for interworking with 5GS.
- **EPS Network Feature Support (IWK N26)** – MME supports IWK N26 indicator to specify whether interworking without N26 interface is supported or not in ATTACH ACCEPT/TAU ACCEPT message.

S6a (HSS) Interface

- **Interworking-5GS-Indicator AVP** – MME supports **Interworking-5GS-Indicator** to indicate whether the interworking between 5GS and EPS is subscribed or not subscribed for the APN.
- **Core-Network-Restrictions AVP** – MME supports **Core-Network-Restrictions** AVP to indicate the types of Core Network that are disallowed for a user.
- **Access-Restriction-Data AVP** – MME supports bit 10 **NR in 5GS Not Allowed** to check whether NR is 5GS is Allowed or Not Allowed. The Access-Restriction-Data AVP is of type Unsigned32 and contains a bit mask where each bit when set to 1 indicates a restriction.

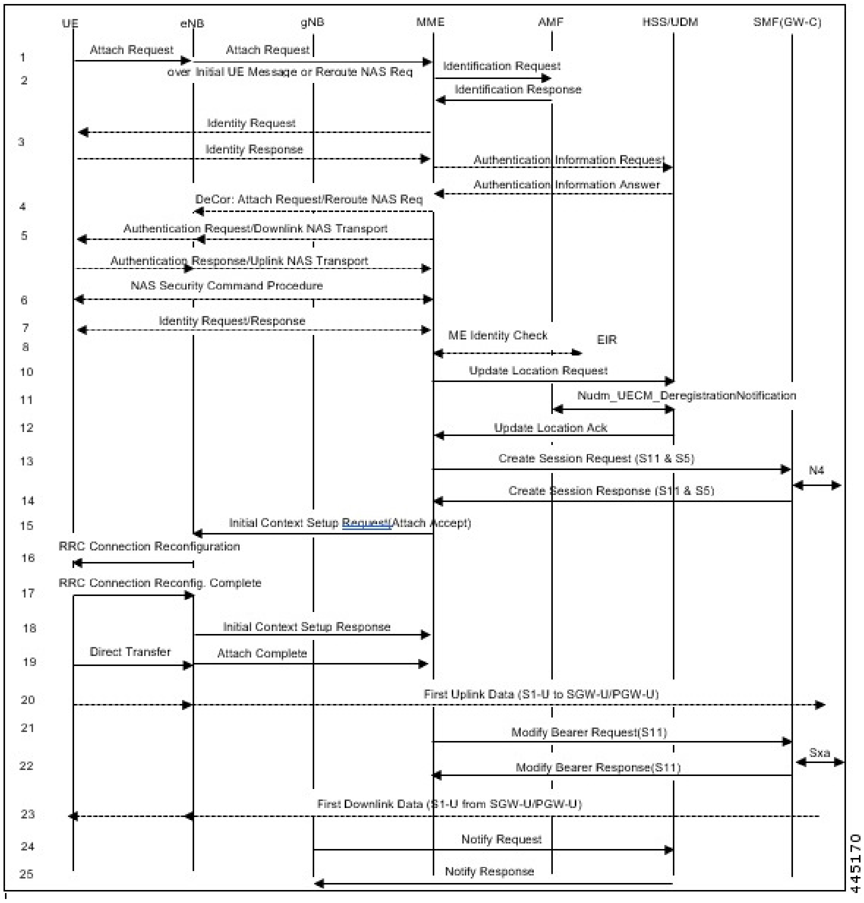
S11 (SGW) Interface

- **Indication Flag** – MME supports 5GSIWKI (5GS Interworking Indication) and REPREFI (Return Preferred Indication) flags.

How it Works

This section describes the call flow procedures related to 5GS interworking with N26 interface : The following call flow describes the working of 5Gs to EPS attach procedure.

Figure 9: E-UTRAN Initial Attach Call Flow


UE
eNB
gNB
MME
AMF
HSS/UDM
SMF(GW-C)
1
Attach Request
Attach Request
over Initial UE Message or Reroute NAS Req
2
Identification Request
Identification Response
Identity Request
3
Identity Response
Authentication Information Request
Authentication Information Answer
4
DeCor: Attach Request/Reroute NAS Req
5
Authentication Request/Downlink NAS Transport
Authentication Response/Uplink NAS Transport
NAS Security Command Procedure
6
7
Identity Request/Response
8
ME Identity Check
EIR
10
Update Location Request
11
Nudm_UECM_DeregistrationNotification
12
Update Location Ack
13
Create Session Request (S11 & S5)
N4
14
Create Session Response (S11 & S5)
15
Initial Context Setup Request(Attach Accept)
RRC Connection Reconfiguration
16
RRC Connection Reconfig. Complete
17
18
Initial Context Setup Response
19
Direct Transfer
Attach Complete
20
First Uplink Data (S1-U to SGW-U/PGW-U)
21
Modify Bearer Request(S11)
Sxa
22
Modify Bearer Response(S11)
23
First Downlink Data (S1-U from SGW-U/PGW-U)
24
Notify Request
25
Notify Response
445170

E-UTRAN Initial Attach Procedure

The following table describes 5GS to EPS attach procedure.

Table 22:

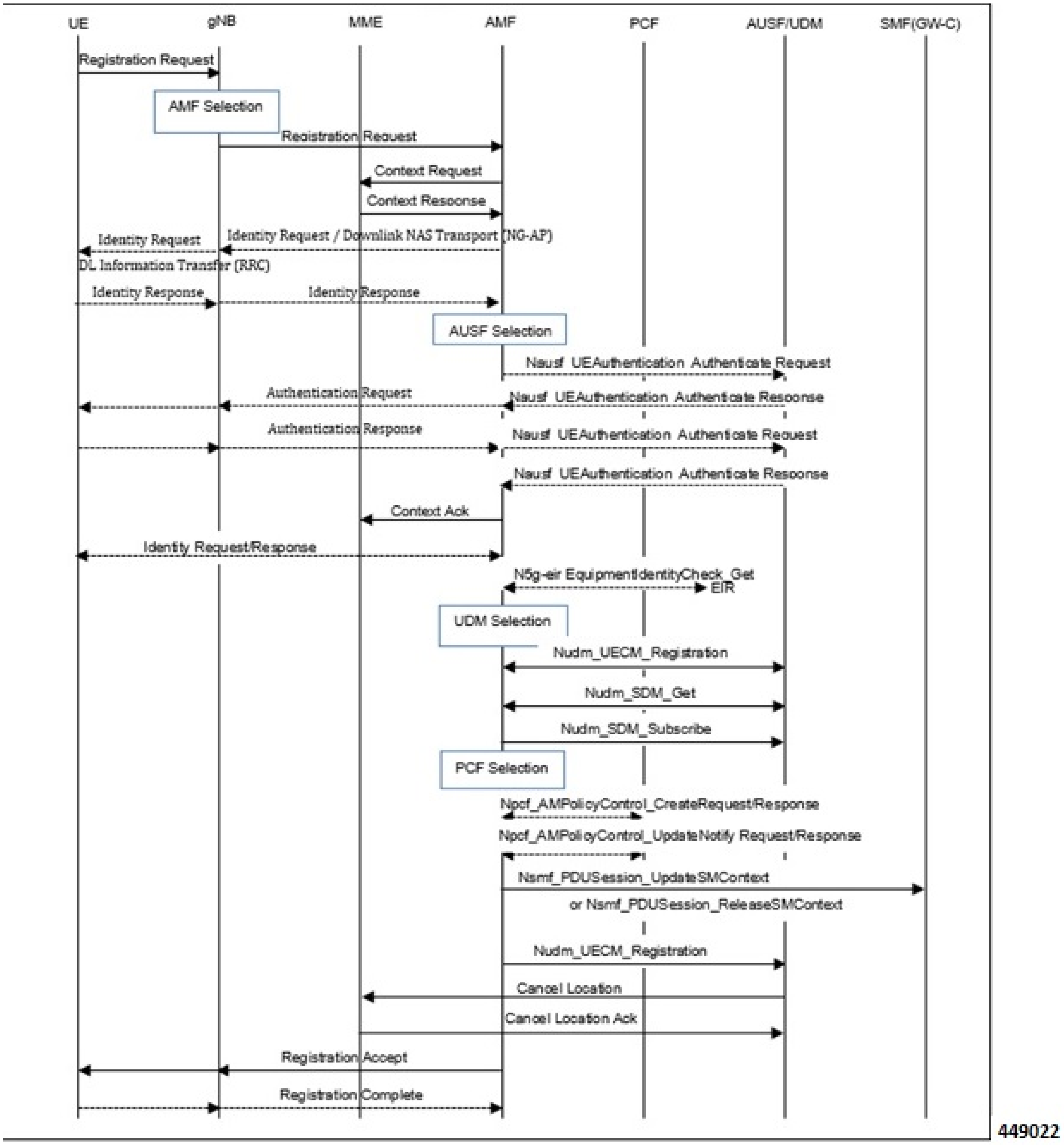
Step	Description
1	Attach Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability IE**. • UE includes GUMMEI in the S1-AP message and. indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped from 5G-GUTI into the EPS mobile identity IE, includes old GUTI type IE with GUTI type set to **native GUTI** and includes the UE status IE with a 5GMM registration status set to **UE is in 5GMM-DEREGISTERED state**.

Step	Description
2	MME construct the 5G-GUTI from the received GUTI IE according to the mapping relationship between GUTI and 5G-GUTI defined in 3GPP TS 23.003. MME uses the constructed 5G GUTI to determine the peer AMF address based on local Static Peer AMF GUAMI configuration. If MME is unable to find the peer AMF address, the new MME sends an Identity Request to the UE to request the IMSI. The UE responds with Identity Response (IMSI).
3	MME sends Identification Request message to the selected peer AMF. .
4	AMF responds with Identification Response message **Note** MME sends Identification Request to the peer AMF irrespective of the "n1-mode" configuration in CC profile (or) MME Service and the feature support check is performed after receiving "Identification Response” message from peer AMF. If the feature support is disabled (or) the UE is unknown in the old AMF, MME initiates Identity procedure with UE.
5	MME sends Update Location Request to HSS and will not set the Dual-registration 5G-indication in ULR-Flag.
6	MME processes and handles the below AVP in the ULA from HSS. MME uses the received information for Mobility restrictions and PGW-C+SMF gateway selection: • Interworking-5GS-Indicator • Core-Network-Restriction • Access-Restriction-Data (NR in 5GS Not Allowed) AVP
7	MME selects PGW-C+SMF based on UE Network capability and mobility restrictions.
8	MME sets the **5GS Interworking Indication** in Indication flags in the Create Session Request and sends to the selected P-GW-C+SMF gateway. MME does not set the Indication bit if Standalone P-GW-C is selected.
9	If the MME receives ePCO from the UE during the Initial Attach or UE requested PDN Connectivity procedures, the MME forwards the ePCO IE to the SGW, if the MME supports ePCO. The SGW shall also forward it to the PGW if the SGW supports ePCO.
10	If UE supports N1 mode in UE network capability, and the Interworking-5GS-Indicator is set to subscribed, MME sets IWKN26 bit to **Interworking without N26 interface not supported** in the Attach Accept message.

EPS to 5GS Mobility Registration Call Flow

The following call flow describes the registration procedure from EPS to 5GS Mobility when, N26 interface is supported for idle and connected states.

Figure 10: EPS to 5GS Mobility Registration using N26 interface


UE
gNB
MME
AMF
PCF
AUSF/UDM
SMF(GW-C)
Registration Request
AMF Selection
Registration Request
Context Request
Context Response
Identity Request
Identity Request / Downlink NAS Transport (NG-AP)
DL Information Transfer (RRC)
Identity Response
Identity Response
AUSF Selection
Nausf UEAuthentication Authenticate Request
Authentication Request
Nausf UEAuthentication Authenticate Response
Authentication Response
Nausf UEAuthentication Authenticate Request
Nausf UEAuthentication Authenticate Response
Context Ack
Identity Request/Response
N5g-eir EquipmentIdentityCheck_Get
EIR
UDM Selection
Nudm_UECM_Registration
Nudm_SDM_Get
Nudm_SDM_Subscribe
PCF Selection
Npcf_AMPolicyControl_CreateRequest/Response
Npcf_AMPolicyControl_UpdateNotify Request/Response
Nsmf_PDUSession_UpdateSMContext
or Nsmf_PDUSession_ReleaseSMContext
Nudm_UECM_Registration
Cancel Location
Cancel Location Ack
Registration Accept
Registration Complete
449022

The following table describes the procedure to register from EPS to 5GS.

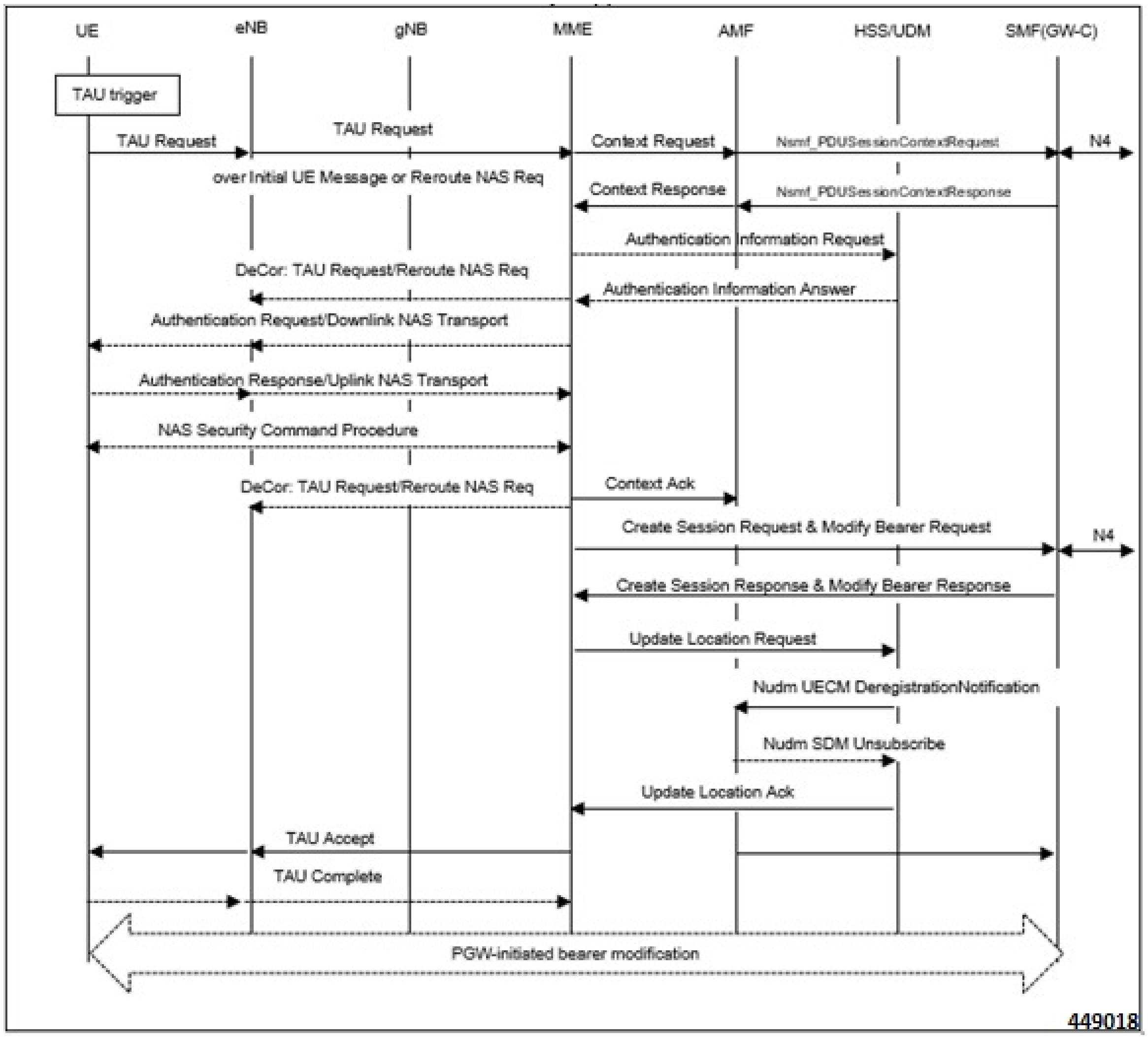
Table 23: EPS to 5GS Mobility Registration Procedure

Step	Description
1	For IDLE mode mobility, the target AMF derives the MME address and 4G GUTI from the old 5G-GUTI and sends Context Request to MME including EPS GUTI mapped from 5G-GUTI and the TAU request message according to TS 23.401. The MME validates the TAU message. **Note** • MME supports FTEID Interface types **S10/N26 MME GTP-C interface (12)** and **N26 AMF GTP-C interface (40)** received in the **Context Request** message from peer AMF. • MME would use the RAT type NR in the **Context Request** message to determine if the peer is AMF.
2	MME includes EPS MM Context, IMSI, ME Identity, UE EPS security context, UE Network Capability, and EPS Bearer context(s) in the Context Response message and sends to the peer AMF. The MME EPS Bearer context includes for each EPS PDN connection the IP address and FQDN for the S5/S8 interface of the PGW-C+SMF and APN. MME also includes in the Context Response new information Return Preferred. Return Preferred is an indication by the MME of a preferred return of the UE to the last used EPS PLMN at a later access change to an EPS shared network. Based on the Return Preferred indication, the AMF stores the last used EPS PLMN ID in UE Context. MME sends Context Response failure if feature support is disabled, Unknown RAT type other than NR is received (or) mobility is restricted.
3	The target AMF sends Context Acknowledge (Serving GW change indication) to MME.
4	HSS+UDM cancels the location of the UE in the MME.

5GS to EPS Idle Mode Mobility Call Flow

The following call flow describes the idle and connected states.

Figure 11:


UE
eNB
gNB
MME
AMF
HSS/UDM
SMF(GW-C)
TAU trigger
TAU Request
TAU Request
over Initial UE Message or Reroute NAS Req
Context Request
Nsmf_PDUSessionContextRequest
N4
Context Response
Nsmf_PDUSessionContextResponse
Authentication Information Request
DeCor: TAU Request/Reroute NAS Req
Authentication Information Answer
Authentication Request/Downlink NAS Transport
Authentication Response/Uplink NAS Transport
NAS Security Command Procedure
DeCor: TAU Request/Reroute NAS Req
Context Ack
Create Session Request & Modify Bearer Request
N4
Create Session Response & Modify Bearer Response
Update Location Request
Nudm UECM DeregistrationNotification
Nudm SDM Unsubscribe
Update Location Ack
TAU Accept
TAU Complete
PGW-initiated bearer modification
449018

UE performs Tracking Area Update (TAU) procedure in E-UTRA/EPS when it moves from NG-RAN/5GS to E-UTRAN/EPS coverage area. The procedure involves a Tracking Area Update to EPC and setup of default EPS bearer and dedicated bearers in EPC and re-activation, if required.

Table 24: 5GS to EPS Idle Mode Mobility Procedure

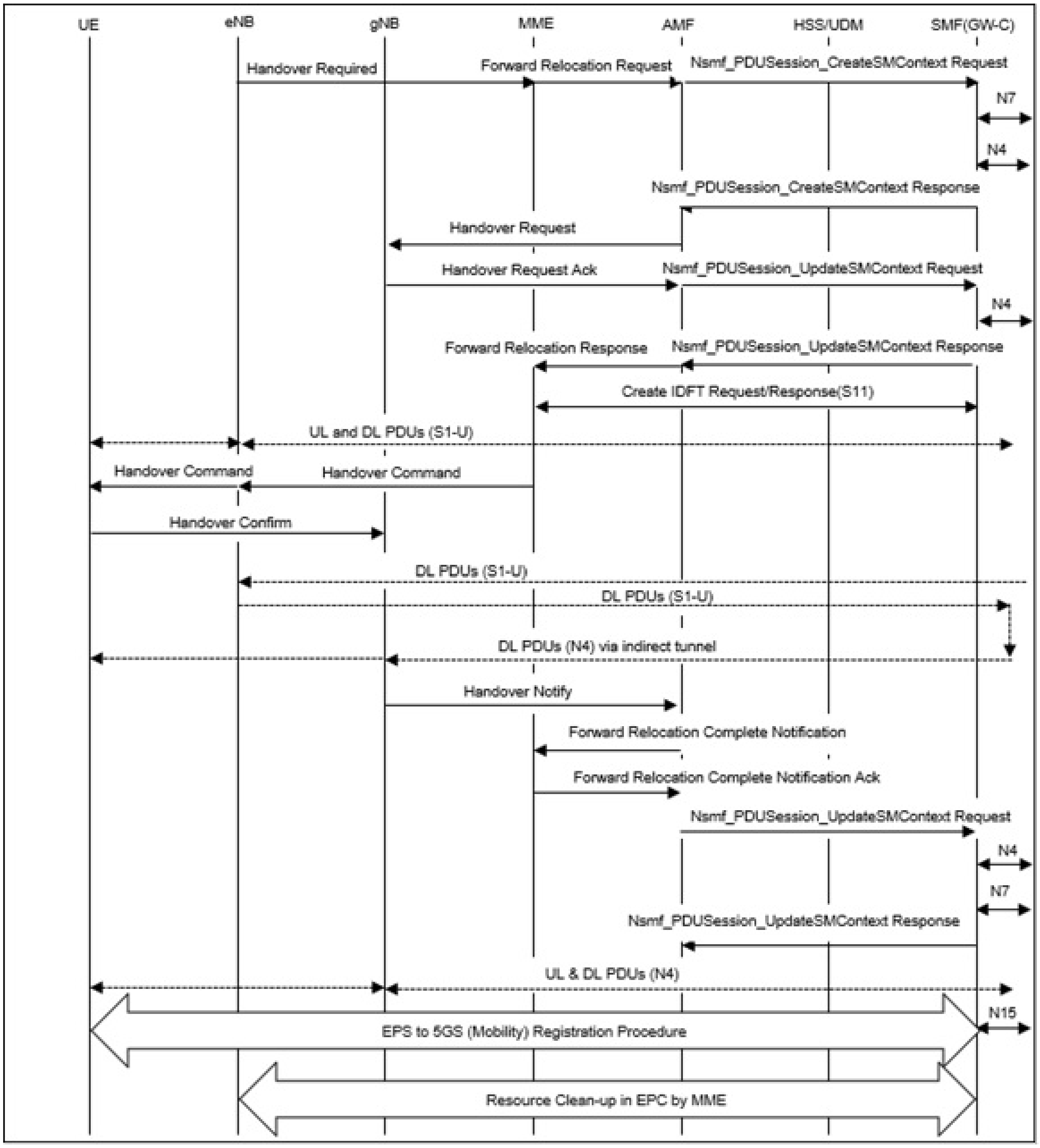
Step	Description
1	Tracking Area Update Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability** IE. • UE includes GUMMEI in the S1-AP message and indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped from 5G-GUTI into the EPS mobile identity IE, includes old GUTI type IE with GUTI type set to **native GUTI** and includes the UE status IE with 5GMM registration status set to **UE is in 5GMM-REGISTERED** state.

Step	Description
2	MME constructs the 5G-GUTI from the received GUTI IE according to the mapping relationship between GUTI and 5G-GUTI defined in 3GPP TS 23.003. MME uses the constructed 5G GUTI to determine the peer AMF address based on local Static Peer AMF GUAMI configuration. If MME is unable to find the peer AMF address, the new MME rejects the TAU Request.
3	MME sends Context Request message to the selected peer AMF.
4	The AMF responds with a Context Response message carrying mapped MM context (including mapped security context), UUT, Return preferred and SM EPS UE Context (default and dedicated GBR bearers) to the MME. If the verification of the integrity protection fails, the AMF returns an appropriate error cause. Return preferred is an optional indication by the AMF of a preferred return of the UE to the 5GS PLMN at a later access change to a 5GS shared network. The PDN GW Address and TEID(s) is part of the EPS Bearer Context for PDN connection in Context Response. However, SGW S11 IP address and TEID for Control Plane is not provided by AMF. **Note** . • MME supports **S10/N26 MME GTP-C** and **N26 AMF GTP-C** FTEID Interface types from peer AMF. • MME sends Context Request to the peer AMF irrespective of the **n1 mode** configuration in CC profile (or) MME Service and the feature support check is performed after receiving **Contect Response** message from peer AMF. If the feature support is disabled, MME rejects the TAU Request and sends the Context Acknowledgement failure.
5	MME selects new SGW-C and send Create Session Request towards the SGW. MME will set the **5GS Interworking Indication** in Indication Flags in the Create Session Request message.
6	MME sends Update Location Request to HSS and will not set the Dual-registration 5G-indication in ULR-Flag.
7	MME processes and handles the following AVPs in the ULA from HSS. • Interworking-5GS-Indicator • Core-Network-Restriction • Access-Restriction-Data (NR in 5GS Not Allowed) AVP. MME uses the received information for Mobility restrictions and PGW-C+SMF gateway selection.
8	If UE supports N1 mode in UE network capability, and the Interworking-5GS-Indicator is set to subscribed, MME shall set IWKN26 bit to “Interworking without N26 interface not supported” in TAU Accept.

EPS to 5GS Handover Call Flow

The following call flow describes the EPS to 5GS handover using N26 interface.

Figure 12:


UE
eNB
gNB
MME
AMF
HSS/UDM
SMF(GW-C)
Handover Required
Forward Relocation Request
Nsmf_PDUSession_CreateSMContext Request
N7
N4
Nsmf_PDUSession_CreateSMContext Response
Handover Request
Handover Request Ack
Nsmf_PDUSession_UpdateSMContext Request
N4
Forward Relocation Response
Nsmf_PDUSession_UpdateSMContext Response
Create IDFT Request/Response(S11)
UL and DL PDUs (S1-U)
Handover Command
Handover Command
Handover Confirm
DL PDUs (S1-U)
DL PDUs (S1-U)
DL PDUs (N4) via indirect tunnel
Handover Notify
Forward Relocation Complete Notification
Forward Relocation Complete Notification Ack
Nsmf_PDUSession_UpdateSMContext Request
N4
N7
Nsmf_PDUSession_UpdateSMContext Response
UL & DL PDUs (N4)
N15
EPS to 5GS (Mobility) Registration Procedure
Resource Clean-up in EPC by MME

The following table describes the handover procedure from EPS to 5GS using N26 interface. 5GS Mobility Registration Procedure is performed, and steps from Context Request to Context Acknowledgement are skipped during the handover to 5GS.

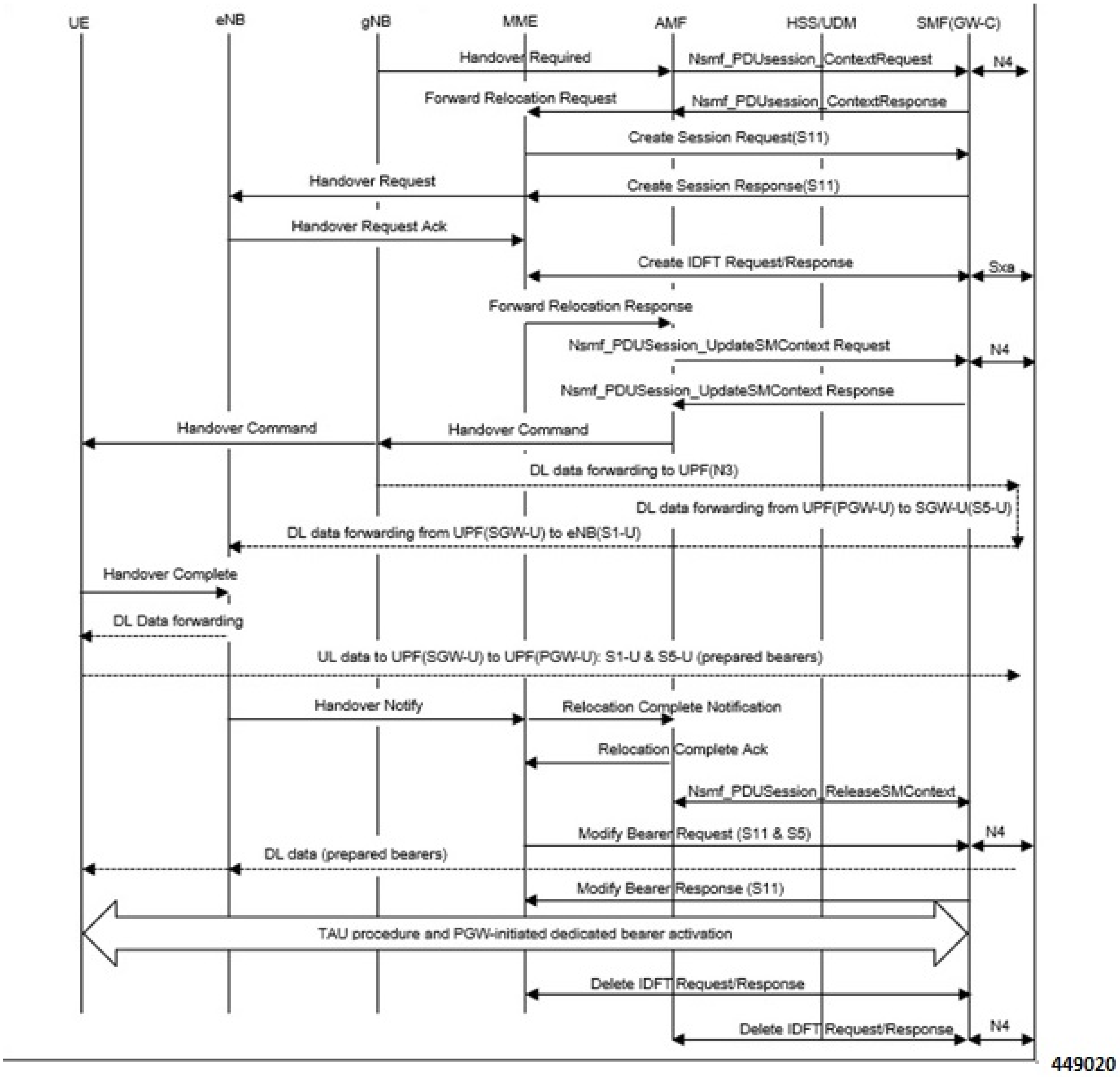
Table 25: EPS to 5GS Handover Procedure

Step	Description
1	MME receives Handover Required from eNB with the Handover type set **EPSto5GS**, Target ID with Global gNB ID and selected 5GS TAI information. **Note** Global ng-eNB is currently not supported.
2	MME uses the 5GS TAI information to determine the peer AMF address based on local Static Peer AMF TAI configuration. If MME is unable to find the peer AMF address or the feature is disabled, MME sends Handover preparation failure to eNB.
3	MME sends Forward Relocation Request message to the selected peer AMF with the following information: • MME includes EPS MM Context, IMSI, ME Identity, UE security context, UE Network Capability, and EPS Bearer context(s) in the Forward Relocation Request message. The MME EPS Bearer context(s) includes for each EPS PDN connection the IP address and FQDN for the S5/S8 interface of the PGW-C+SMF and APN, and for each EPS bearer the IP address and CN Tunnel Info at the UPF+PGW-U for uplink traffic. • MME includes an additional optional parameter Return preferred; Return preferred is an optional indication provided by the MME to indicate a preferred return of the UE to the last used EPS PLMN at a later access change to an EPS shared network. Based on the Return Preferred indication, the AMF stores the last used EPS PLMN ID in the UE Context.
4	MME receives Forward Relocation Response (Cause, Target to Source Transparent Container, S-GW change indication, CN Tunnel Info for data forwarding, EPS Bearer Setup List, AMF Tunnel Endpoint Identifier for Control Plane, Addresses and TEIDs) from AMF. The EPS Bearer Setup list is the combination of EPS Bearer Setup list from different P-GW-C+SMF(s). **Note** MME supports **S10/N26 MME GTP-C** and **N26 AMF GTP-C** FTEID Interface types from peer AMF.
5	The source MME sends Create Indirect Data Forwarding Tunnel Request (addresses and TEIDs for forwarding) to the S-GW. If the S-GW is relocated it includes the tunnel identifier to the target S-GW. The S-GW responds with a Create Indirect Data Forwarding Tunnel Response (S-GW addresses and TEIDs for forwarding) message to the source MME.
6	The source MME sends a Handover Command (Target to Source transparent container, Bearers subject to forwarding, Bearers to Release) message to the source eNodeB. The Bearers subject to forwarding includes list of addresses and TEIDs allocated for forwarding. The Bearers to Release includes the list of bearers to be released.
7	The NG-RAN notifies the AMF that UE is handover over to NG-RAN and AMF sends Forward Relocation Complete Notification message to the source MME. The source MME in response sends a Forward Relocation Complete Acknowledge message to the target AMF.

5GS to EPS Handover Call Flow

The following call flow describes the 5GS to EPS handover using N26 interface.

Figure 13:


UE
eNB
gNB
MME
AMF
HSS/UDM
SMF(GW-C)
Handover Required
Nsmf_PDUsession_ContextRequest
N4
Forward Relocation Request
Nsmf_PDUsession_ContextResponse
Create Session Request(S11)
Handover Request
Create Session Response(S11)
Handover Request Ack
Create IDFT Request/Response
Sxa
Forward Relocation Response
Nsmf_PDUSession_UpdateSMContext Request
N4
Nsmf_PDUSession_UpdateSMContext Response
Handover Command
Handover Command
DL data forwarding to UPF(N3)
DL data forwarding from UPF(PGW-U) to SGW-U(S5-U)
DL data forwarding from UPF(SGW-U) to eNB(S1-U)
Handover Complete
DL Data forwarding
UL data to UPF(SGW-U) to UPF(PGW-U): S1-U & S5-U (prepared bearers)
Handover Notify
Relocation Complete Notification
Relocation Complete Ack
Nsmf_PDUSession_ReleaseSMContext
Modify Bearer Request (S11 & S5)
N4
DL data (prepared bearers)
Modify Bearer Response (S11)
TAU procedure and PGW-initiated dedicated bearer activation
Delete IDFT Request/Response
Delete IDFT Request/Response
N4
449020

The following table describes the handover procedure from 5GS to EPS using N26 interface.

Table 26: 5GS to EPS Handover Procedure

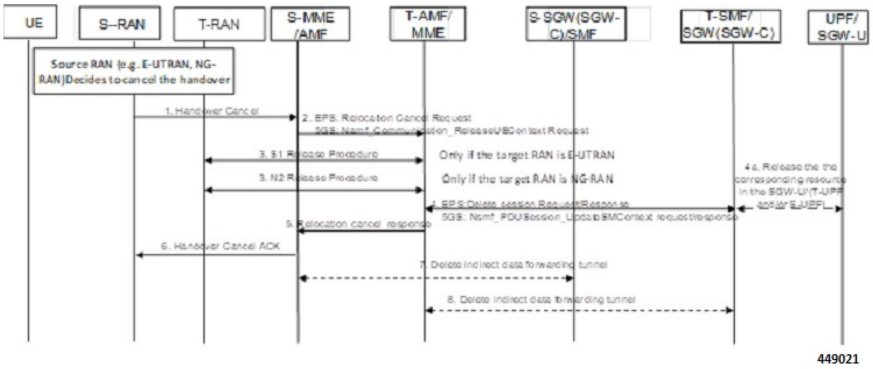
Step	Description
1	MME receives Forward Relocation Request message from AMF. AMF shall include **Return preferred Indication** to indicate preferred return of the UE to the 5GS PLMN at a later access change to a 5GS shared network. AMF includes reserved S-GW address and TEID for both the control plane or EPS bearers in the message. **Note** • MME supports FTEID Interface types **S10/N26 MME GTP-C interface (12)** and **N26 AMF GTP-C interface (40)** received in the **Context Request** message from peer AMF. • MME would use the SGW-C FTEID reserved **TEID** values in the Forward Relocation Request message to determine if the peer is AMF. • If the feature support is disabled, the MME sends Forward Relocation Response failure to peer AMF with cause **Service not supported** .
2	MME selects a new S-GW-C and would send Create Session Request to S-GW and receives Create Session Response from S-GW.
3	MME sends Handover Request message towards eNB with Handover type “5GStoEPS” and includes the Handover Restriction list for eNodeB functions.
4	The target eNodeB sends a Handover Request Acknowledge (EPS Bearer Setup list, EPS Bearers failed to setup list Target to Source transparent container) message to the target MME. The EPS Bearer Setup list includes a list of addresses and TEIDs allocated at the target eNodeB for downlink traffic on S1-U reference point (one TEID per bearer) and addresses and TEIDs for receiving forwarded data if necessary.
5	IDFT enable MME initiate create IDFT Request msg to SMF/GW-C and receives create IDFT response msg from SMF/GW-C.
6	The target MME sends a Forward Relocation Response (Cause, Target to Source transparent container, Serving GW change indication, EPS Bearer Setup List, Addresses and TEIDs) message to the source MME. **Note** For indirect forwarding, this message includes S-GW Address and TEIDs for indirect forwarding (source or target). S-GW change indication indicates that a new S-GW has been selected.
7	The target eNodeB sends a Handover Notify (TAI+ECGI, Local Home Network ID) message to the target MME.
8	The target MME sends a Relocation Complete Notification message to the source AMF. The AMF acknowledges MME with Relocation Complete Acknowledgement message.
9	MME sends Modify bearer request to S-GW and receives Modify bearer response from S-GW.
10	UE initiates Connected mode Tracking Area Update procedure towards MME.

Step	Description
11	If PCC is deployed, the PCF provides the previously removed PCC rules to the P-GW-C+SMF, which triggers the P-GW-C+SMF to initiate dedicated bearer activation procedure and the dedicated Bearer gets activated at MME.

Handover Cancellation Procedure

This section describes Handover cancelation call flow and procedures from EPS to 5GS and from 5GS to EPS.

Figure 14: EPS to 5GS Handover Cancel Call Flow


UE
S--RAN
T-RAN
S-MME /AMF
T-AMF/ MME
S-SGW(SGW-C)/SMF
T-SMF/ SGW(SGW-C)
UPF/ SGW-U
Source RAN (e.g. E-UTRAN, NG-RAN)Decides to cancel the handover
1. Handover Cancel
2. EPS: Relocation Cancel Request
5GS: Namf_Communication_ReleaseUEContextRequest
3. S1 Release Procedure
Only if the target RAN is E-UTRAN
3. N2 Release Procedure
Only if the target RAN is NG-RAN
4a. Release the the corresponding resource in the SGW-U/(T-UPF and/or S-UPF)
4. EPS:Delete session Request/Response
5GS: Namf_PDUSession_UpdateSMContext request/response
5. Relocation cancel response
6. Handover Cancel ACK
7. Delete indirect data forwarding tunnel
8. Delete indirect data forwarding tunnel
449021

EPS to 5GS Handover Cancel Procedure

1. The source eNB decides to cancel the previously requested relocation of Handover resources. This may be due to not enough accepted bearers, UE returned to source cell or any other reason.
2. MME terminates the relocation towards the AMF by sending a Relocation Cancel Request message to AMF. MME also resumes operation on the resources in the source side.
3. The AMF acknowledges the release of all resources on the target side by returning a Relocation Cancel Response (Cause) message to the source MME.
4. If indirect forwarding tunnel is setup during handover preparation, then cancellation of handover triggers the MME to send a Delete Indirect Data Forwarding Tunnel Request message to the S-GW to release the temporary resources used for indirect forwarding.

5GS to EPS Handover Cancel Procedure

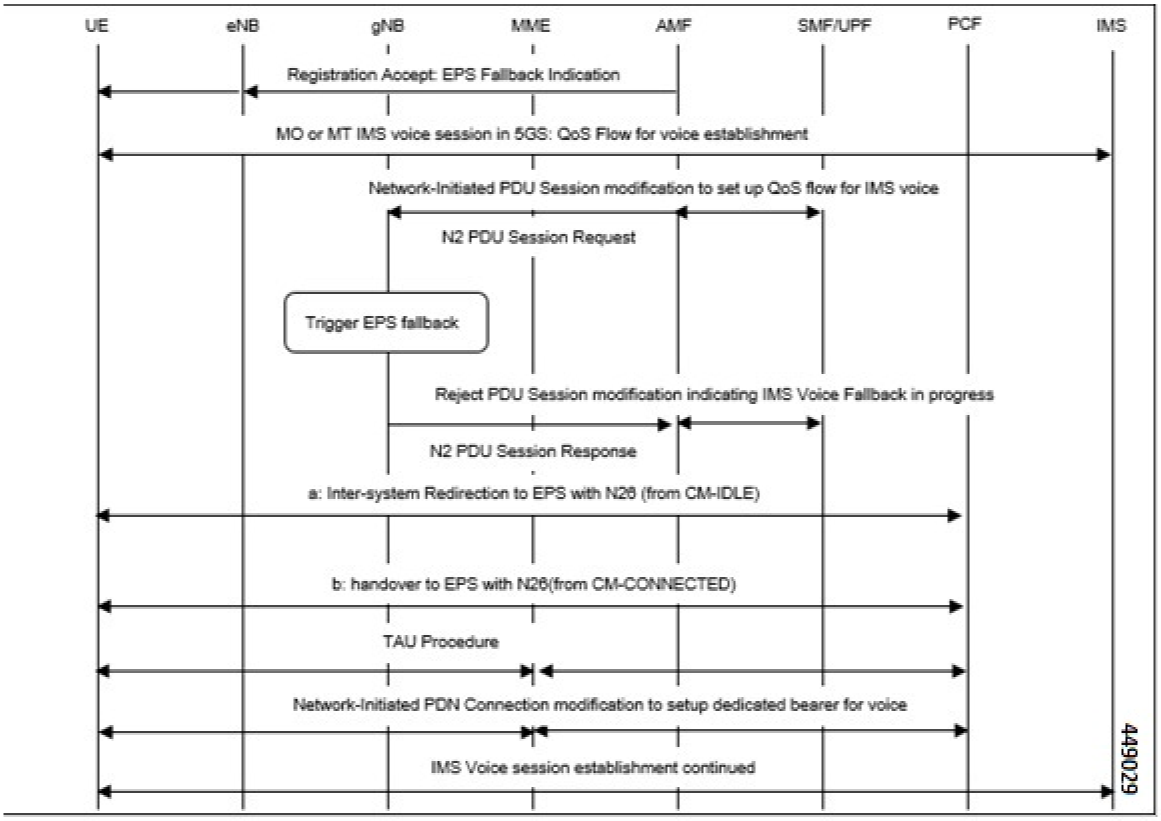
1. MME receives **Relocation Cancel Request** from AMF.
2. MME triggers release of resources towards target RAN node. The target RAN node releases the RAN resource allocated for the handover.
3. MME sends the **Delete session request** (IMSI, Relocation Cancel Indication) to the S-GW/S-GW-C. Based on the Relocation Cancel Indication, MME deletes the session resources established during handover preparation phase in S-GW (S-GW-C and S-GW-U).
4. MME sends **Relocation Cancel Response** towards the AMF.

5. AMF responds with handover cancel ACK towards the source RAN.
6. If indirect forwarding tunnel is setup during handover preparation phase, then cancellation of handover triggers MME to release the temporary resources used for indirect forwarding.

EPS Fallback for IMS Voice Support

MME supports EPS fallback for IMS voice according to 3GPP 23.502.

Figure 15: EPS Fallback for IMS Voice


UE
eNB
gNB
MME
AMF
SMF/UPF
PCF
IMS
Registration Accept: EPS Fallback Indication
MO or MT IMS voice session in 5GS: QoS Flow for voice establishment
Network-Initiated PDU Session modification to set up QoS flow for IMS voice
N2 PDU Session Request
Trigger EPS fallback
Reject PDU Session modification indicating IMS Voice Fallback in progress
N2 PDU Session Response
a: Inter-system Redirection to EPS with N26 (from CM-IDLE)
b: handover to EPS with N26(from CM-CONNECTED)
TAU Procedure
Network-Initiated PDN Connection modification to setup dedicated bearer for voice
IMS Voice session establishment continued
449029

Combined PGW-C and SMF Selection Procedure

MME supports Static P-GW-C/SMF combined Gateway selection. You can configure P-GW-C+SMF in MME Service and in APN profile configuration commands. 5GSIWKI is set when combined P-GW-C/SMF node is selected. The following steps explain the static based combined P-GW-C/SMF selection procdure and how the fallback to the next available option happens if the selection fails:

1. MME chooses Combined P-GW-C/SMF node that supports UE Usage Type and Collocation with S-GW.
2. If step 1 fails, MME selects Combined P-GW-C/SMF node that supports UE Usage type.
3. If step 2 fails, MME selects Combined P-GW-C/SMF node that supports Collocation with S-GW.
4. If step 3 fails, MME selects Combined P-GW-C/SMF node.

5. If step 4 fails, MME selects gateway based on UE Usage type and Standalone P-GW collocation.
6. If step 5 fails, MME selects Standalone P-GW that supports UE Usage type.
7. If step 6 fails, MME selects gateway that supports Standalone P-GW collocation.
8. If step 7 fails, MME selects any gateway from all configured entries.

Limitations

This section describes the known limitations for N26 interface functionality:

- Configuration Transfer Tunnel message is not supported in N26 interface.
- DNS selection is not supported for peer AMF (S10/N26 based) selection.
- DNS selection is not supported for PGW-C/SMF gateway selection.
- Feature specific optional IEs are not supported. For example, Extended Trace Information IE and so on.
- Default EGTP Service will be used for GTPv2 messages on N26 interface.
- Maximum of 32 Peer AMF entries can be configured for GUAMI/TAI configuration

Supported Standards

The N26 feature support is in compliance with the following Standards:

- 3GPP 23.401 version 15.10.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 23.501 version 15.8.0 - System architecture for the 5G System (5GS
- 3GPP 23.502 version 15.8.0 - Procedures for the 5G System (5GS)
- 3GPP 33.501 version 15.7.0 - Security architecture and procedures for 5G System
- 3GPP 24.301 version 15.8.0 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)
- 3GPP 36.413 version 15.8.0 - S1 Application Protocol (S1AP)
- 3GPP 29.272 version 15.10.0 - Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP 29.274 version 15.9.0 - Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP 23.003 version 15.8.0 - Numbering, addressing and identification

Configuring N26 Interface for MME

This section describes the configuration of 5GS Interworking support using N26 interface on MME.

Configuring 5GS Interworking using N26 Interface in Call Control Profile

Use the following configuration to enable 5GS Interworking support using N26 interface.

```
configure
   call-control-profile profile_name
      [ no | remove] n1-mode 5gs-interworking-with-n26
      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 1-64 characters.
- **n1-mode** : Configures interworking with 5GS for UEs supporting N1 mode.
- **5gs-interworking-with-n26** : Enables 5GS-EPS interworking with N26 interface.
- **no** : Disables 5GS-EPS interworking with N26 interface.
- **remove**: Removes the configuration from the Call Control profile and the MME Service configuration applies.

Configuring 5GS Interworking using N26 Interface in MME Service

Use the following configuration to enable 5GS Interworking Support using N26 interface.

```
configure
   context context_name
      mme service  service_name
         [no] n1-mode 5gs-interworking-with-n26
          end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* and must be a string of 1-63 characters.
- **n1-mode**: Configures interworking with 5Gs for UEs supporting N1 mode.
- **5gs-interworking-with-n26**: Enables 5GS-EPS interworking with N26 interface.
- **no**: Disables 5GS-EPS interworking with N26 interface.

Peer AMF Configuration

Configure Peer AMF GUAMI

Use the following configuration to statically configure the peer AMF address in MME service.

```
configure
   context context_name
      mme service service_name
         peer-amf guami { mcc mcc_value mnc mnc_value region-id region_id set-id
 set_id pointer pointer_value address { ipv4_address | ipv6_address }
```

```
      [ no ] peer-amf guami { mcc mcc_value mnc mnc_value region-id region_id
set-id set_id pointer pointer_value }
      end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **peer-amf**: Configures a Peer AMF for 5Gs interworking.
- **guami**: Configures Globally Unique AMF Identifier for this Peer.
- **mcc**: Configures the Mobile Country Code for this Peer AMF.
- **mnc**: Configures the Mobile Network Code for this Peer AMF.
- **region-id**: Configures the Region Identifier for this Peer AMF.
- **set-id** : Configures the Set Identifier for this Peer AMF.
- **pointer**: Configures the Pointer value for this Peer AMF.
- **address**: Configures address of Peer AMF. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.

Configure Peer AMF TAI

```
configure
  context context_name
    mme service service_name
      peer-amf tai-match priority { val mccmcc_value mnc mnc_value tac area_code
address { ipv4_address | ipv6_address }
      [ no ] peer-amf tai-match priority  val
      end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **peer-amf**: Configures a Peer AMF for 5Gs interworking.
- **tai-match**: Configures 5GS Tracking Area Information match for this Peer AMF.
- **mcc**: Configures the Mobile Country Code for this Peer AMF.
- **mnc**: Configures the Mobile Network Code for this Peer AMF.
- **address**: Configures address of Peer AMF. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.

Configure PGW-C with SMF Combined

Use the following command to configure the PGW-C with smf combined configuration in mme-service.

```
configure
  context context_name
```

```
    mme service service_name
      [ no ] pgw-address ipv4_address | ipv6_address ue-usage-type  UUT_Value
collocated-node collocated_name smf-combined   weightweight_value
      end
```

Use the following command to configure the P-GW-C with smf combined configuration in apn-call-control-profile.

```
configure
  context context_name
    apn profile profile_name
      [ no ] pgw-address ipv4_address | ipv6_address ue-usage-type  UUT_Value
collocated-node collocated_name smf-combined
      end
```

NOTES:

- **mme-service** *service_name*: Configures MME Service. *mme_service* must be an alphanumeric string of 1-63 characters.
- **Pgw-address**: Configures p-gw address. Must be followed by address using dotted-decimal notation. This can also be specified as an IPv6 address.
- **ue-usage-type** : Configures UE usage type for disconnecting PDN for up service area.
- **collocated-node**: Configures the Collocation name to select the collocated S/PGW node IP addresses and/or P-GW Node name for 5GS Interworking.

  Note Make sure to configure P-GW Node name under **Collocated-node** for 5GS interworking with N26 interface. This configuration allows P-GW Node Name IE to include the configured name in **Context Response** and **Forward relocation Request** messages from MME to AMF over N26 interface.

- **smf-combined** : Configures a combined P-GW and SMF.
- **no**: Removes the configured PGW address.

Monitoring and Troubleshooting

This section provides information regarding show commands and outputs available to monitor and troubleshoot the N26 Interface feature.

Show Commands and Outputs

show call-control-profile full name

The output of this command includes the **5GS-EPS interworking with N26 interface** field, which indicates if the 5GS-EPS interworking with N26 interface feature is enabled or disabled under N1 mode at call control profile.

show mme-service all

The output of this command includes the following fields:

- **5GS-EPS interworking with N26 interface**
- **Peer AMF GUAMI**
- **Peer AMF TAI**

show mme-service statistics output

The output of this command includes the following fields:

Field	Description
Outbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Outbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS handover procedure.
Inbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS mobility procedure.
Inbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS handover procedure.

show mme-service statistics recovered-values output

The output of this command includes the following fields:

Field	Description
Outbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Outbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS handover procedure.
Inbound relocation using EPS-5GS Mobility procedure	Displays the number of attempts, successes, and failures of outbound relocation using EPS-5GS mobility procedure.
Inbound relocation using EPS-5GS HO procedure	Displays the number of attempts, successes, and failures of Inbound relocation using EPS-5GS handover procedure.

show session disconnect-reasons

The output of this command includes the following fields:

Field	Description
mme-reselection-to-amf	This disconnect reason is incremented, if the subscriber reslects to AMF as part of EPS to 5GS Idle Mobility Registration procedure.

Field	Description
mme-relocation-to-amf	This disconnect reason is incremented, if the subscriber relocates to AMF as part of EPS to 5GS Handover procedure.

Bulk Statistics

MME Schema

MME Service Bulk Statistics

The following MME Service bulk statistics are included in the MME Schema.

Counters	Description
out-mob-4gto5g-n26-attempted	Shows total number of attempted outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-mob-4gto5g-n26-success	Shows total number of successful outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface
out-mob-4gto5g-n26-failures	Shows total number of failed outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-ho-4gto5g-n26-attempted	Shows total number of attempted outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-success,	Shows total number of successful outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-failures	Shows total number of failed outbound relocation using EPS to 5GS Handover procedure in N26 interface.
in-mob-5gto4g-n26-attempted	Shows total number of attempted inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-success	Shows total number of successful inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-failure	Shows total number of failed inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-ho-5gto4g-n26-attempted	Shows total number of attempted inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-success	Shows total number of successful inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-failures	Shows total number of failed inbound relocation using 5GS to EPS Handover procedure in N26 interface.

Counters	Description
mme-decor-ue-usage-type-src-peer-amf	Shows the number of MME subscriber sessions, where UE usage type was obtained from peer AMF as part of handover.

MME Service Backup Bulk Statistics

The following MME Service backup bulk statistics are included in the MME-BK Schema.

Counters	Description
recovered-out-mob-4gto5g-n26-attempted	Shows recovered values for total number of attempted outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
recovered-out-mob-4gto5g-n26-success	Shows recovered values for total number of successful outbound relocation using EPS to 5GS idle mode mobility procedure in N26 interface.
recovered-out-ho-4gto5g-n26-attempted	Shows recovered values for total number of attempted outbound relocation using EPS to 5GS Handover procedure in N26 interface.
recovered-out-ho-4gto5g-n26-success	Shows recovered values for total number of successful outbound relocation using 5GS to EPS handover procedure in N26 interface.
recovered-in-mob-5gto4g-n26-attempted	Shows recovered values for total number of attempted inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
recovered-in-mob-5gto4g-n26-success	Shows recovered values for total number of successful inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
recovered-in-ho-5gto4g-n26-attempted	Shows recovered values for total number of attempted inbound relocation using 5GS to EPS Handover procedure in N26 interface.
recovered-in-ho-5gto4g-n26-success	Shows recovered values for total number of successful inbound relocation using 5GS to EPS Handover procedure in N26 interface.

CHAPTER 16

Rewrite TTL on Downlink Packets

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	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ECS Administration Guide*

Revision History

Revision Details	**Release**
First introduced.	21.19.1

Feature Description

To avoid receiving downlink packets on tethered devices of a subscriber, the tethering blocking feature allows to selectively rewrite TTL on the inner ip-header of all downlink packets for specific flows. Use the configurable option on P-GW to mark the inner IP header TTL with the configured value in the downlink direction between P-GW and S-GW. This allows all the downlink packets related to that specific flow to be consumed at the UE level and downlink packets are not forwarded to the next hop.

How it Works

This section describes a call flow and a procedure for ip-ttl marking on the inner IP header in downlink direction. The following call flow provides the details for setting TTL as "1" in the inner IP header.

Call Flows

Figure 16: Ip-ttl marking on the inner IP header

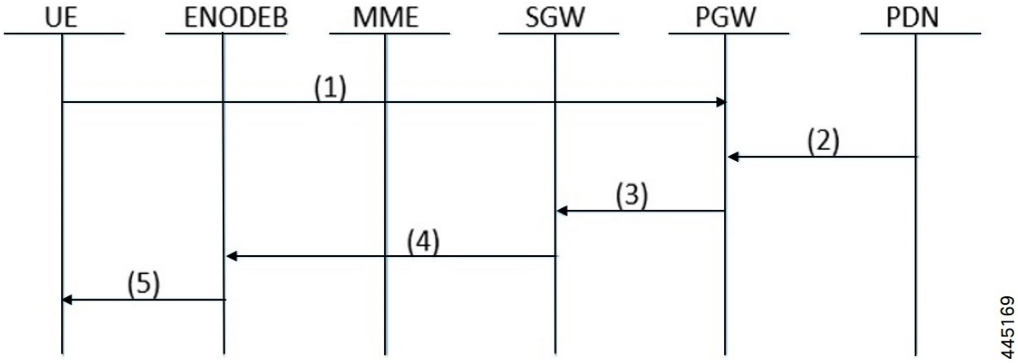


Table 27:

Step	Description
1	UE Attach Procedure and Session is established on all the EPC Nodes such as UE, eNodeB, MME, S-GW and P-GW
2	Downlink traffic is sent for the UE from the PDN. PGW receives the data for a specific flow. The charging-action is selected only for a specific flow. Hence, this feature is applicable only for that specific flows matched by the ruledef and the charging-action combination.
3	PGW encodes the ip-ttl of the inner-IP header with the configured *ttl-value* of the *charging-action* present in *active-charging*. This *ip-ttl* will be forwarded to SGW through S5 interface.

Step	Description
4	Based on the SGW policies, the data are processed further and forwarded towards the UE through eNodeB.
5	UE receives the data from the eNodeB.

Sample Configuration

The following sample configuration describes the configuration of P-GW to mark selectively the inner packet IP of ttl header with specified or configured value:

ip-ttl configuration in charging-action: 4

- If the ip-ttl of the downlink data packet is 8, then the ip-ttl value of the inner packet in the S5 interface is modified or updated to 4.
- If the ip-ttl of the downlink data packet is 2, then the ip-ttl value of the inner packet in the S5 interface remains 2 as the actual value(2) is less than the configured value(4).

Note The inner packet ip-ttl is modified only if the configured ip-ttl value is lower than the value received in the actual downlink packet of that particular flow.

The same rule applies for conflict with other cli for ip-ttl. For example, ip-ttl configuration under the rulebase profile.

Monitoring and Troubleshooting

This section provides the CLI commands available to monitor and troubleshoot the feature

Show Commands

Show active-charging statistics

The output of this show CLI command has been modified to displays count of all the packets that are marked with the configured ttl value to the inner-ip. This is to block the tethering functionality of the UE.

- **Inner IP Tethering Blocked Pkts**

CHAPTER 17

Routing Based on Realm Name S6B

Summary Data

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
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* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Table 28: Revision History

Revision Details	**Release**
First introduced	21.19

Overview of Routing Based on Realm P-GW

Currently, not all diameter applications have an option to have configurable ‘Destination-Realm’ name on initial diameter messages going out of P-GW. As a result, DRAs whenever P-GW is connected to diameter application servers through DRA must look inside those messages, make a routing decision to route it to the correct application server and then overwrite the destination-realm received from client node before sending out to the application server node. However, this generates some level of increased processing and load on the DRA.

This feature provides the facility to fill the ‘Destination-realm’ value from a configurable value to allow DRAs to act in ‘transparent’ mode thus reducing the load on them. It also allows DRAs to use more sophisticated load balancing mechanisms based on ‘Destination-realm’.

Part of this feature was developed for MME (S6a and S13 interfaces). For P-GW, the facility is already present with ‘host-select’ and ‘peer-select’ commands on Gx and Gy interfaces but S6b interface does not have any such facility. This feature fills that gap.

How it Works

Under this feature, ‘Destination-Realm’ AVP in AAR message towards DRA contains the value configured under ‘realm’ as described in the next section. This allows DRAs to act in transparent mode. 'Destination-Realm' AVP is also set to the configured value in further messages for that session, for example, STR.

Enabling Realm for S6b Interface

Use the following configuration to associate the diameter authentication server with a realm name:

```
configure
   context context_name
     aaa group group_name
     diameter authentication server  diameter_host_name priority priority_value
 realm realm_name
    end
```

Note If the 'realm' attribute is configured, then there must be a 'route-entry' with the same 'realm_name'. This is described in the example given below:

Example

```
aaa group s6b
 diameter authentication endpoint s6b
 diameter authentication server dra1.dra.mnc123.mcc456.3gppnetwork.org priority 10 realm
xyz.org

...

diameter endpoint s6b
      origin realm abc.com
      use-proxy
      origin host SPRC01.s6b address 10.239.144.69
      watchdog-timeout 6
      device-watchdog-request max-retries 3
      response-timeout 5
      cea-timeout 3
      reconnect-timeout 30
      connection retry-timeout 10
      peer dra1.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
address 10.1.1.1
      peer dra2.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
address 10.1.1.2
      route-entry realm xyz.org peer dra1.dra.mnc123.mcc456.3gppnetwork.org
```

CHAPTER 18

Supporting Larger Source to Target Container IE in Handover

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
First Introduced.	21.19.6

Feature Changes

Previous Behavior: If S1 Handover includes Source-to-Target-Transparent Container IEs of size greater than 5499 bytes, S1 Handover requests was rejected with ERROR INDICATION (15) and caused Abstract-syntax-error.

New Behavior: MME increased the maximum size of the Source-to-Target-Transparent Container IE from 5499 bytes to 9000 bytes to support the increase in the size of UE radio capabilities driven by additional bands that is supported by RAN specifications and support of significantly more band combinations by UE.

Limitations

The limitations are:

- **General Limitation**: Supports only Larger source eNodeB to target eNodeBE container IE.
- **S1HO Limitation**:
    - The maximum supported size of s1ap packet is 9216.
    - Though the size of IE is less than or equal to 9000, if the size of the packet exceeds 9216, then the packet will be dropped.
- **S10HO Limitation**:
    - The maximum supported packet size is 9188 for VPC platforms.
    - The maximum supported packet size is 7000 for ASR5500 platforms.
    - This limit includes Internal Header + IPv4/Ipv6 Header + UDP Header+ GTPV2 Header + GTV2 Message (Other IEs + Source to Target Container IE).
    - Though the size of IE is less than or equal to 9000, if the size of the packet exceeds 9216, then the packet will be dropped.
    - The Larger Source to Target Container IE in Handover functionality is not supported when the peer fallsback to Gtpv1.

Monitoring and Troubleshooting

This section provides information regarding show commands.

Show Commands and Outputs

show mme-service-statistics-s1ap

The output of this command includes the following fields

```
Protocol Error Statistics:
   Transmitted:
    Transfer Syntax Error:              0  Semantic Error:                     0
    Message Not Compatible:         0
    Abstract Syntax Error:
      Reject:                       0  Ignore And Notify:                  0
      Falsely Constr Msg:           0
Large Packet: 0 >>>> new counter

   Received:
    Transfer Syntax Error:          0  Semantic Error:                     0
    Message Not Compatible:         0
    Abstract Syntax Error:
      Reject:                       0  Ignore And Notify:                  0
      Falsely Constr Msg:           0
Large Packet: 1 Large Container IE: 1 >>>> New counters
```

CHAPTER 19

Support for aaa-acct-arch Bulkstats Counter at System Level

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**
First Introduced.	21.19.6

Feature Changes

Previous Behavior: During archiving the **aaa-acct-archived** counter was not updated and recorded as a context level counter.

New Behavior: During archiving the **aaa-acct-archived** attribute is updated as a system level counter and not accounted as a context level counter as shown in the following example.

```
Context: ISP1, Context-ID 2, PGWCDR-Tramsit: 1 , PGWCDR-Re-Tramsit: 4, PGWCDR-Accept: 0,
PGWCDR-Fail: 5, AAA-Acct-Archive: 985
Context: EPC2, Context-ID 3, PGWCDR-Tramsit: 0 , PGWCDR-Re-Tramsit: 0, PGWCDR-Accept: 0,
PGWCDR-Fail: 0, AAA-Acct-Archive: 985
Context: EPC1, Context-ID 4, PGWCDR-Tramsit: 0 , PGWCDR-Re-Tramsit: 0, PGWCDR-Accept: 0,
PGWCDR-Fail: 0, AAA-Acct-Archive: 985
Context: ISP2, Context-ID 5, PGWCDR-Tramsit: 0 , PGWCDR-Re-Tramsit: 0, PGWCDR-Accept: 0,
PGWCDR-Fail: 0, AAA-Acct-Archive: 985
```

Note In the above example, GTPP config is enabled only for context ISP but the aaa-acct-acrchived counter is displayed across contexts.