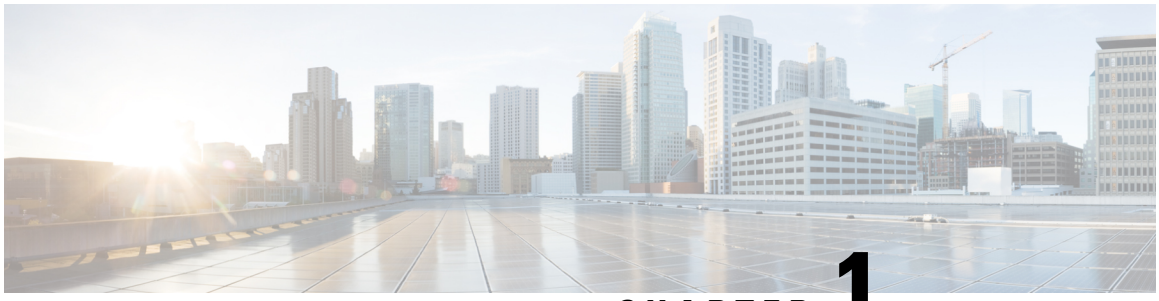
Release Change Reference, StarOS Release 21.20/Ultra Services Platform Release 6.14

First Published: 2020-06-30

Last Modified: 2022-03-17

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



CHAPTER 1

Release 21.20/N6.14 Features and Changes Quick Reference

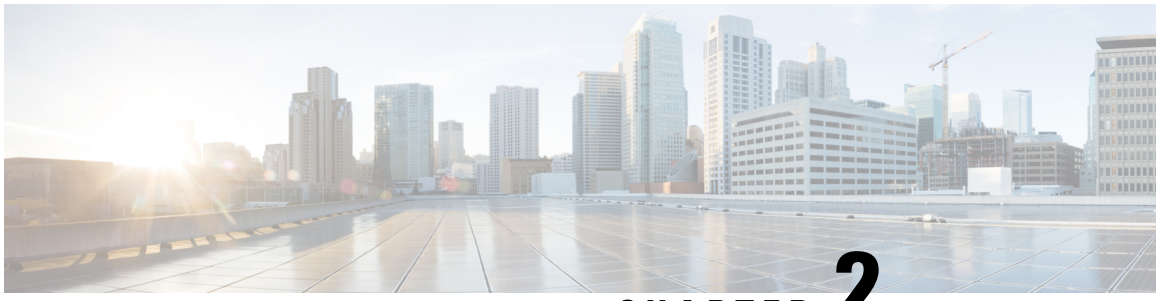
- Release 21.20/6.14 Features and Changes, on page 1

Release 21.20/6.14 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Configuring UE Radio Capability IE Size, on page 11	MME	21.20.3
Connection Release when UE in Idle Mode, on page 57	MME	21.20.26
Cisco Ultra Traffic Optimization, on page 13	P-GW	21.20.4
Counter Enhancements on TAC and LAC Levels, on page 59	MME	21.20.19
Deprecation of Manual Scaling, on page 63	UAS	6.14
Determining GUTI Type using Earlier GUTI Type IE, on page 65	MME	21.20.3
Diameter Route Table Entries Display Limit and Filtration Enhancement , on page 67	• P-GW • S-GW • SAEGW • GGSN	21.20.29
Dynamic TAI List , on page 69	MME	21.20
Emergency Call Support on the ePDG and P-GW, on page 75	P-GW SAEGW	21.20

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
External-Id Support from S6b Interface, on page 87	P-GW SAEGW	21.20
Extended MBR AVP Support within Override Control, on page 95	ECS	21.20.3
Handling Core Dump, on page 99	All	21.20.2
HSS and AuC Interworking Configuration Enhancement, on page 103	MME	21.20
ICMPv6 Response for Fragmented Packets, on page 105	P-GW	21.20.7
IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW, on page 107	P-GW	21.20.11
Inner Fragmentation with VPP Non-CUPS Deployment, on page 109	P-GW	21.20.7
Ignoring SAI, RAI, or CGI in Change Notification Request Messages, on page 111	P-GW	21.20.22
MME Bearer Request Message During Handover Process	MME	21.20.3
Multiple Customized PCO Support, on page 119	GGSN P-GW	21.20.22 21.20.16
5GS Interworking using N26 Interface Support, on page 125	MME	21.20.3
Online Charging Support without Waiting for Credit Control Answer , on page 151	P-GW	21.20.3
Overcoming VoLTE Call Failure	MME	21.20.28
Prevention of Randomization of Well-Known Ports, on page 159	All	21.20
Printing APN Field in EDR Record, on page 161	MME	21.20
Revised Marking for Subscriber Traffic, on page 163	P-GW	21.20.2
Roaming Support for Monitoring Events, on page 171	MME	21.20
RedHat Software Version Update, on page 185	All	21.20.12

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Secondary RAT Usage Report in CDR Records, on page 187	• P-GW • SAEGW • S-GW	21.20.31
Show Fabric Status, on page 201	StarOS	21.20.5
Short Message Service, on page 205	MME	21.20.19
show ip vrf CLI Syntax Changes, on page 237	All	21.20.19
show port npu counter Ouput Command Changes, on page 239	All	21.20.19
Supporting Larger Source to Target Container IE in Handover, on page 197	MME	21.20.3
Support for Presence Reporting Area and Extended QOS on Offline Charging Interface for P-GW and SAEGW, on page 241	P-GW SAEW	21.20.5
Suppressing CCR-U Quota with Validity Timer	GGSN P-GW SAEGW	21.20.16
Support for Tariff-Time-Change in Fast Path, on page 249	P-GW	21.20.22
TCP Reset with Invalid Sequence Number should not Trigger Connection Close, on page 251	P-GW	21.20.25
Writing Rf Charging Records to P-GW Hard Disk, on page 253	P-GW	21.20.5



CHAPTER 2

Feature Defaults Quick Reference

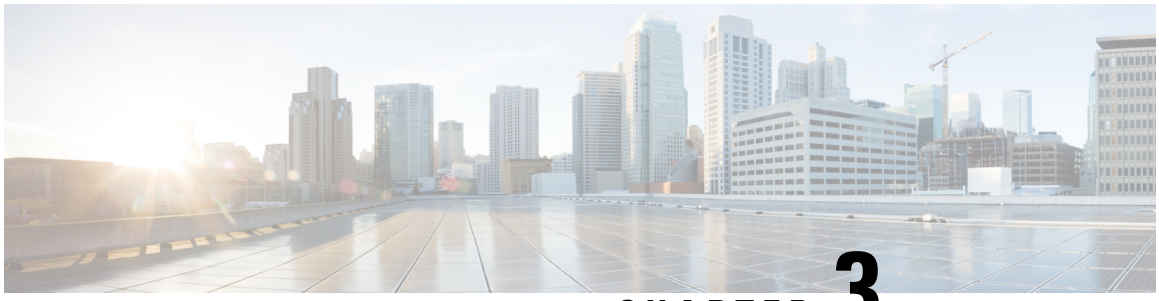
- Feature Defaults, on page 5

Feature Defaults

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

Feature	Default
Configuring UE Radia Capability IE Size	Enabled - Configuration Required
Connection Release when UE in Idle Mode	Enabled - Always-on
Cisco Ultra Traffic Optimization	Disabled - License Required
Counter Enhancements on TAC and LAC Levels	Enabled - Always-on
Short Message Service	Disabled - Configuration Required
Deprecation of Manual Scaling	Disabled - Configuration Required
Determining GUTI Type using Earlier GUTI Type IE	Enabled - Always On
Diameter Route Table Entries Display Limit and Filtration Enhancement	
Dynamic TAI List	Disabled - Configuration Required
Emergency Call Support on the ePDG and P-GW	Enabled - Always-on
External-id Support from S6b Interface	Enabled - Always-on
Extended MBR-AVP Support within Override Control	Disabled - Configuration Required
MME Bearer Request Message Handover	Disabled - Configuration Required
Multiple Customized PCO Support	Disabled - Configuration Required
Handling Core Dump	Enabled - Always-on
HSS and AuC Interworking Configuration Enhancement	Enabled - Always-on

Feature	Default
ICMPv6 Response for Fragmented Packets	Enabled - Configuration Required
Ignoring SAI, RAI, or CGI in Change Notification Request Messages	Disabled - Configuration Required
IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW	Enabled - Always-on
Inner Fragmentation with VPP non-CUPS deployment	Enabled - Configuration Required
N26 Interface Support	Enabled - Always-on
Online Charging Support without Waiting for Credit Control Answer	Enabled - Always-on
Overcoming VoLTE Call Failure	Disabled - Configuration Required
Printing APN Field in EDR Record	Enabled - Always-on
Revised Marking for Subscriber Traffic	Enabled - Always-on
RedHat Software Version Update	Enabled - Always-on
Roaming Support for Monitoring Events	Disabled - Configuration Required
Secondary RAT Usage Report in CDR Records	Disabled - Configuration Required
show ip vrf CLI Syntax Changes	Enabled - Always-on
show port npu counter Ouput Command Changes	Enabled - Always-on
Supporting Larger Source to Target Container IE in Handover	Enabled - Always-on
Support for Presence Reporting Area and Extended QOS on Offline Charging Interface for P-GW and SAEGW	Disabled - Configuration Required
Suppressing CCR-U Quota with Validity Timer Running	Disabled - Configuration Required
Support for Tariff-time-Change in Fast Path	Enabled - Always-on
Prevention of Randomization into Well-Known Ports	Enabled - Always-on
Writing Rf Charging Records to P-GW Hard Disk	Disabled - Configuration Required



CHAPTER 3

Bulk Statisctics Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.20 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 21.20 include:

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

New Bulk Statistics

None in this release.

Modified Bulk Statistics

The following variables are modified in the schema file.

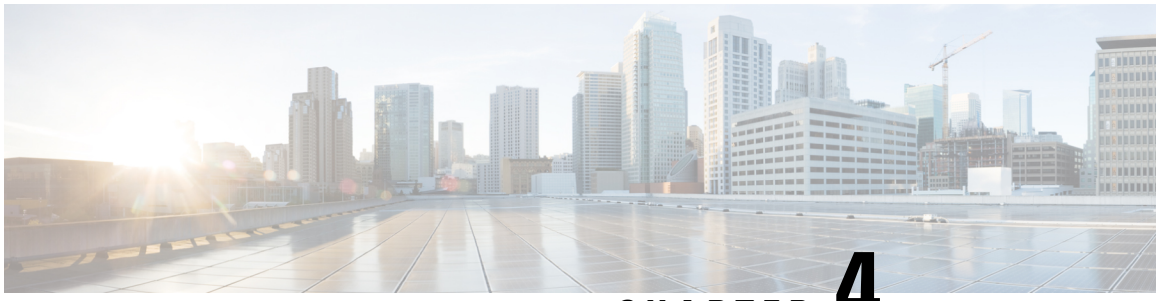
Table 1: Bulk Statistic Variables in the VLAN-NPU Schema

Variables	Description	Data Type
ipv4-mru-excd-rx-frames **Note** In StarOS 21.20 and later releases, the "ipv4-mru-excd-rx-frames" variable is replaced with the following: mru-excd-rx-frames variable.	**Description:** The total number of received frames for packets where the Maximum Receive Unit (MRU) has been exceeded. **Trigger:** Increments whenever a packet with a byte count that exceeds the MRU is received on an interface. **Availability:** Existing interface **Type:** Counter	Int64

Variables	Description	Data Type
ipv4-mru-excd-rx-bytes **Note** In StarOS 21.20 and later releases, the "ipv4-mru-excd-rx-bytes" variable is replaced with the following: mru-excd-rx-bytes variable.	**Description:** The total number of received bytes for packets where the MRU has been exceeded. **Trigger:** Increments whenever a packet with a byte count that exceeds the MRU is received on an interface. **Availability:** Existing interface **Type:** Counter	Int64

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.20 and USP 6.14

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.20 and Ultra Services Platform (USP) 6.14 software releases.

- SNMP MIB Object Changes for 21.20, on page 9
- SNMP MIB Alarm Changes for 21.20, on page 10
- SNMP MIB Conformance Changes for 21.20, on page 10
- SNMP MIB Object Changes for 6.14, on page 10
- SNMP MIB Alarm Changes for 6.14, on page 10
- SNMP MIB Conformance Changes for 6.14, on page 10

SNMP MIB Object Changes for 21.20

This section provides information on SNMP MIB alarm changes in release 21.20.

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 21.20.

- starObjectRCMChassisState
- starObjectRCMReloadReason
- starRCMServiceStart
- starRCMServiceStop
- starRCMConfigPushCompleteReceived
- starRCMConfigPushComplete
- starX3ContextId

Modified SNMP MIB Object

- StarX3ConnType
- starIPSECGroupName
- starX3MDConnDown
- starX3MDConnUp

Deprecated SNMP MIB Object

- starX3ContextName

SNMP MIB Alarm Changes for 21.20

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

SNMP MIB Conformance Changes for 21.20

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

SNMP MIB Object Changes for 6.14

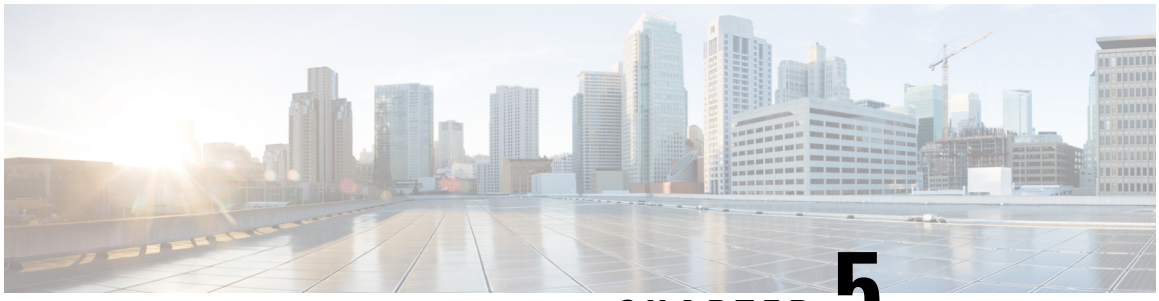
There are no new, modified, or deprecated SNMP MIB object changes in this release.

SNMP MIB Alarm Changes for 6.14

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

SNMP MIB Conformance Changes for 6.14

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



CHAPTER 5

Configuring UE Radio Capability IE Size

- Feature Summary and Revision History, on page 11
- Feature Changes, on page 12
- Command Changes, on page 12

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Configuration of UE Radio Capability IE Size	21.5.26
Configuration of UE Radio Capability IE Size Introduced to 21.18 release.	21.18
Configuration of UE Radio Capability IE Size Introduced to 21.17 release.	21.17.6
First introduced.	21.12.15

Feature Changes

Previous Behavior: When the UE sends its UE Radio Capability packet exceeding 6000 bytes to the MME, the MME is unable to respond to any subsequent Service Request. MME drops the message as the maximum S1AP packet size limit is 6144 bytes.

New Behavior: MME checks the size of UE Radio Capability IE in UE Capability Information Indication message with the configured limit size from New CLI is introduced to limit the size of UE Radio Capability IE.

Command Changes

This section describes the CLI configuration required to configure UE Radio Capability IE size.

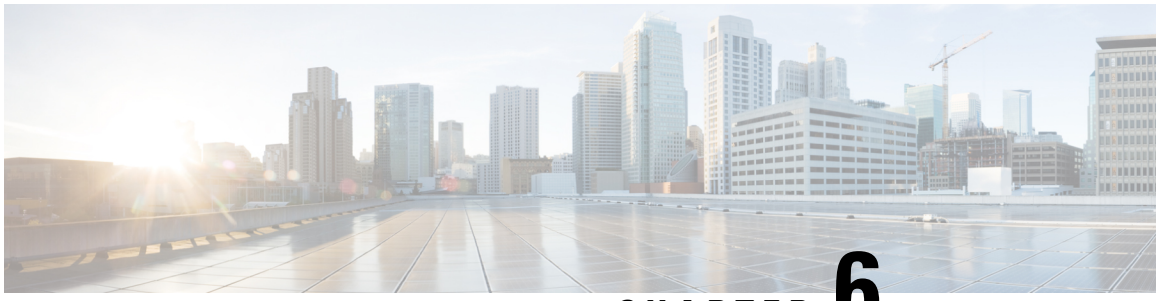
Configuring the UE Radio Capability IE

Use the following configuration to set the size of UE Radio Capability IE.

```
configure
  context context_name
    mme-service mme_service_name
    s1-mme ue-radio-cap
    s1-mme ue-radio-capsize
    no s1-mme ue-radio-cap
    end
```

NOTES:

- **ue-radio-cap**: Sets the size of UE Radio Capability IE default value 5632 bytes.
- **ue-radio-cap size**: Specifies the size of UE Radio Capability IE in bytes. **size** must be an integer in the range of 3072 to 9000 .
- **no s1-mme ue-radio-cap** Disables the UE radio capability size limit.



CHAPTER 6

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

- Feature Summary and Revision History, on page 13
- Overview, on page 14
- How Cisco Ultra Traffic Optimization Works, on page 15
- Configuring Cisco Ultra Traffic Optimization, on page 40
- Monitoring and Troubleshooting, on page 44

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, ranges of configurable policy parameters for Cisco Ultra Traffic Optimization are modified.	21.20.4

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
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

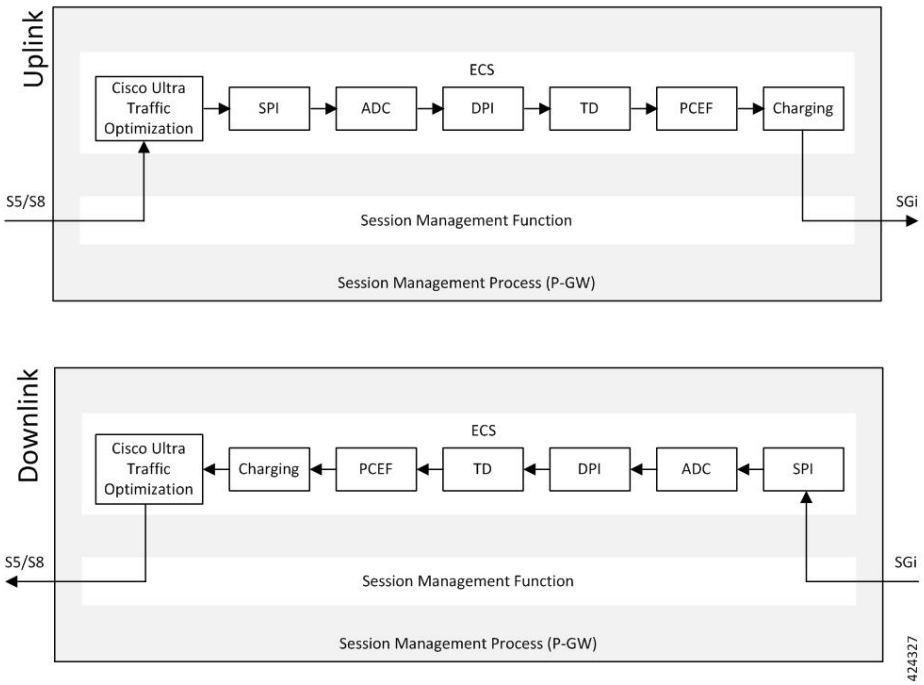
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested 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.



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:

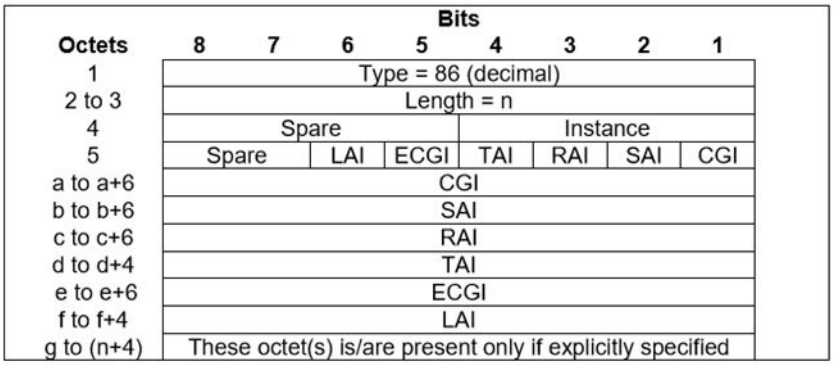
- 92 is the Session Manager instance
- 30278 is the Session Handle orsession number
- 14786055 is the ACS flow identifier

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 1: User Location Information (ULI)



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

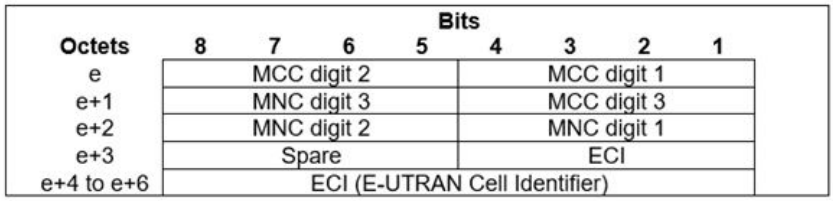
Here 16 represents that ULI Type is ECGI

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 2: ECGI Field



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-timeout**	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	Comment
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 different from Base, the value from Base parameter and an appropriate message will be displayed.
	max- rate	100-100000 kbps	15000	100-500000 kbps	100000	require greater than or equal to base max-rate	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	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	Comment
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 37.

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.

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
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.

Bulk Statistics	Description
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.
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.

Bulk Statistics	Description
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.
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.

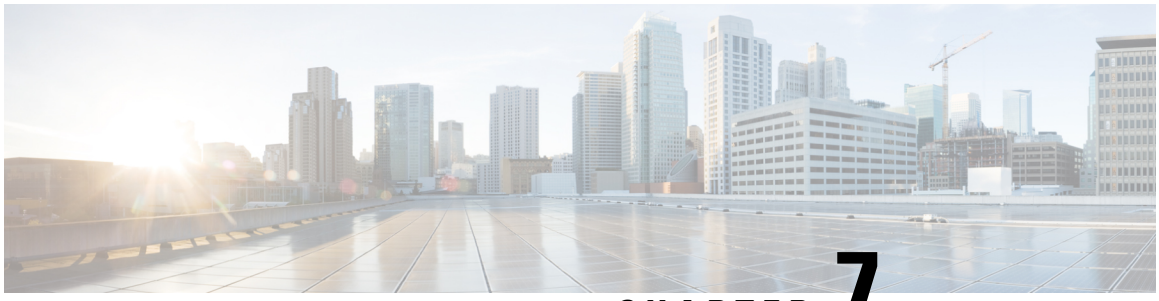
Bulk Statistics	Description
tcp-total-unmanaged-large-flow-count	Indicates the number of TCP total-unmanaged-large-flow count for Cisco Ultra Traffic Optimization.
tcp-total-io-bytes	Indicates the number of TCP total-IO bytes for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-bytes	Indicates 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.
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.

Bulk Statistics	Description
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.
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.

Bulk Statistics	Description
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.
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.

Bulk Statistics	Description
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.
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.

Bulk Statistics	Description
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 7

Connection Release when UE in Idle Mode

- Feature Summary and Revision History, on page 57
- Feature Changes, on page 57

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	*Ultra IoT C-SGN Administration Guide*

Revision History

Revision Details	Release
First Introduced	21.20.26

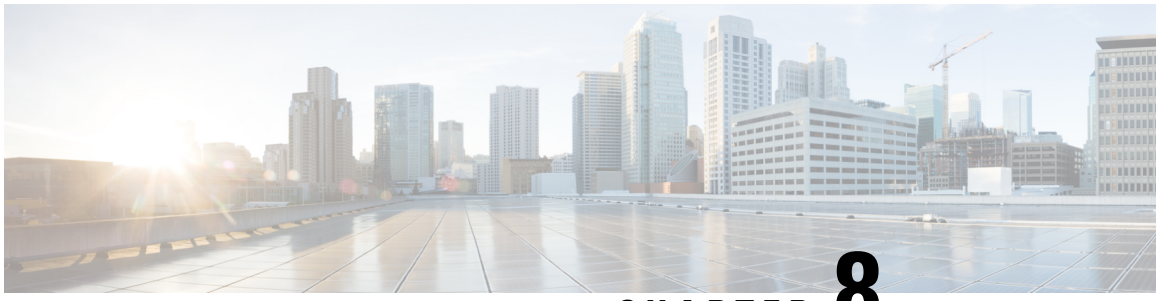
Feature Changes

Previous Behavior: In MME, when UE is in Idle mode, Connection Release (CMR - Connection Management Request) received from SCEF was not supported.

New Behavior: In this StarOS 21.20.26 release, MME supports the Connection Release (CMR - Connection Management Request) received from SCEF when UE in the Idle mode.

Without PDN support, if Connection Release is requested from SCEF for the last PDN in the UE Idle mode, MME initiates:

- Paging when ppf flag was TRUE
- Detach with Re-Attach required towards UE after successful completion of paging.



CHAPTER 8

Counter Enhancements on TAC and LAC Levels

- Feature Summary and Revision History, on page 59
- Feature Description, on page 60
- Monitoring and Troubleshooting, on page 60

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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
The counters that were introduced in release 21.17.9 are now supported in release 21.20.19.	21.20.19
New counters are added in the TAl schema	21.17.9

Feature Description

In StarOS 21.17 and later releases, counters on TAC and LAC level are enhanced to add them on TAI schema and LAC object. This is required to monitor basic KPI on TAL/LAC level. These counters calculates KPI pertaining to attach success ratio, quantity of attached idle or connect users, and Dedicated bearers success rate on TAC level.

Monitoring and Troubleshooting

Show Commands and Output

show mme-service statistics tai

This section provides information on the show commands available to support this feature.

Table 2: show mme-service statistics tai Output Descriptions

Field	Description
ESM Statistics	
NW Initiated Dedicated Bearer Activations	
Attempted	This sub-group displays the total number of attempted ESM network intiated dedicated bearer activations for each TAI.
Success	This sub-group displays the total number of successful ESM network intiated dedicated bearer activations for each TAI.
Failures	This sub-group displays the total number of failed ESM network intiated dedicated bearer activations for each TAI.
Session Statistics	
Total Subscribers	
Attached Calls	The total number of EPS Mobility Management call-line statistics on attached current calls for each TAI.
Connected Calls	The total number of EPS Mobility Management call-line statistics on connected current calls for each TAI.
Idle Calls	The total number of EPS Mobility Management call-line statistics for each TAI indicating idle current calls.
EMM Control Messages	
Received	

Field	Description
Attach Complete	Displays total number of EMM Attach Complete message received from UE indicating increments for each Attach Complete message received from UE.
Attach Request	Displays total number of EMM Attach Requests received from UE indicating increments for each Attach Request message received from UE.
PDN Connectivity Reject:	
Other Reasons	Displays total number of ESM messages sent for each TAI by the MME. This indicates that the PDN connection has been rejected for a cause other than one of those listed in the output generated by the **show mme-service statistics esm-only** command.

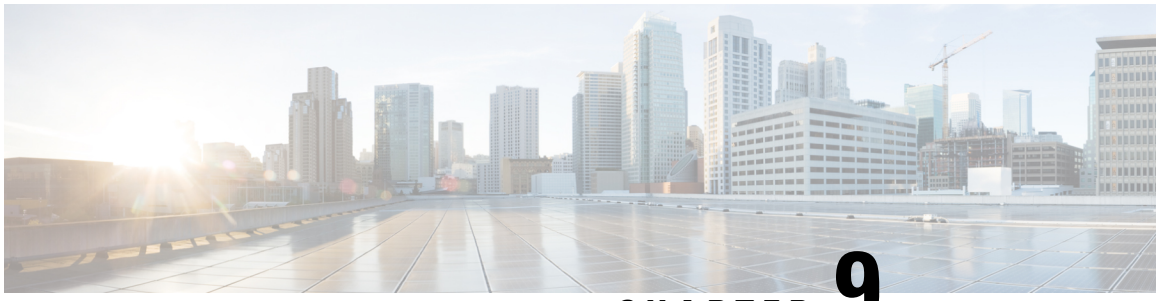
Bulk Statistics

TAI Schema

The following counters are available in the TAI schema.

Bulk Statistics	Description
tai-esm-msgtx-pdncon-rej-other-reasons	Shows the total number of ESM messages sent for each TAI by the MME. This indicates that the PDN connection is rejected for a cause other than one of those listed in the output generated by the **show mme-service statistics esm-only** command
tai-emm-msgrx-attach-req	Shows the total number of EMM Attach Requests received from UE. This is incremented for each Attach Request message received from UE.
tai-emm-msgrx-attach-complete	Shows the total number of EMM Attach Complete message received from UE. This is incremented for each Attach Complete message received from UE.
tai-emmcall-attach-currcall	Shows the total number of EPS Mobility Management call-line statistics on attached current calls for each TAI.
tai-emmcall-connect-currcall	Shows the total number of EPS Mobility Management call-line statistics on connected calls for each TAI.
tai-emmcall-idle-curcall	Show the total number of EPS Mobility Management call-line statistics on idle current calls for each TAI.
tai-dedi-brr-activation-nw-attempted	Shows the total number of ESM Network initiated dedicated bearer activations attempted for each TAI.

Bulk Statistics	Description
tai-dedi-brr-activation-nw-success	Shows the total number of successful ESM Network-initiated dedicated bearer activations for each TAI.
tai-dedi-brr-activation-nw-failures	Shows the total number of failed ESM Network-initiated dedicated bearer activations for each TAI.



CHAPTER 9

Deprecation of Manual Scaling

- Feature Summary and Revision History, on page 63
- Feature Changes, on page 63

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*

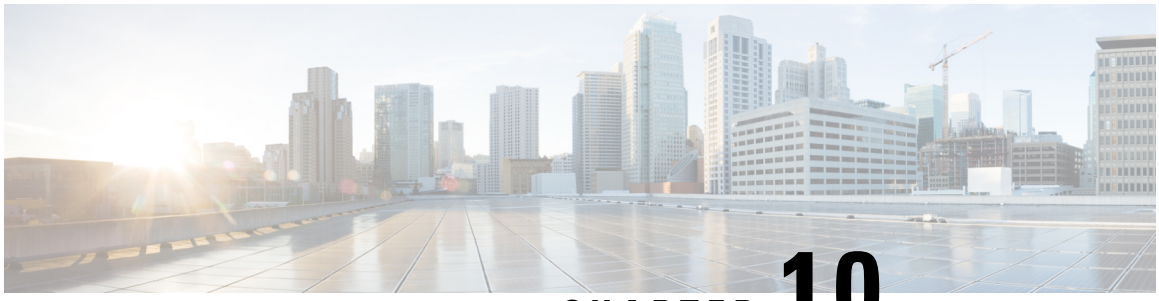
Revision History

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 10

Determining GUTI Type using Earlier GUTI Type IE

- Feature Summary and Revision History, on page 65
- Feature Changes, on page 66

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	21.20.3

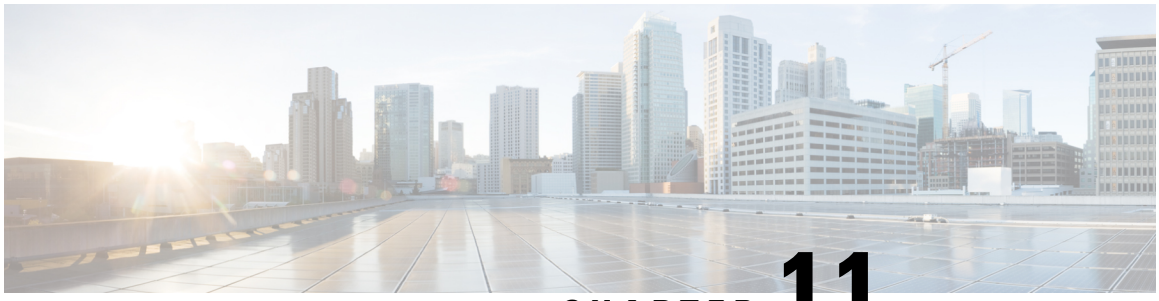
Feature Changes

According to the 3GPP specification 23.401, the MME resolves the old MME/SGSN using Globally Unique Temporary Identity (GUTI) sent earlier in the Attach request and TAU request messages, and determines if the earlier GUTI is mapped or native by one of the following two methods:

- Indication using most significant bit (MSB) in MME Group ID.
- Explicit indication sent from UE to MME (Old GUTI type IE).

Previous Behavior: MME used the MME Group ID MSB bit to determine the GUTI type for the UEs moving from old MME or SGSN.

New Behavior: MME uses the old GUTI type IE to determine the GUTI type for the UEs moving from old MME/SGSN/AMF. If old GUTI Type IE is not present, then MME uses MME Group ID MSB bit to determine the GUTI type.



CHAPTER 11

Diameter Route Table Entries Display Limit and Filtration Enhancement

- Feature Summary and Revision History, on page 67
- Feature Changes, on page 68

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW • GGSN
Applicable Platform(s)	All
Feature Default	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

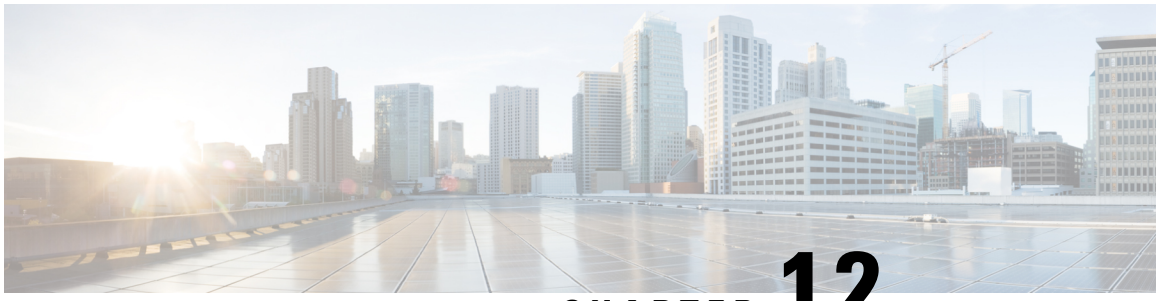
Revision Details	Release
Support for a limit and filtration on displaying route entries is added.	21.20.29

Feature Changes

Previous Behavior: The CLI output for the diameter route table does not have any limit and filtration on displaying route entries and this resulted to crash and restart of CLI task when there is a huge list of diameter route entries.

New Behavior: A limit is enforced and expired route entries are filtered while displaying the diameter route entries.

Impact on Customer: As the limit and filtration are enforced for the existing CLI **show diameter route table debug-info**, the changes introduced avoids the CLI task crash/reload for the cases where there is a huge list of diameter route entries to be shown/displayed. This limit is applicable for diameter route display during SSD collection and regular CLI **show diameter route table debug-info** execution.



CHAPTER 12

Dynamic TAI List

- Feature Summary and Revision History, on page 69
- Feature Description, on page 70
- Configuring dynamic-tal in mme-service and call-control-profile, on page 71
- show call-control-profile all, on page 71
- Monitoring and Troubleshooting, on page 72

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 release supports Dynamic TAI lists as enahncement to Tracking Area list management.	21.20

Feature Description

To reduce the signaling message during the location update procedure and to manage the border areas more efficiently, MME maintains the historic TAI list for each UE. If the Dynamic Tracking Area List (DTAL) feature is enabled:

- When UE sends for the first time the Attach/TAU request message, MME saves this TAI in Historic TAI list and sends the TAL with configured values of TAI-mgmt-objs.
- Whenever MME detects TAI change, MME updates the historic list with new TAI details.
- When MME sends the Attach/TAU Accept, the new Dynamic TAL gets filled. This new DTAL will be a combination of Configured TAI-mgmt-objs and historic TAI list. MME saves the TAI to a maximum number of 16. MME uses the same TAL list as sent in ATTACH/TAU Accept message for paging.

Important MME uses the same DTAL as part of paging. Based on the DTAL depth configuration, the number of TAI in the historic list will be more and TAL list will have more TAC, resulting in more than normal level of paging. Based on paging load there will be impact in CPU usage.

How it works:

- When MME builds the DTAL, TAI entries from the tai-mgmt-obj takes precedence. If the tai-mgmt-obj already has 16 entries, the Dynamic TAL gets filled with those entries and the TAI entries from historic list is not considered.
- If the number of TAI in tai-mgmt-obj is less than 16, the remaining entries are filled from historic TAI list based on the depth configuration or the remaining empty entries in the TAL List, whichever is the least.
- Historic TAI list contains list of the TAI visited by UE. The entries are sorted by time. When the list reaches the maximum number of entries, the oldest TAI gets removed.
- Each User Equipment (UE) in the same tracking area can have its TAL list because of the difference in dynamic TAI.

Note The Historic TAI List is not recovered as part of Session manager recovery. After the Session manager recovery, MME will build the Historic TAI List for UE from beginning.

Limitation

As UE does not perform TAU procedure when moving to dynamically learnt TAL, S-GW will not be reassigned/reallocated as per TAI-mgmt-obj configuration.

Configuring dynamic-tal in mme-service and call-control-profile

Use the following CLIs to enable or disable and to configure depth of the TAL maintained for each UE.

Configuring CLI dynamic-tal in mme-service

```
configure
   context context_name
      mme-service service_name
        dynamic-tal depth depth-value
        [ no ] dynamic-tal
        end
```

NOTES:

- **mme-service** *service_name*: Specifies the name of the MME service and and must be a string of 1-63 characters.
- **dynamic-tal** *depth-value*: Configures the dynamic-tal for MME service users. MME maintains historic TAI list per UE up to the configured depth value.
- **depth** *depth-value*: Number of unique historic entries in TAL up to a maximum of 16.
- **no**: Removes the depth value in an MME Service.

Configuring CLI dynamic-tal in call-control-profile

```
configure
   context context_name
   call-control-profile  profile_name
       dynamic-tal depth depth-value
       [ no ] dynamic-tal
       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.
- **dynamic-tal** : Configures the dynamic-tal. MME maintains historic TAI list for each UE up to the configured depth value.
- **depth** *depth-value*: Number of unique historic entries in TAL up to a maximum of 16.
- **no** : Removes the depth value.

show call-control-profile all

The output of the above command is modified to display the Dynamic TAL List for each UE. Last Dynamic TAI History displays up to a maximum of 16 reported TAIs and is not controlled based on the configured depth value in mme-service.

```
UE Tracking Information: Last Dynamic TAI History
       |                Last Reported TAI |           Last Update
  ------------------------------------------------------------------------------
   (1)    (123,456)                0x1a7c             Fri Jun 12 09:09:11 2020
   (2)    (123,456)                 0x92e              Fri Jun 12 09:09:11 2020
   (3)    (123,456)                0x22c4             Fri Jun 12 09:09:10 2020
```

Monitoring and Troubleshooting

Show Commands and Output

show mme-service all

The output of the above command is modified to display the configured dynamic-tal depth value and not configured dynamic-tal depth value in mme-service and call-control-profiles.

For example, when dynamic-tal depth value is configured the following output is displayed:

```
Service name              : mme1
          Context                   : ingress
          Status                    : STARTED
          Bind                      : Done
..
          Dynamic TAL Depth         : 5
```

When dynamic-tal depth value is not configured the following output is displayed.

```
Service name              : mme1
          Context                   : ingress
          Status                    : STARTED
          Bind                      : Done
..
          Dynamic TAL Depth         : Not defined
```

show mme-service statistics tai

The output of this command includes the following Intra MME TAU Requests:

- Dynamic TAI List Periodic TAU—Displays the number of attempts, successes, and failures of Dynamic TAI list periodic tracking area update (TAU).
- Dynamic TAI List TA Updating—Displays the number of Dynamic TAI List TA updates, attempts, successes, or failures associated with all MME services.

show mme-service statistics

When the dynamic TAL list feature is enabled, new TAL statistics and existing TAU statics gets updated for MME service level EMM and TAI Statistics. The output of this command includes the following TAU sub-group:

Field	Description
Dynamic TAI List Periodic TAU	Displays the number of attempts, successes, and failures of Dynamic TAI list periodic tracking area update (TAU).

Field	Description
Dynamic TAI List Normal TAU without SGW Relocation	Displays the number of Dynamic TAI List Norma TAU, without S-GW relocation, attempts, successes, or failures associated with all MME services.
Dynamic TAI List TAU with Bearer Activation	Displays the number of Dynamic TAI list TAU, with bearer actvation, attempts, successes, or failures associated with all MME services.
Dynamic TAI List TAU with SGW Relocation	Displays the number of Dynamic TAI List TAU, with S-GW relocation, attempts, successes, or failures associated with all MME services.

Bulk Statistics

This section provides information on the bulk statistics for the Dynamic TAL feature.

MME-Schema

The following existing TAU bulk statistics are included in the MME Schema.

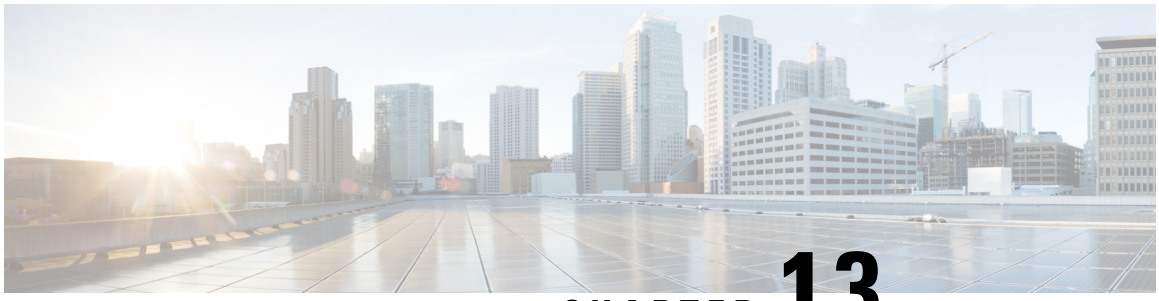
Counters	Description
dtal-tau-periodic-attempted	The total number of Dynamic TAI List Periodic TAU requests attempted.
dtal-tau-periodic-success	The total number of Dynamic TAI List Periodic TAU requests succeeded.
dtal-tau-periodic-failures	The total number of Dynamic TAI List Periodic TAU requests failed.
dtal-tau-normal-attempted	The total number of EMM Dynamic TAI List TAU request attempts where the EPS update type is set to TA updating (without S-GW relocation).
dtal-tau-normal-success	The total number of EMM Dynamic TAI List TAU request succeeded.
dtal-tau-normal-failures	The total number of EMM Dynamic TAI List TAU request failed.
dtal-tau-active-attempted	The total number of EMM Dynamic TAI List TAU with bearer activation attempts.
dtal-tau-active-success	The total number of EMM Dynamic TAI List TAU with successful bearer activation.
dtal-tau-active-failures	The total number of EMM Dynamic TAI List TAU with failed bearer activation.
dtal-tau-sgw-change-attempted	The total number of EMM Dynamic TAI List TAU with S-GW relocation attempts.
dtal-tau-sgw-change-success	The total number of EMM Dynamic TAI List TAU with S-GW relocation success.

Counters	Description
dtal-tau-sgw-change-failures	The total number of EMM Dynamic TAI List TAU with S-GW relocation failures.

TAI Schema

The following existing TAI bulk statistics are included in the MME Schema.

Counters	Description
tai-dtal-intra-tau-attempted	The total number of Dynamic TAI List Intra-MME normal TAU attempted with or without S-GW change.
tai-dtal-intra-tau-success	The total number of Dynamic TAI List Intra-MME normal TAU succeeded with or without S-GW change.
tai-dtal-intra-tau-failures	The total number of Dynamic TAI List Intra-MME normal TAU failed with or without S-GW change.
tai-dtal-tau-periodic-attempted	The total number of Intra-MME Dynamic TAI List Periodic TAU attempted.
tai-dtal-tau-periodic-success	The total number of Intra-MME Dynamic TAI List Periodic TAU succeeded.
tai-dtal-tau-periodic-failures	The total number of Intra-MME Dynamic TAI List Periodic TAU failed.



CHAPTER 13

Emergency Call Support on the ePDG and P-GW

This feature provides emergency call support on the ePDG and P-GW.

- Feature Summary and Revision History, on page 75
- Feature Description, on page 76
- How it Works, on page 77
- Configuring AAA Failure Handling for S2b Emergency Calls, on page 83
- Configuring APN and S6b Authorization, on page 84
- Monitoring and Troubleshooting, on page 85

Feature Summary and Revision History

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

Revision History

Revision Details	Release
This release supports new emergency calls from S2b Interface. **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	21.1

Feature Description

The ePDG and P-GW support emergency call establishment over untrusted WiFi for the P-GW as per 3GPP Release 13. Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normal attached UEs and, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in a limited service state does not require a subscription.

Authentication Authorization Requests (AAA) to Diameter now carry the new Emergency-Indication AVP for Untrusted WiFi emergency calls. Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, in the event that the 3GPP AAA Server has to apply traffic reduction.

Supported Functionality

3GPP Release 13 Emergency Call Support on the ePDG and P-GW includes the following functionality:

- Emergency call establishment over untrusted Wi-Fi for the P-GW. The P-GW includes the new **Emergency-Indication** AVP over the AAA S6b interface only during Emergency PDN connection establishment.
- Lawful Intercept is supported for Emergency PDNs over the S2b interface.
- Various Create Session Request message IEs have been modified to support all four different behaviors of emergency bearer establishment.
- Intra- and Inter-chassis recovery are supported for emergency call over the S2b interface.
- Network initiated dedicated bearer creation is supported for emergency calls over the S2b interface.
- The maximum APN restriction is ignored for emergency APN.
- Multiple PDNs are supported for emergency calls over the S2b interface.
- Context replacement for emergency calls over the S2b interface without IMSI with same IMEI is supported.
- P-GW emergency related statistics and bulkstats are available.
- Graceful shutdown of S2b emergency calls is supported.

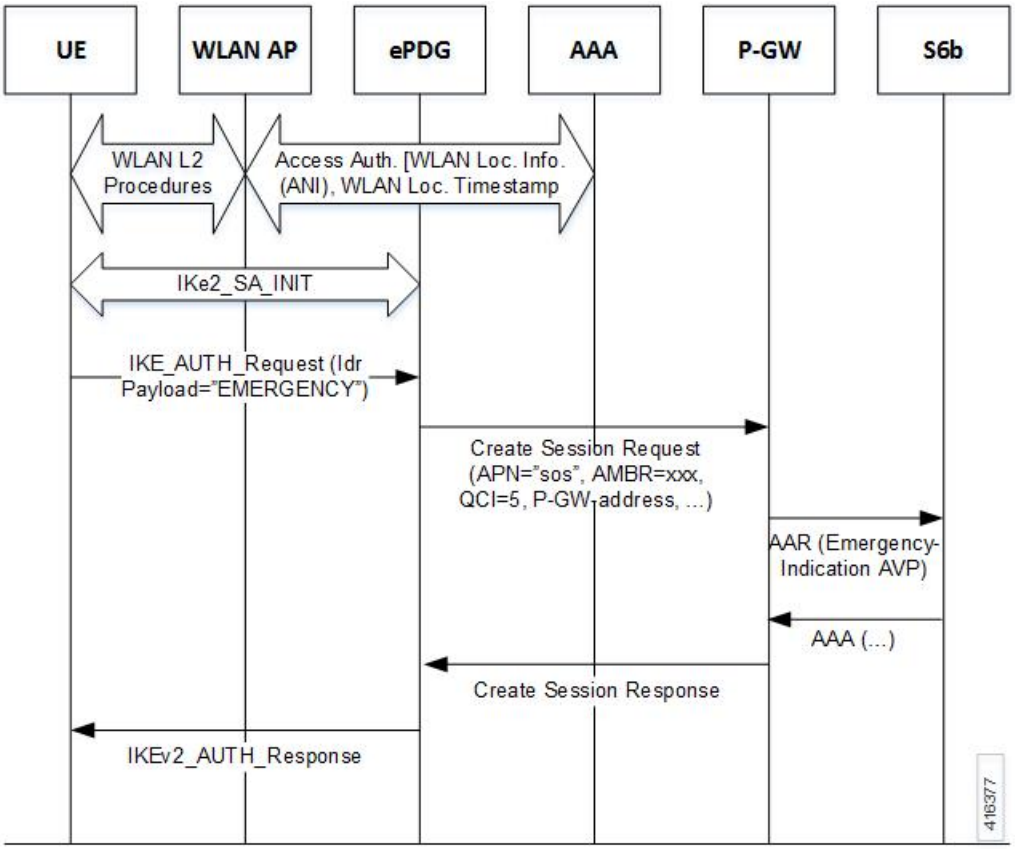
Previous Behavior: Emergency calls were not supported for the S2b interface. Also, handoff between the s2b interface and LTE was not supported for emergency calls.

New Behavior: Emergency calls are now supported on the S2b interface and handover is also supported for emergency calls from the S2b interface to LTE and vice-versa for "authenticated imsi" only.

How it Works

The ePDG sends a Create Session Request (CSReq) message to the P-GW. The P-GW deduces the emergency related policies to apply from the Access Point Name (APN) received in the CSReq message. For emergency attached User Equipment (UE), if the International Mobile Station Identifier (IMSI) cannot be authenticated or the UE has not provided it, then the International Mobile Equipment Identifier (IMEI) is used as UE identifier.

Figure 3: Call Flow: 3GPP R13 Emergency Call Support on the ePDG and P-GW



The P-GW sends the **Emergency-Indication** AVP over the s6b interface so that the 3GPP AAA server only applies specific policies for emergency services. For an unauthenticated UE, the 3GPP AAA server does not update the Home Subscriber Server (HSS) with the identity of the P-GW. For an authenticated UE, this indication is sent together with the "PDN GW currently in use for emergency services" message, which comprises the PDN GW address and the indication that the PDN connection is for emergency services to the HSS, which stores it as part of the UE context for emergency services.

Support is available for all four different behaviors of emergency bearer establishment:

- Valid UEs only.
- Only UEs that are authenticated are allowed.
- IMSI required, authentication optional.
- All UEs are allowed.

This section describes the new Attribute Value Pair (AVP) and modified Information Elements that support the feature.

Emergency-Indication AVP

A new **Emergency-Indication** AVP is defined in the Authentication and Authorization Request to signal a request to establish a PDN connection for emergency services.

Information Elements

This section describes other important elements in a Create Session Request that have been modified to work properly with the feature.

Table 3: Information Elements in a Create Session Request

Information Elements	P	Condition/Comment	IE Type	Ins.
IMSI	C	The IMSI is included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, except for the case: If the UE is emergency attached and the UE is UICCless. The IMSI shall be included in the message on the S4/S11 interface, and on the S5/S8 interface if provided by the MME/SGSN, but not used as an identifier. - If UE is emergency attached but IMSI is not authenticated. The IMSI is included in the message on the S2a/S2b interface.	IMSI	0

Information Elements	P	Condition/Comment	IE Type	Ins.
MSISDN	C	For an E-UTRAN Initial Attach and a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN the IE is included when used on the S11 interface, if provided in the subscription data from the HSS. For a PDP Context Activation procedure and a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN the IE is included when used on the S4 interface, if provided in the subscription data from the HSS. The IE is included for the case of a UE Requested PDN Connectivity, if the MME has it stored for that UE. It is included when used on the S5/S8 interfaces if provided by the MME/SGSN. The ePDG includes this IE on the S2b interface during an Attach with GTP on S2b , UE initiated Connectivity to Additional PDN with GTP on S2b and a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, Initial Attach for emergency session (GTP on S2b), if provided by the HSS/AAA. The TWAN includes this IE on the S2a interface during an Initial Attach in WLAN on GTP S2a, UE initiated Connectivity to Additional PDN with GTP on S2a and a Handover to TWAN with GTP on S2a, if provided by the HSS/AAA.	MSISDN	0
ME Identity (MEI)	C	The MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface: - If the UE is emergency attached and the UE is UICCless. - If the UE is emergency attached and the IMSI is not authenticated. For all other cases the MME/SGSN includes the ME Identity (MEI) IE on the S11/S4 interface if it is available.	MEI	0
	CO	The TWAN/ePDG shall include the ME Identity (MEI) IE on the S2a/S2b interface, if it is available.		
Serving Network	C	This IE is included on the S4/S11, S5/S8 and S2b interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN, a UE requested PDN connectivity, an Attach with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b and an Initial Attach for emergency session (GTP on S2b).	Serving Network	0

Information Elements	P	Condition/Comment	IE Type	Ins.
Indication Flags	C	This IE shall be included if any one of the applicable flags is set to 1. Applicable flags are: - Unauthenticated IMSI: This flag is set to 1 on the S4/S11 and S5/S8 interfaces if the IMSI present in the message is not authenticated and is for an emergency attached UE.	Indication	0
Selection Mode	C	This IE is included on the S4/S11 and S5/S8 interfaces for an E-UTRAN initial attach, a Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN, a PDP Context Activation, a Handover from Trusted or Untrusted Non-3GPP IP Access to UTRAN/GERAN and a UE requested PDN connectivity This IE is included on the S2b interface for an Initial Attach with GTP on S2b, a Handover to Untrusted Non-3GPP IP Access with GTP on S2b, a UE initiated Connectivity to Additional PDN with GTP on S2b and an Initial Attach for emergency session (GTP on S2b) The IE indicates whether a subscribed APN or a non-subscribed APN chosen by the UE/MME/SGSN/ePDG/TWAN was selected. This IE is included on the S2a interface for an Initial Attach in WLAN on GTP S2a, a Handover to TWAN with GTP on S2a and a UE initiated Connectivity to Additional PDN with GTP on S2a. The value is set to "MS or network provided APN, subscription verified".	Selection Mode	0
	CO	When available, this IE is sent by the MME/SGSN on the S11/S4 interface during TAU/RAU/HO with S-GW relocation.		
UE Local IP Address	CO	The ePDG includes this IE on the S2b interface during an Initial Attach for emergency session (GTP on S2b). Otherwise the ePDG shall include this IE on the S2b interface based on local policy.	IP Address	0
UE PDP Port	CO	The ePDG includes this IE on the S2b interface if NAT is detected and the UE Local IP Address is present.	Port Number	0
WLAN Location Information	CO	This IE is included on the S2b interface if the WLAN Location Information is available.	TWAN Identifier	1
WLAN Location Timestamp	CO	This IE is included on the S2b interface, if the WLAN Location Timestamp is available.	TWAN Identifier Timestamp	0

Emergency Handover Support

When a subscriber makes an emergency call over WLAN, user equipment (UE) adds *sos* to the *NAI* to indicate that this is an emergency attach to ePDG. ePDG informs P-GW about this emergency attach in create session request. When the caller moves away from WLAN into LTE coverage or vice versa, the call gets handed over without being dropped.

P-GW supports following emergency call handovers:

- **Handover of Emergency Calls from LTE to Wi-Fi(S2b)** : Handovers of emergency calls from LTE to Wi-Fi (S2b) for authenticated UE is supported. While the UE moves from LTE to untrusted Wi-Fi, LTE triggers an Authentication Authorization Request (AAR) to the S6b server with the AVP *Emergency-Indication* sent in that Authentication and Authorization Request (AAR). Also, an STR is sent when a Wi-Fi (S2b) call is cleared.:

  1. The ePDG sends Create Session Request to the P-GW.
  2. If the UE requested P-CSCF in the IKE Config request, P-CSCF is requested.
  3. Downlink packets are sent on LTE access. The ePDG includes the IP address that is received within the IKE message from the UE in the PAA (PDN Address Allocation) in the GTPv2 Create Session Request.
  4. The P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
  5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
  6. 3GPP AAA sends AAA to the P-GW.
  7. The Policy and Charging Rules Function (PCRF) acknowledges IP-CAN Session Modification with a Credit Control Answer (CCA).
  8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
  9. ePDG sends Create Bearer Response message.
  10. P-GW sends the Delete Bearer Request message.
  11. The S-GW sends Delete Bearer Response message to the P-GW.

- **Handover of Emergency Calls from Wi-Fi(S2b) to LTE** : Handover of Emergency Calls from Wi-Fi (s2b) to LTE for authenticated UE is supported. Since an emergency call in LTE does not have S6b interface authorization enabled, handover of emergency calls from untrusted Wi-Fi to LTE triggers a Session Termination Request (STR) to the S6b server:

  1. The MME selects the P-GW from the MME Emergency Configuration Data and sends a Create Session Request.
  2. The S-GW sends a Create Session Request.
  3. P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR), if Gx authentication is enabled or P-GW applies the local policy and does not query PCRF if local policy is configured. P-GW sends Session Termination Request to S6b server and P-GW provides IPv6 Prefix and/or IPv4 address in PAA.

Note If the MME indicates Piggyback support, then, the P-GW piggybacks the Create Bearer Request message to the Create Session Response message.

4. The MME sends a Modify Bearer Request message to the S-GW.
5. The S-GW processes each message independently. The S-GW forwards the Create Bearer Response to the P-GW(without piggybacking).

- **Emergency PDN Handover with HO=0**: Handovers from LTE to Wi-Fi is supported:

1. The ePDG sends Create Session Request to the P-GW. P-CSCF is requested if the UE requested P-CSCF in the IKE Config request.

Note Downlink packets are dropped at the P-GW while the session is being handed over to WLAN.

2. P-GW checks for an LTE session.
3. If there is an LTE session, the P-GW sends AAR to the 3GPP AAA to authorize the APN for the subscriber and to update P-GW address on the HSS for the APN.
4. 3GPP AAA sends AAA to the P-GW.
5. The P-GW sends an indication of IP-CAN modification to the PCRF with Credit Control Request (CCR).
6. The PCRF acknowledges of IP-CAN Session Modification with a Credit Control Answer (CCA) message. This message includes the Policy and Charging rules. The P-GW enforces and triggers for events that must be reported by the P-GW.
7. If Online flag is enabled and if P-GW does not have quota for the WLAN rating group, or if Online Charging Server (OCS) has not sent a 4011 for the WLAN rating group previously, then the P-GW sends a CCR-u to the OCS reporting the usage.
8. The P-GW identifies the S5 session and reallocates the requested IP address session and responds back to the ePDG with a Create Session Response message.
9. After the P-GW sends the Create Session Response, the P-GW sends an interim Accounting Request (ACR) to the OFCS.
10. The OFCS responds with an ACA to the P-GW.
11. P-GW sends the Delete Bearer Request to the S-GW.
12. The S-GW sends Delete Bearer Response to the P-GW.

Configuring AAA Failure Handling for S2b Emergency Calls

Emergency calls over the S2b interface should not be rejected due to a failure from the S6b server. To ensure this, failure handling must be configured in the APN which is used for emergency calls .

Handling is configured in the **aaa group** so that emergency calls continue regardless of failures as indicated by the result code.

To configure AAA failure handling for S2b emergency calls:

```
configure
  context ingress_context_name
    aaa group default
      diameter authentication failure-handling authorization-request
result-code 3000 to 5999 action continue
       diameter authentication failure-handling authorization-request
request-timeout action continue
          end
```

Note the following assumptions:

- If an IP-CAN Session Modification Request triggered by the PCRF removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signaling, then the PCEF starts a configurable emergency inactivity timer. When the configured period of time expires, the P-GW initiates an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session
- If the Gx/S6b interface returns a Virtual APN, which is not configured as an emergency APN, then the call is rejected with the cause code "APN_DENIED_NO_SUBSCRIPTION

To configure failure handling template for Gx failure (PCRF down):

```
configure
  failure-handling-template gx_template
   msg-type any failure-type diabase-error action continue local-fallback

       end
```

Following example shows failure handling template configuration for Gx failure (PCRF return ErrorCode):

```
configure
  failure-handling-template gx_template
     msg-type credit-control-initial failure-type diameter result-code
3000 to 5999 action continue local-fallback
       msg-type credit-control-update failure-type diameter result-code
 3000 to 5999 action continue local-fallback
           end
```

Following example shows failure handling template configuration for Gx delayed response:

```
configure
  failure-handling-template gx_template
    msg-type credit-control-initial failure-type resp-timeout action
continue
       msg-type credit-control-update failure-type resp-timeout action
```

```
continue
          end
```

To configure local policy for Gx failure (PCRF down or PCRF return ErrorCode):

```
configure
        local-policy-service service_name
          ruledef  ruledef_name
             condition priority  priority  { variable { eq | ge | gt | le |
 lt | match | ne | nomatch } regex | string_value | int_value | set }
            end
```

```
configure
  local-policy-service service_name
    actiondef   actiondef_name
      action priority  priorityaction_name arguments
        end
```

```
configure
  local-policy-service service_name
    eventbase   eventbase_name
      rule priority  priority   [ event list_of_events ] ruledef
ruledef_name actiondef actiondef_name [ continue ]
        end
```

```
configure
  contextcontect_name
    ims-auth-service   service_name
      [ no ] policy-control
        associate failure-handling-template gx_template
          associate local-policy-service  service_name
            end
```

Configuring APN and S6b Authorization

Configuring APN to attach emergency PDN on LTE

For emergency PDN handover with S6b Gx, configure APN mode to attach emergency PDN on LTE.

```
configure
  context context_name
    apn apn_name
      emergency-apn
      end
```

Enabling S6b Authorization

Following is the sample configuration to enable S6b authorization:

```
configure
```

```
context context_name
  pgw-service service_name
    apn apn_name
      authorize-with-hss [ egtp[gn-gp-enabled] [ s2b [gn-gp-enabled]
 [ s5-s8 [gn-gp-enabled | gn-gp-enabled]] [ report-ipv6-addr ]| lma [
s6b-aaa-group aaa-group-name | report-ipv6-addr ] | report-ipv6-addr ]
[ default | no ] authorize-with-hss
       end
```

Enabling S2b Interface eGTP Service

Use the following configuration to enable S2b Interface eGTP service:

```
configure
  context context_name
    egtp-service service_name
      interface-type { interface-cgw-egress | interface-epdg-egress |
interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn |
 interface-sgw-egress | interface-sgw-ingress }
      end
```

Following the example configuration to enable S2b Interface eGTP service:

```
configure
       context EPC2
        egtp-service PGW21EGTP
         interface-type | interface-pgw-ingress [ s2b ] [ s2a ]
                          end
```

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature

Show Commands and Output

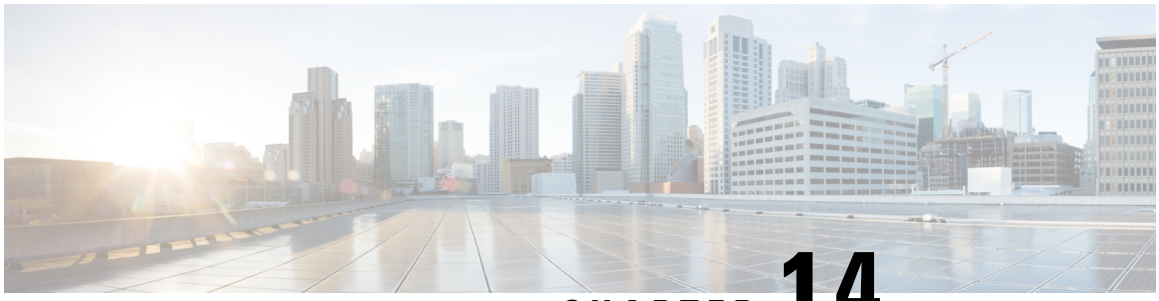
This section provides information regarding show commands and their outputs in support of the feature.

show apn

```
pdp type:  ipv4 and ipv6
apn type:  emergency
ehrpd access: N/A
absolute timeout :  0           idle timeout :  0
emergency inactivity timeout :  1000
idle-timeout-activity ignore-downlink:   Disabled
…..
```

show pgw- service-statistics-all

```
pgw# show pgw-service statistics all
PGW Node Level Statistics:
VPN Name: local
Total bearers active:
  Default bearers:    5                                  Dedicated bearers:  5
    Normal bearers:   2                                  UE-initiated:  0
    Emergency bearers (Auth-IMSI): 1                     Network-initiated: 5
    Emergency bearers (Unauth-IMSI):1                    Normal bearers:   2
    Emergency bearers (Only IMEI): 1                     Emergency bearers (Auth-IMSI):  1
    Emergency bearers (Unauth-IMSI):1

    Emergency bearers (Only IMEI): 1
```



CHAPTER 14

External-Id Support from S6b Interface

- Feature Summary and Revision History , on page 87
- Feature Description, on page 88
- How it Works, on page 88
- Monitoring and Troubleshooting, on page 91
- Bulk Statistics, on page 93

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	Enabled - Always On
Related Changes in This Release	Not applicable
Related Documentation	• *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.20

Feature Description

LTE Network Elements (NE), which supports Mobile Station International Subscriber Directory Number (MSISDN) as an identifier for UE, currently supports External-Id as an alternative ID for the MSISDNLess device. This is required to authorize Mobile Private Network (MPN) call using 3GPP External-Id for the MSISDNLess device.

External-Id is received in the Network Access Identifier (NAI) format with a maximum size of 22 characters. The operator must ensure the correct format and size of the External-Id value.

Note An MSISDNLess UE is assigned with an International Mobile Subscriber Identity (IMSI) number.

The LTE interfaces such as Gx, Rf, S6b, and RADIUS accounting messages pass External-Id as an alternative ID of MSISDN.

Note Gy/Rf and Gz/CDR interfaces are not required to support External-Id value.

Limitations

Following are the limitations:

- External-Id value supports only E-UTRAN and E-UTRAN NB-IOT RAT types.
- External-Id is not supported for Handover scenarios. For example, LTE to 3G and LTE to Wi-Fi handovers and vice versa.

How it Works

The following call flow and procedure describes how the feature works:

Figure 4: Call flow for New Session Establishment

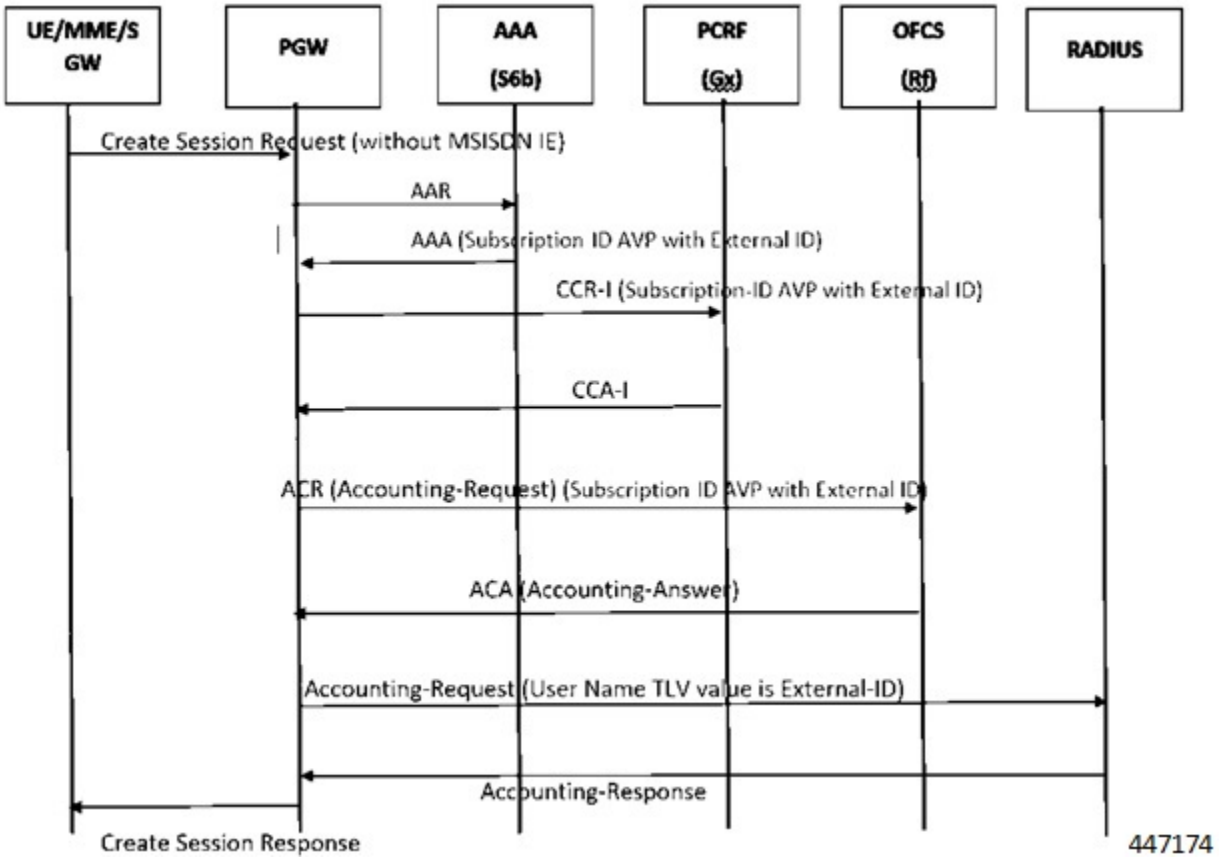


Table 4: Procedure

Step	Description
1	The S-GW sends a Create Session Request message with or without MSISDN IE for MSISDNLess LTE UE devices to the P-GW.
2	The P-GW receives Creation Session Request message and sends authentication/authorization request message to 3GPP AAA server over S6b interface when external authentication is enabled.
3	The P-GW receives External-Id value in subscription-Id AVP from 3GPP AAA server over S6b interface. This value inherits all the sub sessions of session or pointer. **Note** External-Id received during initial attach persists throughout the session. The External-Id that is received from the S6b server after the initial attachment is ignored.
4	P-GW propagates External-Id value to PCRF in Credit Control Request (CCR) Initial message over Gx interface for getting policies and Offline Charging System (OFCS) over Rf interface for diameter-based accounting or RADIUS accounting server.

Step	Description
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 the Monitoring Event Report parameter or to acknowledge the deletion of the identified monitoring event configuration at the time of request. **Note** At P-GW, if S6b interface is not configured for LTE call or External-Id value is not received in AAA message from 3GPP AAA server, then a call is continued and session is established

Sample Behavior Scenarios

Following are Message types and the behavior of External-Id in Gx and Rf interfaces.

Table 5: RAT Type Behavior

RAT Type	Behavior
3G	External-Id value not supported
EUTRAN	External-Id value supported
NB-IoT	External-Id value supported
Trusted-Wi-Fi	External-Id value not supported
Untrusted-Wi-Fi	External-Id value not supported
eHRPD	External-Id value not supported

Table 6: Handoff Behavior

Handoff	Behavior
E-UTRAN > **NB-IoT**	External-Id value supported
NB-IoT > **E-UTRAN**	External-Id value supported
E-UTRAN > **3G**	External-Id value not supported*
E-UTRAN > **3G** > **E-UTRAN**	External-Id value not supported*
3G > **E-UTRAN**	External-Id value not supported*
3G > **E-UTRAN** > **3G**	External-Id value not supported*

Handoff	Behavior
E-UTRAN > **Wi-Fi**	External-Id value not supported*
E-UTRAN > **Wi-Fi** > **E-UTRAN**	External-Id value not supported*
Wi-Fi > **E-UTRAN**	External-Id value not supported*
Wi-Fi > **E-UTRAN** > **Wi-Fi**	External-Id value not supported*

Note * If UE is attached with supported RAT type and moved to not supported RAT type, then external-Id is not supported for all the subsequent handovers(HO).

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the External-Id feature support over S6b interface.

Show Commands and Outputs

show subscribers pgw-only full all

show subscribers pgw-only full all

The following example displays the External ID value in output:

```
Username: 0121234569085403@nai.epc.mnc023.mcc121.3gppnetwork.org
  Subscriber Type : Visitor
  Status          : Online/Active
  State           : Connected
  Connect Time    : Wed Mar 18 11:29:09 2020
  Auto Delete     : No
  Idle time       : 03h23m01s
  MS TimeZone     : n/a              Daylight Saving Time: n/a
  Access Type: gtp-pdn-type-ipv4      Network Type: IP
  Access Tech: eUTRAN                    pgw-service-name: pgw-ingress
  Callid: 00004e3c                         IMSI: 121234569085403
  MSISDN: n/a                              External ID: 9326737200@abc.com
  Interface Type: S5S8GTP                Low Access Priority: N/A
  TWAN Mode: N/A
  eMPS Bearer: No
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: Enabled
  Access Peer Profile: default
  Acct-session-id (C1): AC100A1E00000034
  ThreeGPP2-correlation-id (C2): 004112D9 / 002sujt5
  Card/Cpu: 1/0                          Sessmgr Instance: 1
```

show subscribers saegw-only full all

The following example displays the External ID value in output:

- pgw# show subscribers saegw-only full all

```
 Username            : 0214365789012345@nai.epc.mnc036.mcc214.3gppnetwork.org
   SAEGW Call mode   : Co-located
   Subscriber Type   : Visitor
   Status            : Online/Active
   State             : Connected
   Bearer State      : Active
   Connect Time      : Thu Apr 23 21:59:35 2020

   SAEGW UID         : 10001
   Idle time         : 00h04m09s
   Auto Delete        : No
   Fastpath Eligible  : No

   Callid           : 00004e21                   IMSI               : 214365789012345

   Card/Cpu          : 1/0                        Sessmgr Instance    : 1
   Source context    : ingress                    Destination context : egress
   Bearer Type       : Default                    Bearer-Id           : 5
   Access Type       : gtp-pdn-type-ipv4          Network Type        : IP
   Access Tech       : eUTRAN                     saegw-service-name  : saegw-service
   MSISDN           : n/a                       External ID        : 9900000000@abc.com

   TWAN Mode         : N/A
   eMPS Bearer       : No
   MS TimeZone       :                            Daylight Saving Time: n/a
```

show pgw service statistics all

The following example displays the External ID value in output:

```
show pgw-service statistics all
VPN Name: local
Subscribers Total:
  Active: 1
  S6b Assume Positive: 0
PDNs Total:
  Active:  1    Setup: 1
  Released:  0    Rejected: 0
Session Discovery Req statistics:
  Total IMSI+IP lookup: Total get call info evt for Rule Info:
      Attempted:  0      Attempted: 0
      Success:  0      Success: 0
      Failed:  0      Failed: 0
  Total get session info events for session sync: 0
External-Id Present Session Statistics:
  Active Sessions:  1    Total Created Sessions: 1
  Released Sessions:  0
```

show saegw-service statistics all

show saegw-service statistics all function pgw

The following example displays the External_Id value in output:

```
Subscribers Total:
  Active: 1
  S6b Assume Positive: 0
PDNs Total:
  Active: 1    Setup:  1
  Released: 0    Rejected: 0
Session Discovery Req statistics:
  Total IMSI+IP lookup:   Total get call info evt for Rule Info:
      Attempted:  0      Attempted: 0
      Success:    0      Success:   0
      Failed:     0      Failed:    0
  Total get session info events for session sync: 0
External-Id Present Session Statistics:
  Active Sessions: 1    Total Created Sessions:   1
  Released Sessions: 0
```

Bulk Statistics

This section provides information on the bulk statistics for the External-id feature suuport over s6b interface.

P-GW Schema

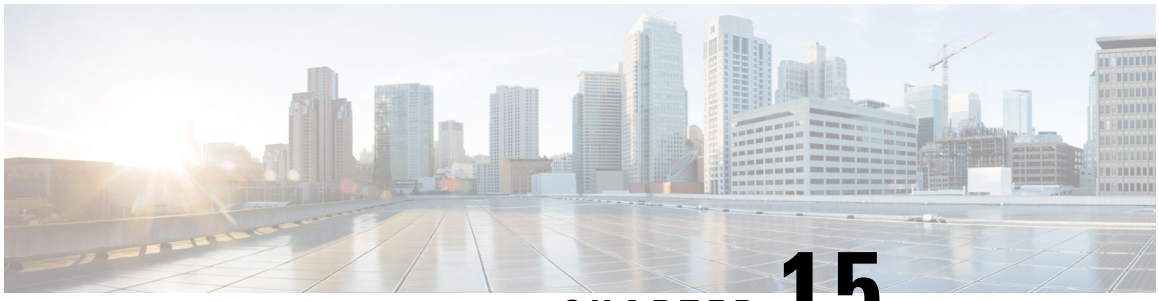
The following bulk statistics are added for P-GW in the P-GW schema in support of the External-id feature.

Counters	Description
external-id-active-sessions	Number of active sessions with external-id from s6b.
external-id-total-sessions	Number of total sessions with external-id from s6b.

SAEGW Schema

The following bulk statistics are added for SAEGW in the SAEGW schema in support of the External-id feature.

Counters	Description
external-id-active-sessions	Number of active sessions with external-id from s6b.
external-id-total-sessions	Number of total sessions with external-id from s6b.



CHAPTER 15

Extended MBR AVP Support within Override Control

- Feature Summary and Revision History, on page 95
- Feature Description, on page 96
- How it Works, on page 96
- Monitoring and Troubleshooting, on page 97

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Thie Extended MBR AVP in Override Control feature is fully qualified in this release.	21.20.3

Revision Details	Release
In this release, support is added for Extended MBR AVP in Override-Control feature to allow the overridden parameters to be specified for a rule (static or predefined), for one or all charging actions (using a wildcard), with the ability to exclude certain rules. **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.	21.20

Feature Description

To obtain the User Equipment (UE) speed above 4.2 Gbps, PCRF must send Override Control AVPs that support Tethering traffic MBR and/or GBR up to 10Gbps when UE moves to 5G coverage area. However, the existing override-control customized AVP definition only supports the actual speed up to 4.2 Gbps. This is because the maximum rate defined for Max-Requested-Bandwidth-DL/UL and Guaranteed-Bitrate-DL/UL are limited to (2^32-1) bps.

To address this requirement, the override control feature is enhanced to support the following four new AVPs, which are represented in kbps. With the extended AVPs, speeds up to 4.2 Tbps are supported:

- Override-Extended-Max-Requested-BW-UL
- Override-Extended-Max-Requested-BW-DL
- Override-Extended-Guaranteed-Bitrate-UL
- Override-Extended-Guaranteed-Bitrate-DL

These new AVPs allows PCEF to set the Extended Maximum Bandwidth/Bitrate. These overrides shall be sent by PCRF using the Override Control AVP construct in a Credit Control Answer (CCA) or ReAuth-Request (RAR) message over Gx interface.

How it Works

The following table summarizes the Override and the corresponding Override-Extended AVPs. The fundamental difference between the Override and the corresponding Override-Extended AVPs is the unit in which the bitrate is specified. While the former specifies the bitrate in bit per second, the latter has the unit in kbps. Both being an unsigned-32 integer, the former supports a bandwidth limitation of ~4.2Gbps, while the latter supports bandwidth up to ~4.2Tbps.

Table 7: Override AVPs for which Override-Extended AVPs are defined

Override AVP (Unit = bits per sec)	Override-Extended AVP (Unit = kilobits per sec)
Override-Max-Requested-BW-UL	Override-Extended-Max-Requested-BW-UL
Override-Max-Requested-BW-DL	Override-Extended-Max-Requested-BW-DL
Override-Guaranteed-Bitrate-UL	Override-Extended-Guaranteed-Bitrate-UL

Override AVP (Unit = bits per sec)	Override-Extended AVP (Unit = kilobits per sec)
Override-Guaranteed-Bitrate-DL	Override-Extended-Guaranteed-Bitrate-DL

The following table summarizes how the AVPs are applied at P-GW. P-GW applies either Override or corresponding Override-Extended AVPs only and not the combination of both. P-GW simultaneously supports UEs with Override AVPs or Override-Extended AVPs.

Table 8: P-GW Application of Override and/or Override-Extended AVPs for a UE

CCA-I/CCA-U/RAR	Action at P-GW
All parameters received as Override AVP	Override parameters received in CCA-I applied and subsequently updated with params received in CCA-U. This legacy behavior applies to UEs for which the PCRF policy is unchanged.
All parameters received as Override-Ext AVP	Override-Extended parameters received in CCA-I, which is applied and subsequently updated with parameters received in CCA-U.
Some parameters received as Override and some others as Override-Ext	If the Parameter have both Override-MBR and Override-Extended-MBR AVPs, the extended override parameter is applied.
For a UE with Extended Parameter (s) applied once	If extended parameter (s) is applied once, then the subsequent updates happen only through extended override parameters. Any updates with override parameter shall be ignored. For example, If there are Override-Max-Requested-BW-UL AVP and Override-Max-Requested-BW-DL and their corresponding extended AVPS, “Override-Extended-Max-Requested-BW-UL” and “Override-Extended-Max-Requested-BW-DL,” when there is an update with Override-Max-Requested-BW-UL AVP and Override-Max-Requested-BW-DL, then the corresponding extended parameters (Override-Extended-Max-Requested-BW-UL) are applied already. If there are any subsequent updates to Override-Max-requested-BW_DL the updates will happen only through Override-Extended-Max-Requested-BW-UL. Any updates on Override-Max-Requested-BW-DL shall be ignored.

Monitoring and Troubleshooting

This section provides information on the show commands available to support this feature.

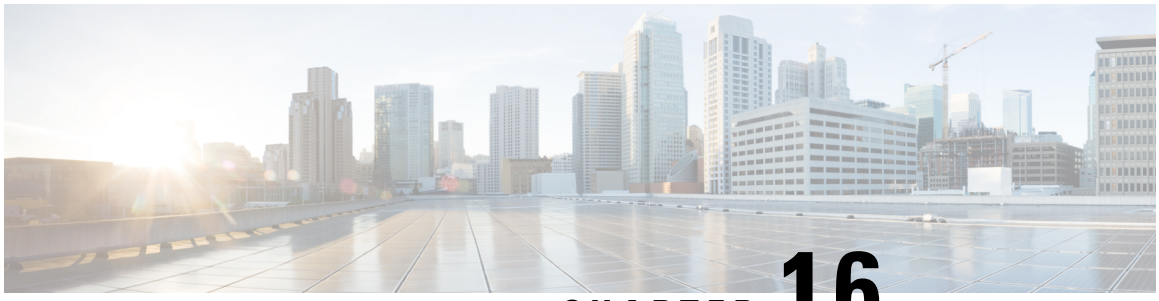
Show Commands and Output

show active-charging subscribers callid override-control

The output of this command includes the following fields:

Override Control:

- Extended MBR UL—This AVP defines the maximum bit rate in kbps that is allowed for the uplink direction.
- Extended MBR DL—This AVP defines the maximum bit rate in kbps that is allowed for the downlink direction .
- Extended GBR UL—This AVP defines the guaranteed bit rate in kbps that is allowed for Uplink direction. This AVP is included only for rules on dedicated bearers.
- Extended GBR DL—This AVP defines the guaranteed bit rate in kbps that is allowed for downlink direction. This AVP is included only for rules on dedicated bearers.



CHAPTER 16

Handling Core Dump

- Feature Summary and Revision History, on page 99
- Feature Changes, on page 100
- Command Changes, on page 101
- Performance Indicator Changes, on page 101

Feature Summary and Revision History

Summary Data

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

Revision History

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

Revision Details	Release
With this release, changes are made to the maximum number of core transfers and the format of the core filename.	21.20
First introduced.	Pre 21.2

Feature Changes

Previous Behavior:

- Maximum number of core transfers:

  When more than one process crashes, the simultaneous core file transfer was limited to a maximum of two at any given point of time and based on first come first serve basis.

  The maximum simultaneous core file transfer was increased from one to two cores as VPP crashes could induce simultaneous crashes in the boxer. Atleast one VPP full core has to be transferred at any time for debugging.

  Issue: When the process crashes in the 1st non-VPP -> 2nd non-VPP -> 3rd VPP sequence, the VPP core is discarded, transfer is based on first come first serve basis, and maximum of two cores are transferred.

- Core Filename:

  When the process crashes, the core file is transferred and stored with the filename compiled by its card number, CPU number, and hextime to make it unique and identifiable.

  Format: **crash-<cardno>-<cpuno>-<hextime>-core**

  Issue: When two or more processes crash at the same hextime along with the same card and CPU number, the generated cores are written to the same core filename causing corruption.

New Behavior:

- Maximum number of core transfers:

  The maximum number of core transfers are restricted to two in case of [1] and one in case of [2] with one non-VPP and one VPP always at any given point of time.

  1. Maximum core transfer to two: For cores generated in the below sequences, both 1st and 2nd cores are transferred.

     1st non-VPP -> 2nd VPP core

     1st VPP + 2nd non-VPP core

  2. Maximum core transfer to one: For cores generated in the below sequences, the 1st core is transferred and the 2nd core is discarded.

     1st VPP -> 2nd VPP core

     1st non-VPP -> 2nd non-VPP core

- Core File Name:

  For all cores, the filename is extended by adding the PID of the process to make it unique, even when two or more processes crash at the same hextime along with the same card and CPU number.

Format: **crash-<cardno>-<cpuno>-<pid>-<hextime>-core**

Customer Impact:

The scripts must be updated to the new format, if the coded core filename is in the old format.

Old format for core file: **crash-<cardno>-<cpuno>-<hextime>-core**

New format for core file: **crash-<cardno>-<cpuno>-<pid>-<hextime>-core**

Command Changes

Configuring VPP Core Transfer

Use the following configuration to enable or disable mandating VPP core transfer along with non-VPP.

```
configure
   [ no ] crash enable vpp-core-transfer
   exit
```

NOTES:

- **crash enable vpp-core-transfer**: Enables mandating VPP core transfer.
- **no crash enable vpp-core-transfer**: Disables mandating VPP core transfer.
- Default: Enabled

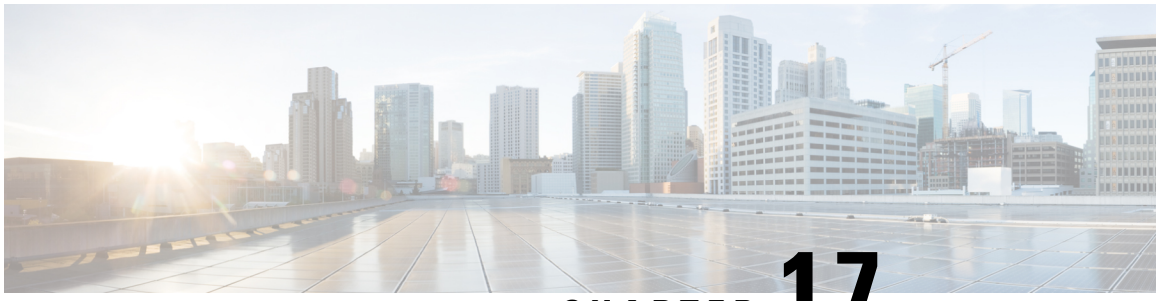
Performance Indicator Changes

show crash config

The existing **show crash config** command is enhanced to display the VPP core transfer status. The **Mandatory VPP Core Transfer** field displays whether VPP core transfer is enabled or disabled.

Sample Output:

```
# show crash config
URL                          : /hd-raid/cores
Disk Space Limit             : Not Configured
Rotate Core Files Limit      : 15 (default)
Core File Max-Size           : 4096 MB
Core File Compression        : gzip
Core Transmit Timeout        : 120 seconds
Core Obfuscation             : disabled
Async Core Transfer          : enabled
Mandatory VPP Core Transfer  : enabled
Critical Task                : enabled
#
```



CHAPTER 17

HSS and AuC Interworking Configuration Enhancement

- Feature Summary and Revision History, on page 103
- Feature Description, on page 104

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

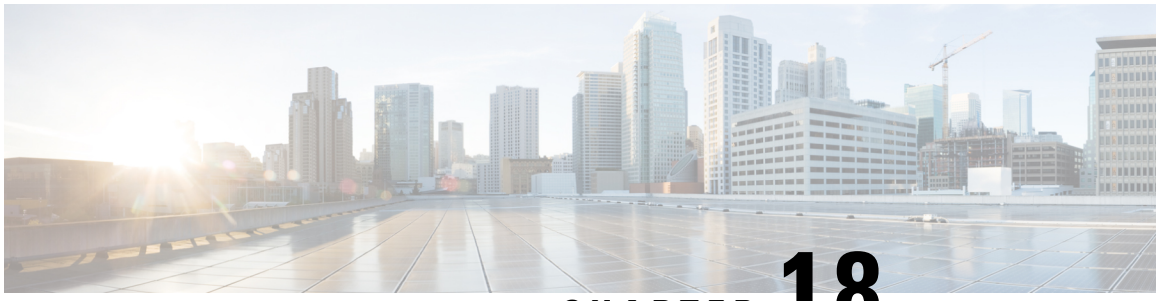
Revision Details	Release
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. This feature is fully qualified in this release.	21.20
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. **Important** 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 18

ICMPv6 Response for Fragmented Packets

- Feature Summary and Revision History, on page 105
- Feature Changes, on page 105

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

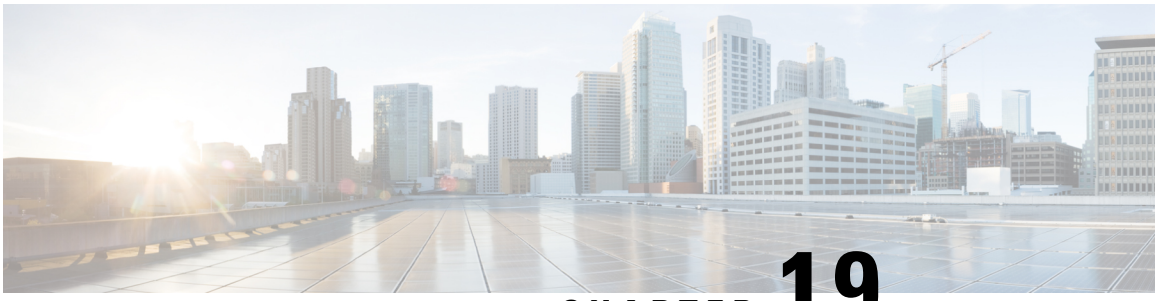
Revision Details	Release
First Introduced	21.20.7
In this release, P-GW supports Inner Fragmentation with VPP Non-CUPS Deployment.	21.15.x

Feature Changes

Previous Behavior: When an IPv6 packet with IP payload length is more than the data-tunnel-mtu value, ICMPv6 packet too big response is sent and the packet is dropped.

New Behavior: A fragmented IPv6 packet with IP payload length (for all fragments combined) of more than the data-tunnel-mtu value will not be dropped with ICMPv6 packet too big response. The packet is inner fragmented and forwarded with VPP non-CUPS deployment.

Customer Impact: Inner fragmentation is done overriding the **policy ipv6 tunnel mtu exceed notify-sender** under APN configuration.



CHAPTER 19

IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW

- Feature Summary and Revision History, on page 107
- Feature Changes, on page 108

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	*P-GW Administration Guide*

Revision History

Revision Details	Release
The StarOS 21.20.11 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW.	21.20.11
The StarOS 21.15.52 is enhanced with IPv4/IPv6 address encoding change in Flow-Description AVP under Application-Detection-Information AVP for APPLICATION-START event trigger from P-GW.	21.15.52

Feature Changes

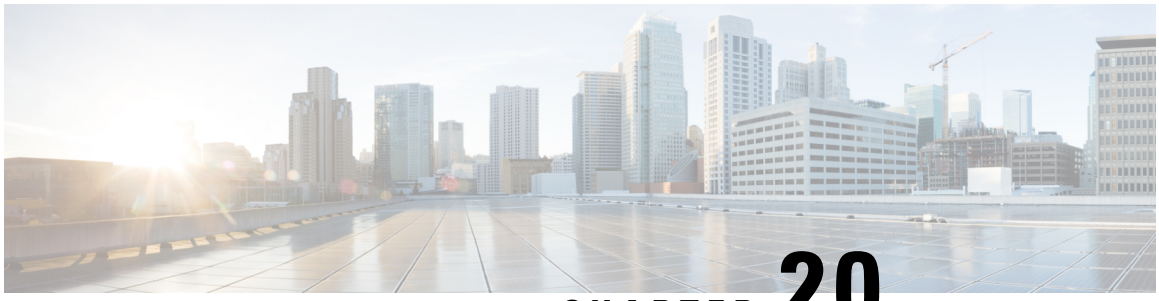
Previous Behavior: In CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF was encoded as:

- For ipv4 flows a netmask of /0 was used
- For ipv6 flows prefix length of 0 was used

New Behavior: In the release 21.15.52, in CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF is encoded as:

- For ipv4 flows a netmask of /32 is used
- For ipv6 flows prefix length of 128 is used

Customer Impact: PCRF receives flow description value with 32/128 netmask/prefix. If PCRF rejects the value, ADC over Gx will not work.



CHAPTER 20

Inner Fragmentation with VPP Non-CUPS Deployment

- Feature Summary and Revision History, on page 109
- Feature Changes, on page 110

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

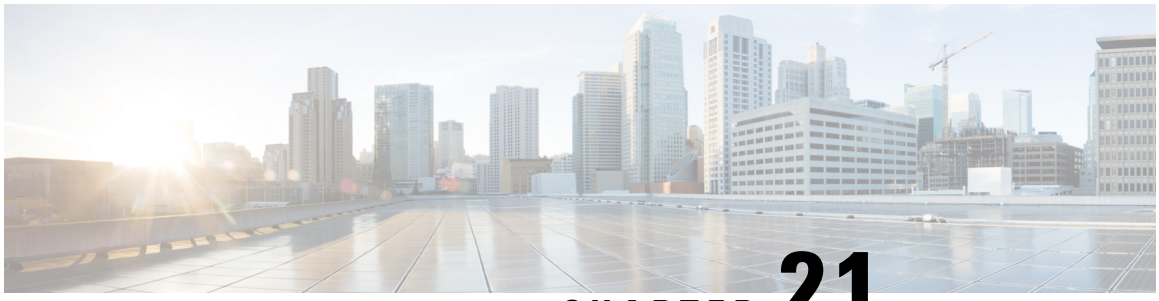
Revision Details	Release
In this release, P-GW supports Inner Fragmentation with VPP Non-CUPS Deployment.	21.20.7

Feature Changes

Previous Behavior: When VPP is enabled for non-CUPS deployment, GTP-U header, and transport layer length is not used to determine the inner fragmentation threshold while sending downlink packets towards S-GW/eNodeB. This resulted in outer fragmentation of downlink packets.

New Behavior: When VPP is enabled for non-CUPS deployment, GTP-U header, and transport layer length is used to decide the inner fragmentation threshold while sending downlink packets towards S-GW/eNodeB. This change is applicable for both IPv4 and IPv6 Packet Data Network (PDN) type.

Customer Impact: When VPP is enabled for non-CUPS deployment, there will be an overall reduction in downlink packets with outer fragmentation towards S-GW/eNodeB.



CHAPTER 21

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

- Feature Summary and Revision History, on page 111
- Feature Changes, on page 112
- Command Changes, on page 113
- Performance Indicator Changes , on page 113

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
In this release, CLI configuration is supported to control the RAI/SAI/CGI in Change Notification Request message for P-GW and S-GW services.	21.20.22
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

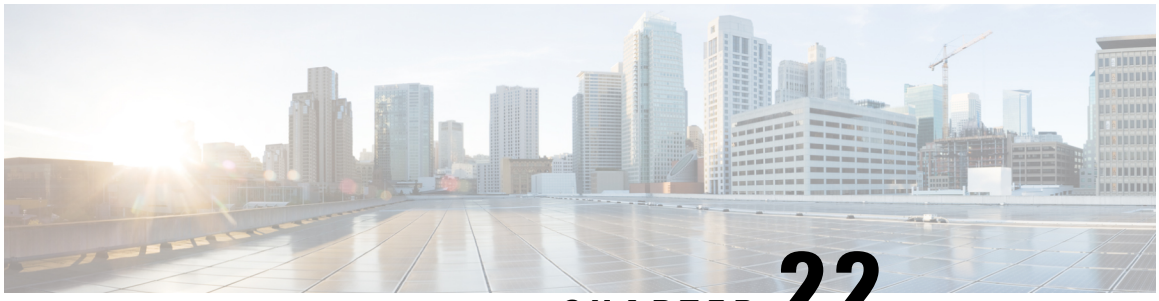
This command has been modified to display the following output

```
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 22

MME Bearer Request Message During Handover Process

- Feature Summary and Revision History, on page 115
- Overview, on page 116
- How It Works, on page 116
- Updating Bearer Response During 3G to 4G GnGp HO and TAU Process, on page 117
- Show Commands and Outputs, on page 117

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, MME supports: • EGTPC buffering when UBR arrives between Create Session Request and Response sequence. • If dedicated bearer information is present both the delayed ERAB and MBC procedures are triggered allowing the remaining bearer details from the stored UBR to be sent to the UE.	21.21
First introduced	21.20

Overview

In MME, there are Key Performance Index (KPI) failures seen in the GTPv2 Update Bearer Request messages received during the 3G-to-4G Handover/TAU procedures.

To overcome this issue, a globally enabled flag is used as an entry in the MME Service to improve the KPI success rate of GTPv2 Update Bearer Request failures during the following 3G-to-4G Handover/TAU procedures:

- Gn/Gp SGSN to MME Tracking Area Update procedure
- Gn/Gp SGSN to MME combined hard handover and SRNS relocation procedure

When enabled, if an Update Bearer Request (UBR) message is received during the Gn/Gp procedures the UBR is stored, and an Update Bearer Response with “Request Accepted” cause code 16 is sent back to the SGW. On completion of the Gn/Gp procedure, if a UBR is stored the MME (depending on other events) sends a delayed E-RAB Modify Request message to the eNB using the QoS details in the stored UBR.

Note The delayed E-RAB Modify procedure is non-3GPP compliant behavior. This procedure is non-3GPP compliant and is not designed to be enabled dynamically. If configured dynamically, it could interfere with UE's in mid bearer modification procedures and cause adverse affects. Hence, this feature should only be enabled during system start-up from saved CLI configuration.

How It Works

If an update bearer request is received during a Gn/Gp Handover /TAU procedure instead of discarding the message (if it arrives in between a Create Session Request/Response sequence) or responding with a “Temporarily rejected due to handover/TAU/RAU procedure in progress” cause code 110, a successful response with cause code 16 is sent, and the UBR is stored for later E-RAB modification processing.

The new feature is active through the CLI flag. After receiving an Update Bearer Request, MME sends a bearer response with Cause Code 16 as "Request Accepted" to the SGW and then stores the Update Bearer Request for processing it later once the 3G-to-4G Handover/TAU procedure is completed.

Once the Gn/Gp Handover/TAU procedure is completed, if there is no "HSS Initiated Subscribed QoS Modification" procedure-based modify bearer command to process, a delayed E-RAB Modify procedure is performed towards the eNB/UE. It ensures that the eNB/UE's QoS parameters are in sync with the MME/SGW/PGW using the information in the stored update bearer request. If the modify bearer command message fails (either via a modify bearer failure Indication or re-transmission timeout) then the delayed E-RAB modify procedure is performed to ensure the eNB/UE's QoS parameters are in sync with the MME/SGW/PGW.

Important If dedicated bearer information is present both the delayed ERAB and MBC procedures are triggered allowing the remaining bearer details from the stored UBR to be sent to the UE.

If any error occurs during the delayed E-RAB Modify procedure towards the eNB/UE, the MME performs a "UE Context Release Command" procedure towards the eNB/UE, to rectify the error situation.

Updating Bearer Response During 3G to 4G GnGp HO and TAU Process

Use the following configuration to update the bearer response during 3G to 4G GnGp HO and TAU process:

```
configure
   context context_name
     mme-service mme_service_name
        [ no ] buffer-ubreq-from-3g-to-4g
end
```

Show Commands and Outputs

show update-bearer-request-stats

The output of this command displays the update bearer Response Cause Code (CC16) statistics during HO/3G-4G TAU:

The output of this command includes the following fields:

show mme-service *mme_service_name*

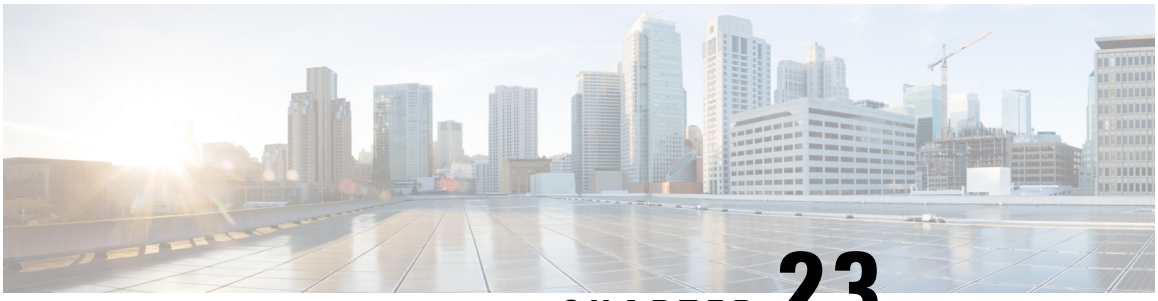
The output of this command displays the configuration of all MME services:

- **buffer-ubreq-from-3g-to-4g** – Displays the enabled and disabled bearer response during 3G-4G GnGp HO and TAU process.

show mme-service all

The output of this command displays the configuration of all MME services:

- **buffer-ubreq-from-3g-to-4g** – Displays the enabled and disabled bearer response during 3G-4G GnGp HO and TAU process.



CHAPTER 23

Multiple Customized PCO Support

- Feature Summary and Revision History, on page 119
- Feature Description, on page 120
- How it Works, on page 120
- Configuring PCO, on page 121
- Monitoring and Troubleshooting, on page 123

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Support is added for additional Protocol Configuration Options, Custom6 through Custom10.	21.26

Revision Details	Release
Support is added to display a confirmation message before deleting or modifying an existing Container ID value in the Global Configuration mode.	21.24
Enhanced Protocol Configutaion Options (ePCO) support is added with the existing new operator defined PCO for UWB Indicator.	21.20.22
First introduced.	21.20.16

Feature Description

With the multiple PCO support feature, P-GW and GGSN sends customized Protocol Container Options (PCOs) to MS GTP messages. Custom1 is an existing PCO and its Container ID value is FF00H.

P-GW and GGSN support PCOs ranging from Custom1 through Custom10.

The global PCO container IDs are modified during runtime. This modification affects only the new subscriber sessions and doesn't affect the existing subscriber sessions. The PCO container IDs ranging from FF03 to FFFF are configurable.

Operator Defined PCO for Ultra Wideband (UWB) Indicator

P-GW supports either Protocol Configuration Options (PCO) or Enhanced Protocol Configuration Options (ePCO) based on the EPCOSI indication bit received from an UE in Create Session Request and Modify Bearer Request.

If the EPCOSI bit is set, P-GW sends PCO containers in the ePCO IE. If the EPCOSI bit isn't set, then P-GW sends PCO containers in PCO IE.

Note 3G (UMTS) PCO notification to the UE is added to support the Gn or Gp mode. GGSN doesn't support ePCO IE.

How it Works

This section describes the updation of PCO values using the Gx and Gy interfaces. The term Gateway (GW) is interchangeably used in this chapter for P-GW and GGSN.

Updating PCO Value Using Gx Interface

This section describes the procedure to update PCO values using the Gx interface.

- The Policy and Charging Rules Function (PCRF) sends a request to activate the predefined rules.
- If the activation is successful and if the charging action is configured for PCO, then the retrieved value is sent to the UE.

- If the predefined rule creation is performed during session creation (CCA), then the retrieved PCO is sent to the UE in Create Session Response for P-GW and Create PDP Context Response for GGSN.
- If the predefined rule activation is sent in the middle of the session (CCA-U), then the retrieved PCO is sent to the UE with the next message.
- The PCRF sends a request to deactivate predefined rules.
- If the removal of predefined rules is successful and if PCO is configured for charging action, then the configured value in the APN is returned to UE with the next message.
- If multiple predefined rules are enabled, then the last charging action configured for PCO, in the order of rules sent, is considered as valid and Session Manager is updated with the value.

Note Ensure that the last predefined rule has the correct PCO value for this scenario. The remaining requested rules will follow the regular predefined rule activation procedure.

Updating PCO Value Using Gy Interface

This section describes the procedure to update PCO values using the Gy interface.

- The Online Charging System (OCS) sends a filter ID to enable the corresponding post-processing dynamic rule.
- If the rule activation is successful and if the associated charging action is configured for PCO, then the retrieved value is sent to the Session Manager through the Session Update Indication event.
- The GW sends the PCO value to UE.
- If the OCS sends multiple filter IDs, then the charging action associated with the last filter ID is used for PCO.
- The CRF sends a request to deactivate the predefined rules.
- On successful removal of the predefined rules, if charging action is configured for PCO, then a default PCO value under APN will be returned to UE with the next message.

Configuring PCO

This section describes the PCO configuration. CLI modifications are not permitted when calls are active for APN Configuration mode and Global Configuration mode, but modifications are permitted for active-charging service.

Configuring PCO in Charging Action Mode

Use the following sample configuration to configure multiple PCOs in the ACS Charging Action Configuration Mode.

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

```
      charging-action action_name
         { pco-custom1 | pco-custom2 | pco-custom3 | pco-custom4 |
pco-custom5 | pco-custom6 | pco-custom7 | pco-custom8 | pco-custom9 |
pco-custom10 } custom_value
         end
```

NOTES:

- **pco-custom1 - pco-custom10** *custom_value*: Configures multiple operator-specific PCOs. custom_value must be an integer in the range of 0-255.

Configuring Custom1 PCO in APN Configuration Mode

Use the following sample configuration to configure Custom1 PCO in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-option custom1 [ ue-requested ]
         end
```

NOTES:

- **pco-option custom1**: Configures operator defined PCO container custom1 mode. By default, its container ID value is fixed to 0.
- **ue-requested**: Configures to include Custom PCO Options in PCO IE, only when it requested by UE.
- **no**: Removes custom1 PCO configuration in the APN Configuration mode.

Configuring Multiple PCOs in APN Configuration Mode

Use the following sample configuration to configure multiple PCOs in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-options { { custom1 | custom2 | custom3 | custom4 |
custom5 | custom6 | custom7 | custom8 | custom9 | custom10 } [ ue-requested
 value custom_value | value custom_value ] }
         end
```

NOTES:

- **custom1 - custom10**: Configures APN to include custom PCO options in PCO IE.
- **ue-requested**: Configures to include custom PCO Options in PCO IE, only when it is requested by UE.
- **value** *custom_value* : Configures the default container value of custom PCO. custom_value must be an integer in the range of 0-255.
- **no**: Removes PCO configuration in the APN Configuration mode.

Configuring PCO Container ID in Global Configuration Mode

Use the following sample configuration to configure multiple PCOs in the Global Configuration mode.

```
configure
  [ no ] pco-options { custom2 | custom3 | custom4 | custom5 | custom6 |
 custom7 | custom8 | custom9 | custom10 } container-id container_id_value
  end
```

NOTES:

- **pco-options { custom2 - custom10}**: Configures custom PCO options in PCO IE.
- **container-id** *container_id_value*: Configures the operator defined container ID and the value ranging from FF03 to FFFF.
- **no**: Removes PCO container ID configuration in the Global Configuration mode.

Note The custom1 container ID is not configurable in the Global Configuration mode as its container value is fixed to FF00H.

Note If you delete or modify an existing container ID value for an ongoing session, it affects only the new sessions and does not affect the ongoing or existing sessions.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging charging-action all

The output of this command is enhanced to display the following field.

Table 9: show active-charging charging-action all Command Output Descriptions

Field	Description
PCO-Custom1-10 value	Indicates the action value for multiple operator-specific PCOs. The value can range from 1 to 10.

show active-charging sessions full all

The output of this command is enhanced to display the following fields.

Table 10: show active-charging sessions full all Command Output Descriptions

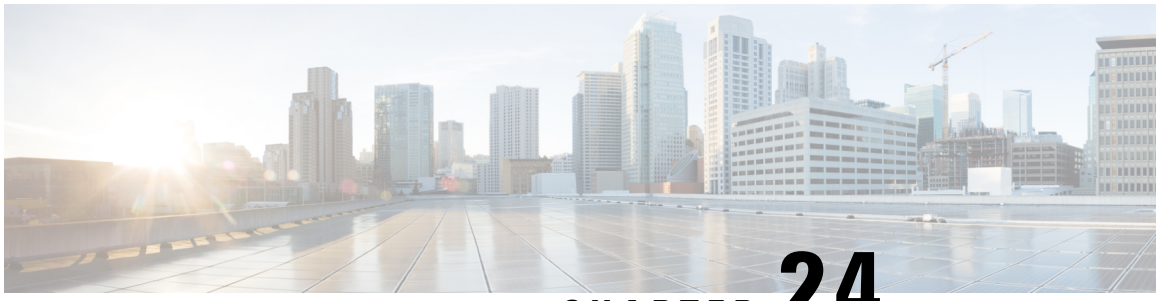
Field	Description
custom	Indicates Operator specific custom option.
Value	Indicates the value used for sending in custom PCO container.
Interface	Indicates the interface such as Gx. Gy or n/a based on the following conditions: • Gx: The charging rule is applied from the Gx interface that has custom PCO value. • Gy: The charging rule is applied from the Gy interface that has custom pco value. • n/a: The configured PCO value which is applied from APN profile.

show apn all

The output of this command is enhanced to display the following fields.

Table 11: show apn all Command Output Descriptions

Field	Description
Custom1-10 value	Specifies the action value for multiple operator-specific PCOs. The value can range from 1 to 10.
UE-Requested	Specifies PCO to the UE, which requested for new PCO option.



CHAPTER 24

5GS Interworking using N26 Interface Support

This chapter describes the following topics:

- Feature Summary and Revision History , on page 125
- Feature Description, on page 126
- How it Works, on page 128
- Configuring N26 Interface for MME, on page 142
- Monitoring and Troubleshooting, on page 145

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
Support is introduced for dynamic selection mechanism to select PGW-C+SMF and peer-AMF.	21.25

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

5GS interworking with N26 interface, the User Equipment (UE) operates in the 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 MME.

MME uses either the static or dynamic mechanism to select PGW-C+SMF and peer-AMF.

MME supports the following interworking procedures with N26 interface:

- Attach
- EPS to 5GS Mobility Registration
- 5GS to EPS Idle Mode Mobility
- 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 the 5GS interworking 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 a GUMMEI in Access Stratum signalling mapped from the 5G-GUTI and is indicated as **Mapped from 5G-GUTI**.
- **Handover Type**— This indicates the type of handover that was triggered in the source side. The Handover type IE currently supports **EPSto5GS** and **5GStoEPS** type.
- **Handover Restriction List**— This supports **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**—This supports **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 theUE 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 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 type and contains a bit mask where each bit when set to 1 indicates a restriction.

S11 (SGW) Interface:

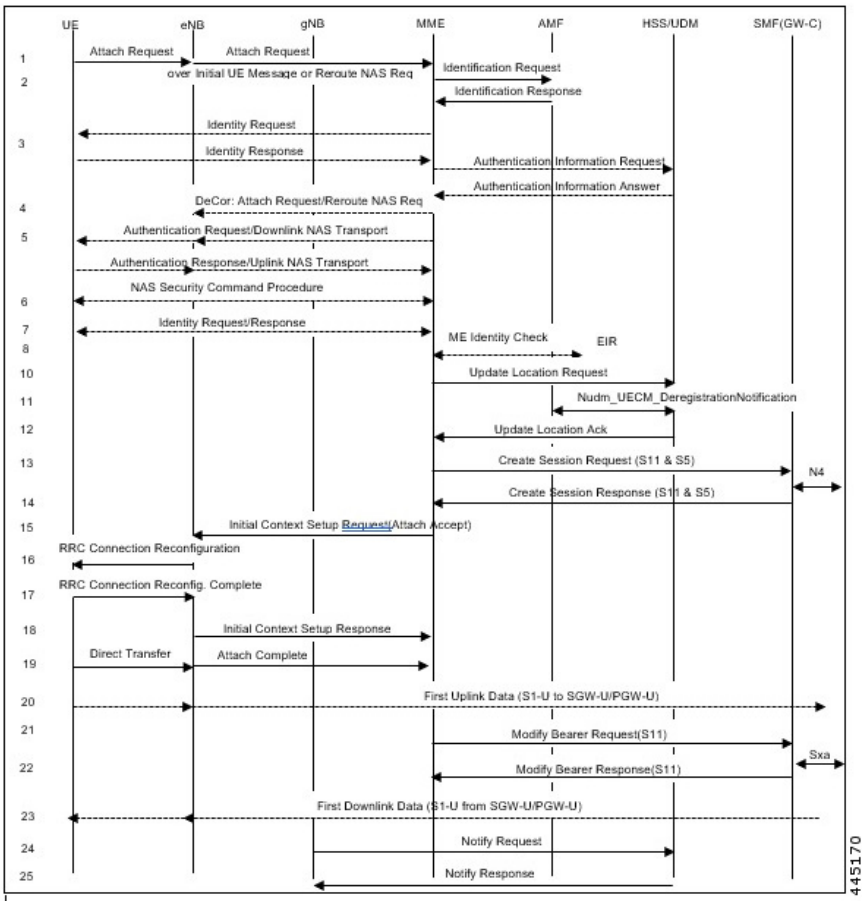
- **Indication Flag** — MME supports 5GSIWKI (5GS Interworking Indication) and REPREFI (Return Preferred Indication) flags.

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 5: E-UTRAN Initial Attach Call Flow



E-UTRAN Initial Attach Procedure

The following table describes 5GS to EPS attach procedure.

Table 12: E-UTRAN Initial Attach Procedure

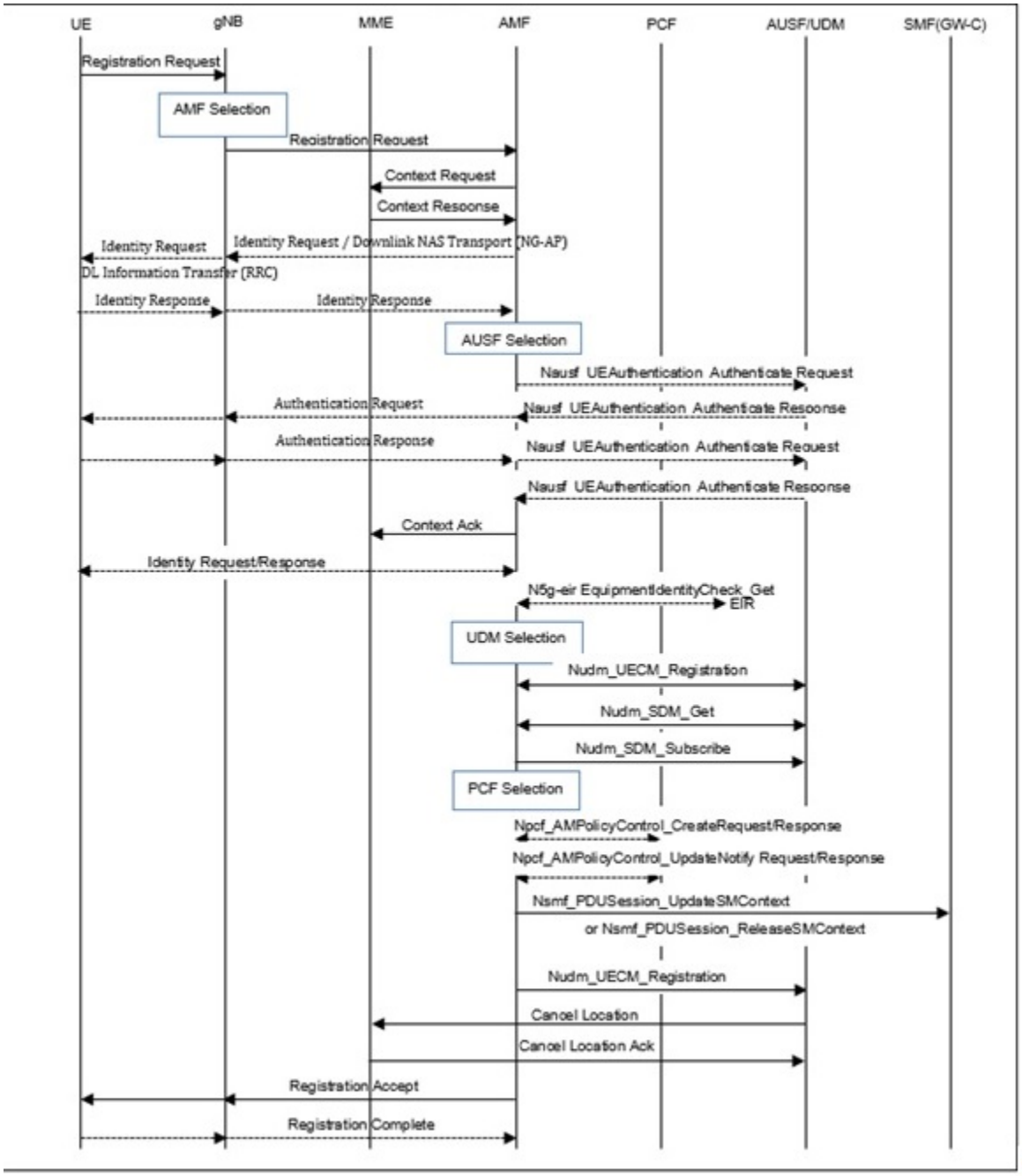
Step	Description
1	Attach Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability IE**. • UE includes GUMMEI in the S1-AP message and. indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped from 5G-GUTI 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**.
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 DNS or local Static 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 based on the following mechanisms: • Static configuration • Dynamic DNS configuration
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.

Step	Description
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 6: EPS to 5GS Mobility Registration Call Flow



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

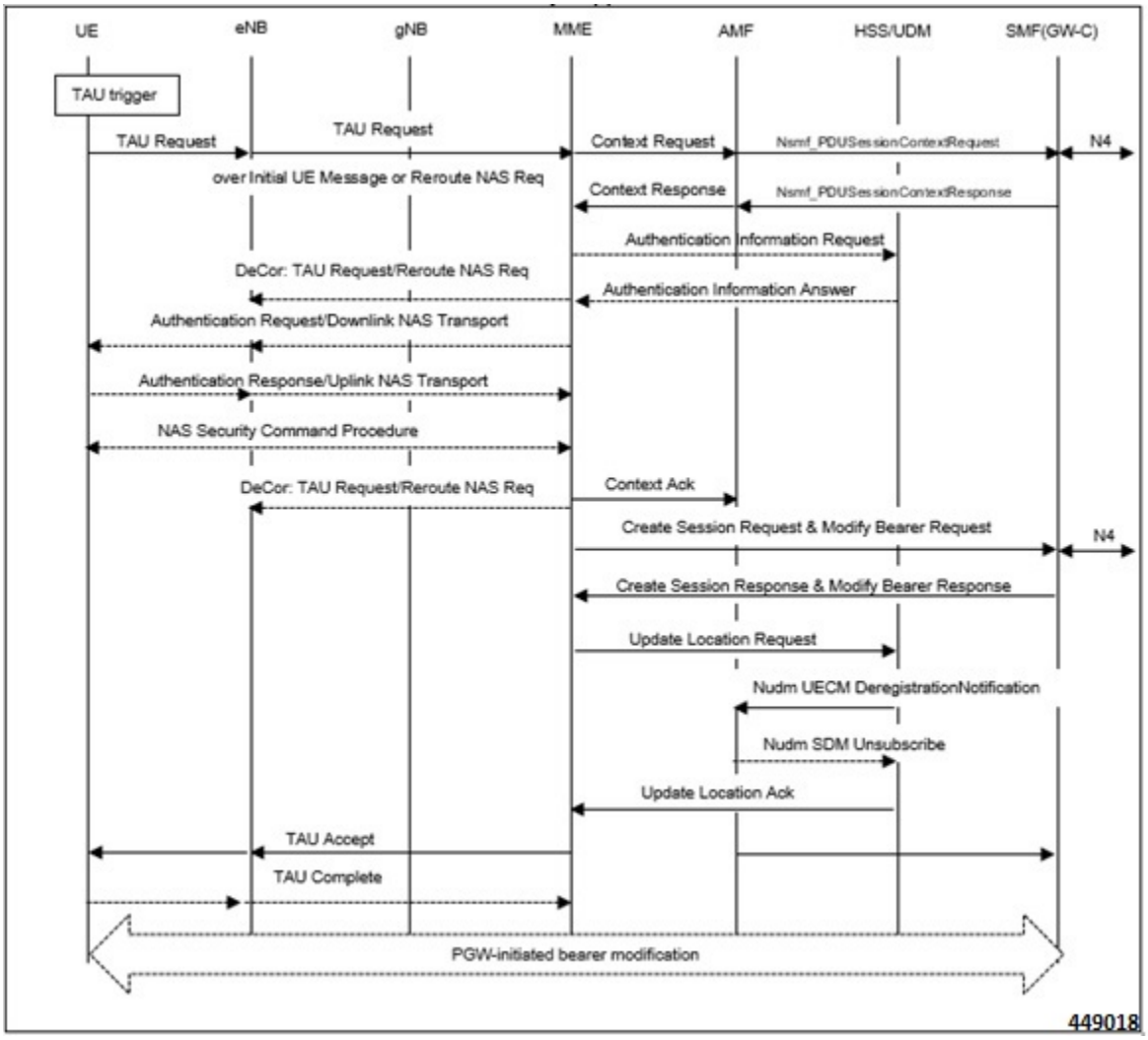
Table 13: EPS to 5GS Mobility Registration Procedure

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 7: 5GS to EPS Idle Mode Mobility Call Flow



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 14: 5GS to EPS Idle Mode Mobility Procedure

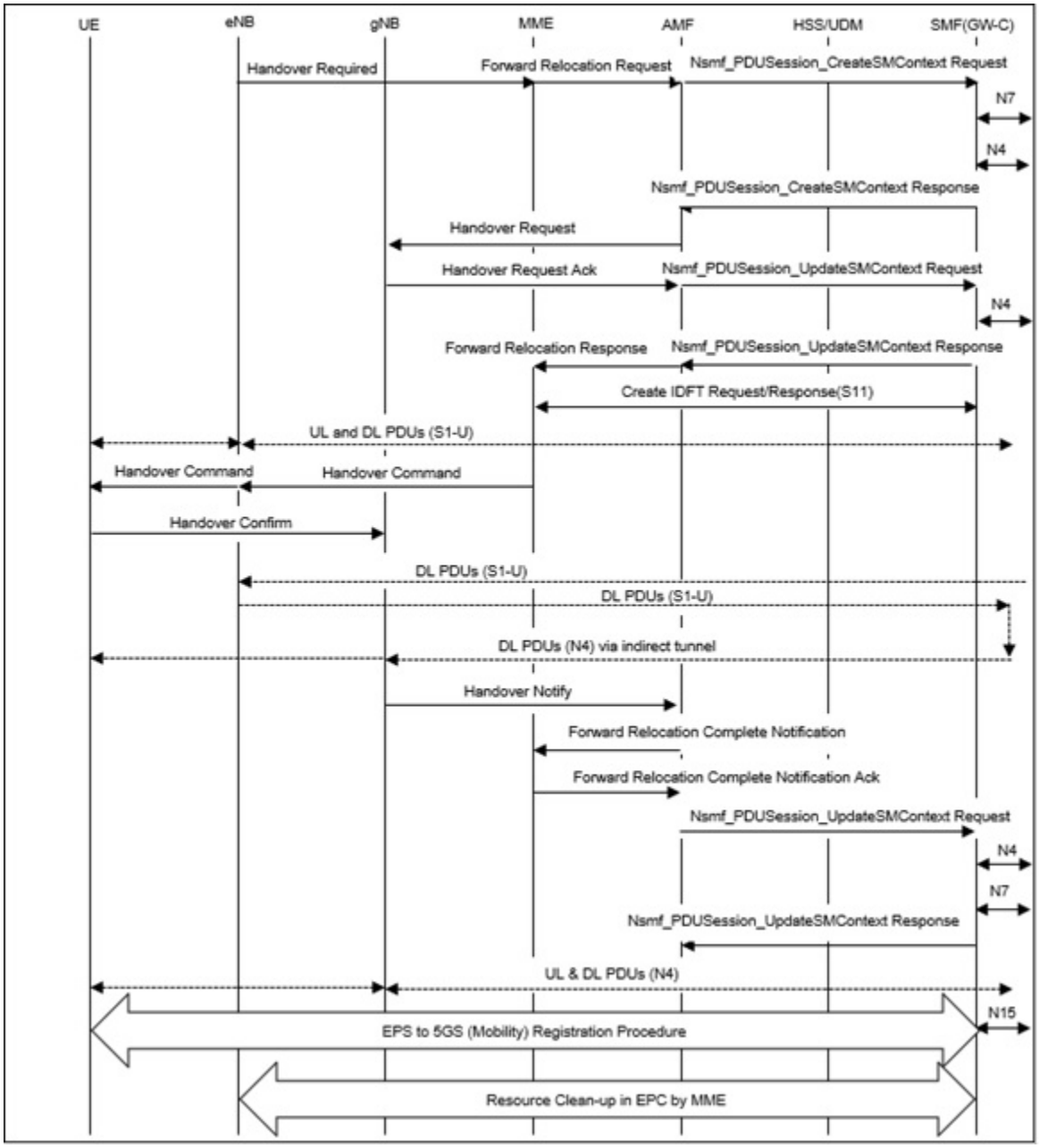
Step	Description
1	Tracking Area Update Request is carried over Initial UE Message with following conditions: • UE includes N1-mode capability in the **UE Network Capability** IE. • UE includes GUMMEI in the S1-AP message and indicates that GUMMEI is Mapped from 5G-GUTI. • UE includes a GUTI, mapped 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 DNS or local Static 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 8: EPS to 5GS Handover Call Flow



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.

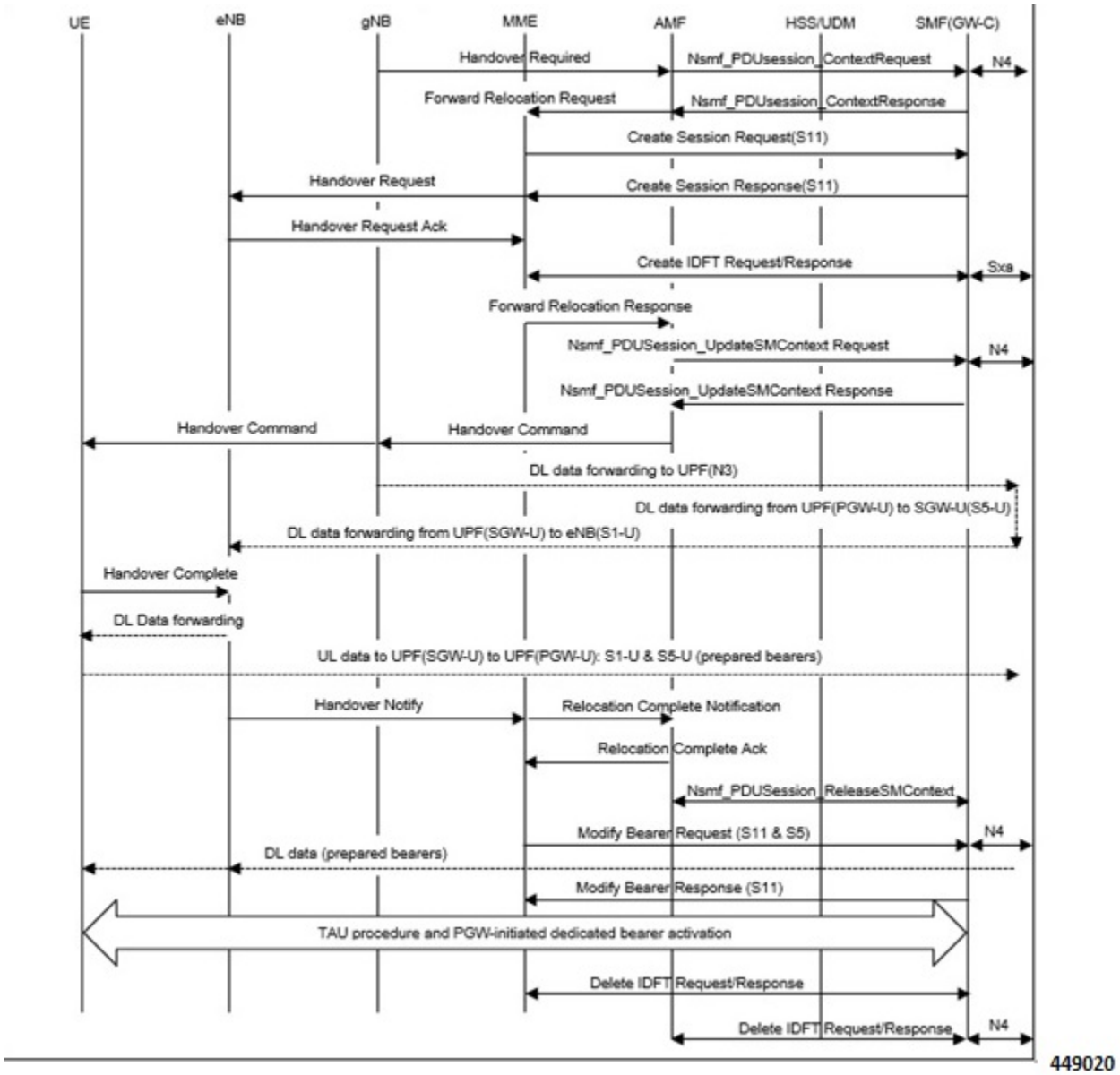
Table 15: EPS to 5GS Handover Procedure

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 DNS or local Static 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 9: 5GS to EPS Handover Call Flow



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

Table 16: 5GS to EPS Handover Procedure

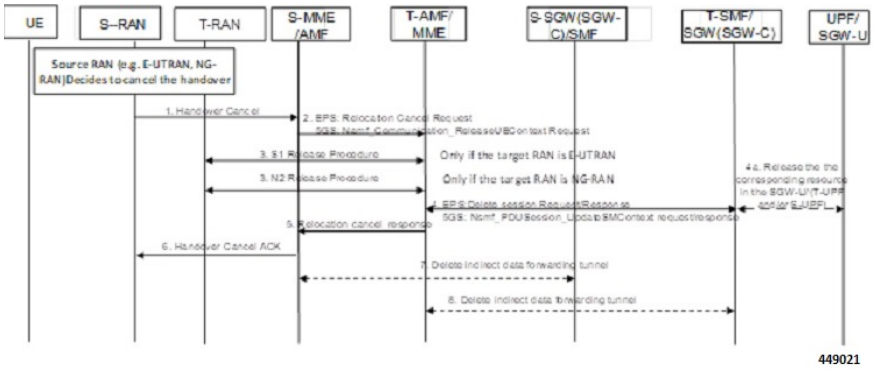
Step	Description
1	MME receives Forward Relocation Request message from AMF. AMF shall include **Return preferred Indication** to indicate preferred return of the UE to the 5GS PLMN at a later access change to a 5GS shared network. AMF includes reserved S-GW address and TEID for both the control plane 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 10: EPS to 5GS Handover Cancel Call Flow



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

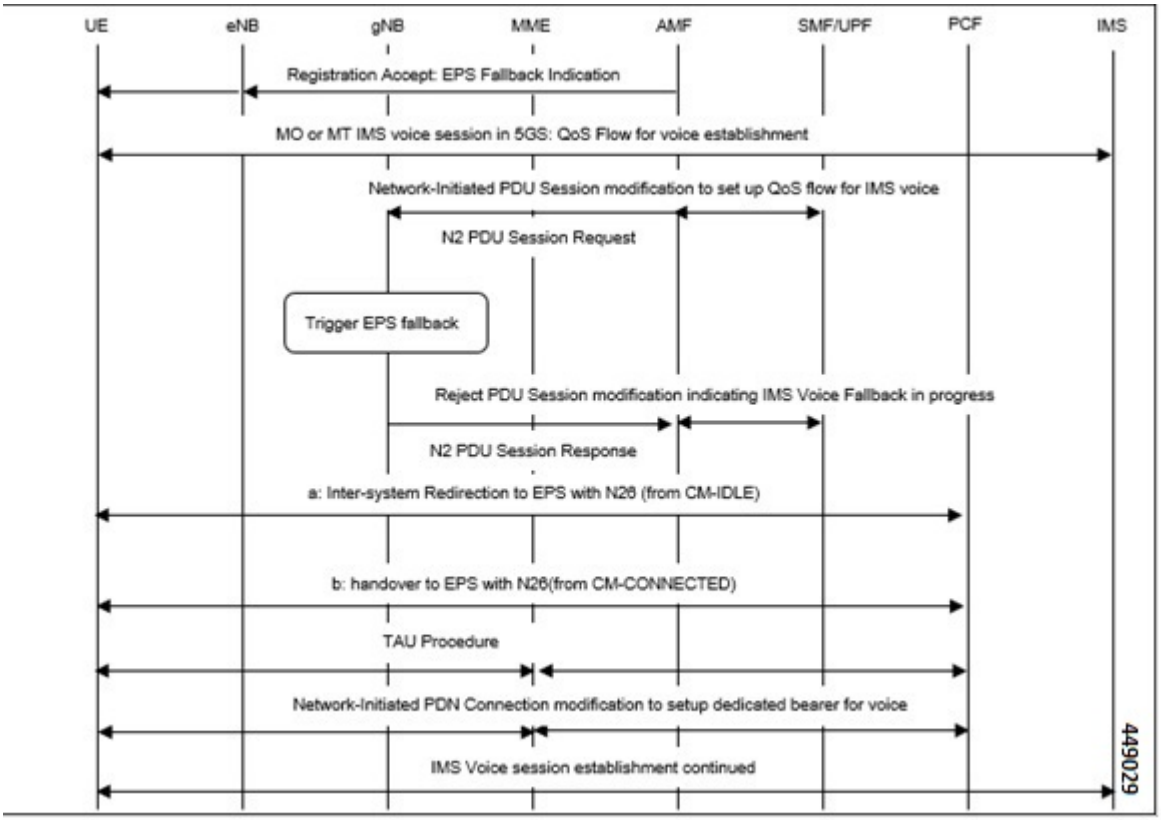
1. MME receives **Relocation Cancel Request** from AMF.
2. MME triggers release of resources towards target RAN node. The target RAN node releases the RAN resource allocated for the handover.
3. MME sends the **Delete session request** (IMSI, Relocation Cancel Indication) to the S-GW/S-GW-C. Based on 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 11: EPS Fallback for IMS Voice



Combined PGW-C and SMF Selection Procedure

MME supports DNS and Static PGW-C/SMF combined Gateway selection. You can configure PGW-C+SMF in MME Service and in APN profile configuration commands for static gateway selection. 5GSIWKI is set when combined PGW-C/SMF node is selected.

The following steps explain the static based combined P-GW-C/SMF selection procedure and how the fallback to the next available option happens if the selection fails:

1. MME chooses Combined PGW-C/SMF node that supports UE usage type and collocation with S-GW.
2. If step 1 fails, MME selects the Combined PGW-C+SMF node that supports UE usage type.
3. If step 2 fails, MME selects the Combined PGW-C+SMF node that supports collocation with S-GW.

4. If step 3 fails, MME selects the Combined PGW-C+SMF node.
5. If step 4 fails, MME selects the gateway based on UE usage type and standalone PGW collocation.
6. If step 5 fails, MME selects the standalone PGW that supports UE usage type.
7. If step 6 fails, MME selects the gateway that supports standalone PGW collocation.
8. If step 7 fails, MME selects any gateway from all configured entries.

The following steps explain the DNS-based combined PGW-C+SMF selection procedure and how fallback occurs to the next available option if the selection fails:

1. MME selects a gateway matching the UE Usage type, DCNR, and SMF network capability.
2. If step 1 fails, MME selects the gateway matching the DCNR and SMF network capability.
3. If step 2 fails, MME selects the gateway matching the UE usage type and SMF network capability.
4. If step 3 fails, MME selects the gateway matching the SMF network capability.
5. If step 4 fails, MME selects the gateway matching the UE usage type and DCNR network capability.
6. If step 5 fails, MME selects the gateway matching the DCNR network capability.
7. If step 6 fails, MME selects the gateway matching the UE usage type.
8. If step 7 fails, MME selects the gateway matching the default service parameter.
9. If step 8 fails, MME selects the gateway based on local static configuration.

Note The above steps are only for reference purpose based on probable combination where UE/MME supports UUT, DCNR and SMF capability. The selection order varies/depends based on the DNS response, UE capability and MME configuration.

Limitations

This section describes the known limitations for the N26 interface functionality:

- Configuration Transfer Tunnel message is not supported.
- Feature-specific optional IEs are not supported. For example, Extended Trace Information IE.
- Default EGTP service is used for GTPv2 messages on N26 interface.
- A maximum of 32 peer-AMF entries can be configured for GUAMI or TAI configuration.
- NBIoT and CIOT optimization is not supported.
- PGW-C+SMF selection for Emergency Attach or Emergency PDN is not supported.

Supported Standards

The N26 feature support is compliant 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
- 3GPP 29.303 version 15.5.0 - Domain Name System Procedures

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.

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.

Configuring DNS Peer AMF

Use the following sample configuration to configure peer-AMF selection using the DNS interface:

```
configure
   mme-service mme_svc_name
      dns peer-amf
      end
```

NOTES:

- **dns peer-amf**: MME sends a DNS query to the DNS server for selecting AMF.

Note The **dns pgw** command under MME Service and Call Control Profile can be reused to configure DNS to select the PGW-C+SMF 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 mme-service statistics 5gs-interworking

Table 17: show mme-service statistics 5gs-interworking Command Output Descriptions

Field	Description
Attach Request Rcvd	Displays the number of Attach Request messages received with UE advertising N1 Mode support.
TAU Request Rcvd	Displays the number of TAU Request messages received with UE advertising N1 Mode support.
SMF-Combined	Displays the number of times P-GW DNS selection procedures performed with DNS RR including the N1 Mode network capability.
NR Capable	Displays the number of times P-GW DNS selection procedures performed with DNS RR including the NR network capability.
Common	Displays the number of times P-GW DNS selection procedures performed with DNS RR excluding the N1 Mode network capability.
PGW Local Config	Displays the number of times P-GW selection procedures performed with locally configured P-GW address, without considering the N1 Mode network capability.

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 reselects AMF as part of the 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 the 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	Displays the total number of attempted outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-mob-4gto5g-n26-success	Displays the total number of successful outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface
out-mob-4gto5g-n26-failures	Displays the total number of failed outbound relocation using EPS to 5GS Idle mode mobility procedure in N26 interface.
out-ho-4gto5g-n26-attempted	Displays the total number of attempted outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-success,	Displays the total number of successful outbound relocation using EPS to 5GS Handover procedure in N26 interface.
out-ho-4gto5g-n26-failures	Displays the total number of failed outbound relocation using EPS to 5GS Handover procedure in N26 interface.
in-mob-5gto4g-n26-attempted	Displays the total number of attempted inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-success	Displays the total number of successful inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-mob-5gto4g-n26-failure	Displays the total number of failed inbound relocation using 5GS to EPS Idle mode mobility procedure in N26 interface.
in-ho-5gto4g-n26-attempted	Displays the total number of attempted inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-success	Displays the total number of successful inbound relocation using 5GS to EPS Handover procedure in N26 interface.
in-ho-5gto4g-n26-failures	Displays the total number of failed inbound relocation using 5GS to EPS Handover procedure in N26 interface.

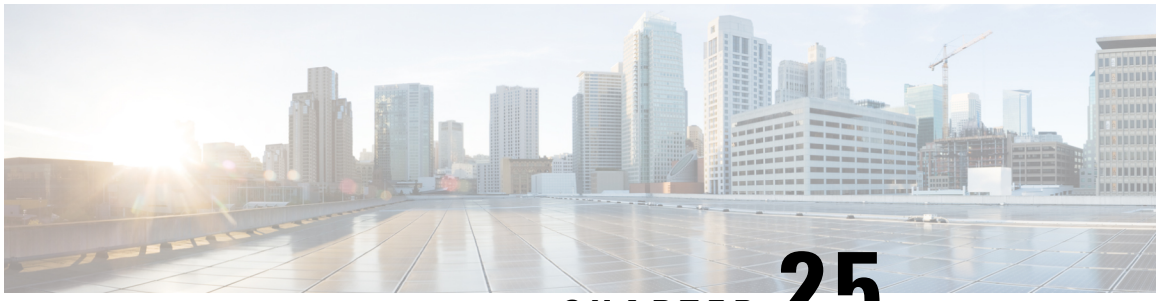
Counters	Description
mme-decor-ue-usage-type-src-peer-amf	Displays the the number of MME subscriber sessions, where UE usage type was obtained from peer AMF as part of handover.
n1-mode-atttach-req	Displays the total number of Attach Requests received with N1 mode supported.
n1-mode-tau-req	Displays the total number of TAU Requests received with N1 mode supported.
n1-mode-dns-pgw-selection-smf	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.
n1-mode-dns-pgw-selection-nr	Displays the number of times P-GW DNS selection procedures are performed with DNS RR including the NR network capability.
n1-mode-dns-pgw-selection-common	Displays the number of times P-GW DNS selection procedures are performed with DNS RR excluding the N1 Mode network capability.
n1-mode-dns-pgw-selection-local	Displays the total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the N1 Mode network capability.

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.

Counters	Description
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 25

Online Charging Support without Waiting for Credit Control Answer

- Feature Summary and Revision History, on page 151
- Feature Description, on page 152
- How it works, on page 152
- Configuring Online Response Required Parameter, on page 153
- Monitoring and Troubleshooting, on page 153

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release new CLI for online response is added under the APN level and the feature is fully qualified for this release.	21.20.3
First introduced.	21.20

Revision Details	Release
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.	

Feature Description

For 5G subscribers, all rating groups and all bearers require to have the online charging flag set to "yes" and a Gy session established to create billing records. In order not to delay a call setup or block data flow for APNs/bearers/rating groups, P-GW supports a new feature to allow charging to be done over Gy but not delay session setup or hold up data. This will mimic 5G-ChF (Charging Function) behavior through OCS.

Policy and Charging Rules Function (PCRF) indicates through the following two AVPs, which bearers need the above behavior:

- Charging Level AVP –**Online-Response-Required** AVP is defined at the Charging level and is available only when the online charging is enabled. This AVP controls if the Session Create Response must "Wait" for CCA or not.
- Override Control AVP–**Online-Response-Required** is defined at the Override Control level and is available only when online charging is enabled. This AVP overrides the new charging AVP that is received from Policy and Charging Rules Function (PCRF).

How it works

The following call flow and procedure describes how the CCR is triggered during session create.

Table 18: Procedure

Step	Description
1	The P-GW receives Session Create Request.
2	Checks the charging AVPs received from PCRF.
3	In the PCRF, either **OnlineResponseRequired** or **Override-OnlineResponseRequired** AVP is activated in the Gx Interface at charging level or Override level with an option to WAIT to DONT_WAIT. The following action happens based on the Rule selection: • If the Session Create Request is received with WAIT rule indicating OnlineResponseRequired, Session Create response waits for CCA-I over Gy interface before sending the Session Create response. • If the Session Create Request is received with DONT_WAIT rule, Session Create response does not wait for CCA-I response.
4	P-GW sends Session Create Response based on the new AVP.

The following scenarios describe how the data flow is processed:

- If there is no quota the P-GW will Assume Positive for that flow.
- If there is Quota:
  - When the Charging level AVP specifies DONT_WAIT, then there is no traffic drop.
  - When the Quota expires, P-GW will Assume positive. Except for the Error Code 4012, if there is any error code P-GW triggers Assume Positive

Configuring Online Response Required Parameter

Use the following commands to configure the Online Response required AVP in the APN configuration mode.

```
configure
   context  context_name
      apn apn_name
         bearer-control-mode  mixed
           use-gx-avp-online-response-required
           no  use-gx-avp-online-response-required
            end
```

Notes:

- **apn** : Specifies the Access Point name.
- **bearer-control-mode mixed** : This keyword indicates that the bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well. By default it is diabled.
- **use-gx-avp-online-response-required**: Enables P-GW to function according to the behavior requested in Gx AVP OnlineResponseRequired or override-OnlineResponseRequired.
- **no**: Disables the OnlineResponseRequired or override-OnlineResponseRequired feature for the specified APN.

Monitoring and Troubleshooting

Show Commands and Output

show-active-charging subscribers

The output of the above command has been enhanced to display the new parameter which shows the online response required rule definition chosen as Don't Wait. For example:

```
Override Control :
  Rule Name :
                      qci3
  Charging Parameters:
    Rating Group     : 555
    Service ID       : 333
    Online Enabled   : TRUE
```

```
    Offline Enabled  : TRUE
    Online Response Required: Don't Wait
  Policy Parameters:
    MBR UL           : 50000
    MBR DL           : 50000
```

show-active-charging-sessions-full-all

The output of the above command has been enhanced to display the new parameter which shows the online response required rule definition chosen as Wait.

```
For example
Dynamic Charging Rule Definition(s) Configured:
Name                 Prior Content-Id Chrg-Type Rule Parameters
-------------------- ----- ---------- --------- --------------------------
       ruleName_Dean     5         55      Both Gate Status:      Allow All
                                                QoS Class Identifier:     1
                                                ARP Priority Level:       6
                                                Reporting Level: Rating Grp
                                                Metering Method:   Duration
                                                Uplink MBR:        40960000
                                                Downlink MBR:      40960000
                                                Uplink GBR:        40960000
                                                Downlink GBR:      40960000
                                                Filter 1:
                                                Direction:           Uplink
                                                Dst Addr  0.0.0.0/0
                                                Filter 2:
                                                Direction:         Downlink
                                                Src Addr  0.0.0.0/0
                                                Filter 3:
                                                Direction:           Uplink
                                                Dst Addr  ::/0
                                                Filter 4:
                                                Direction:         Downlink
                                                Src Addr  ::/0
                                                Online Response Required: Wait
```

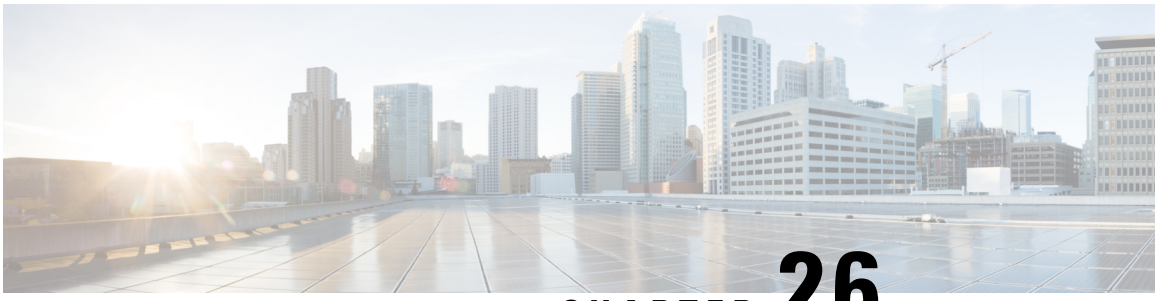
show apn-name

Use the following show apn name command output to verify the command entries.

Table 19:

Field	Description
Access Point Name (APN)	Indicates the name of the access point name (APN) for which counters are displayed.
Authentication Context	Name of the system context used for authentication for this APN.
Pdp Type	Indicates the type of PDP context. Pdp types are as follows: • IPv4 • IPv6

Field	Description
Emergency	Specifies whether **emergency-apn** option is configured in this APN or not.
Delay Tolerant	Displays whether Delay Tolerant behavior for PDN connection is available for UE in Power Saving Mode or not
PCO Options	Specifies which customized PCO (Protocol Configuration Options) options are sent in the network to MS GTP messages. PCO Options are as follows: • Custom1 • Mode • Link MTU • Nonlink MTU • ePDG Selection FQDN
Online Charging without Wait	Shows that the Online charging without Wait is defined at the APN level is disabled.



CHAPTER 26

Overcoming VoLTE Call Failure

- Feature Summary and Revision History, on page 157
- Feature Description, on page 158

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.20.28

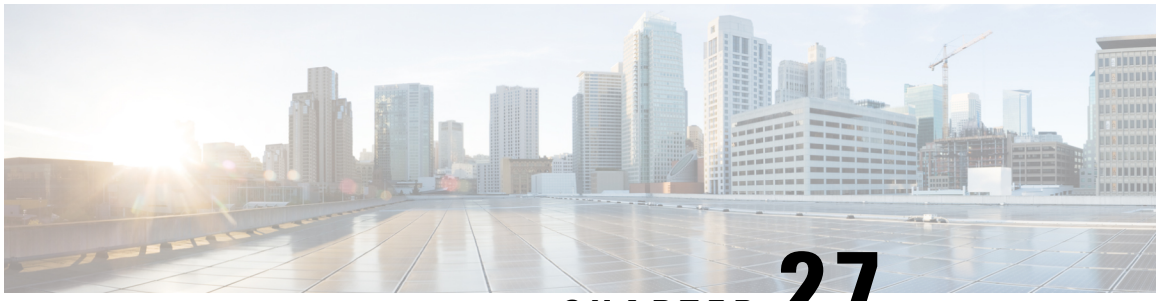
Feature Description

During the Create Bearer Request (CBR) process, eNB receives ERAB Modification Indication before receiving Dedicated Bearer Accept and this suspends the CBR process. The S1 response flag was set to zero during the process when CBR got suspended.

The CBR process is resumed only after receiving ERAB Modification Confirmation. Before sending the CBR response, S1 response flag is checked, which is set to zero. Due to this, the CBR gets rejected as the dedicated bearer response is not received for the bearer.

Note The S1 response flag is set when Dedicated Bearer Accept is received from UE.

To overcome this, the flag must not be set to zero when suspending the received bearer S1 response. If S1 response is received, the flag and S1 request are set to 1 (TRUE).



CHAPTER 27

Prevention of Randomization of Well-Known Ports

- Feature Summary and Revision History, on page 159
- Feature Changes, on page 160

Feature Summary and Revision History

Summary Data

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

Revision History

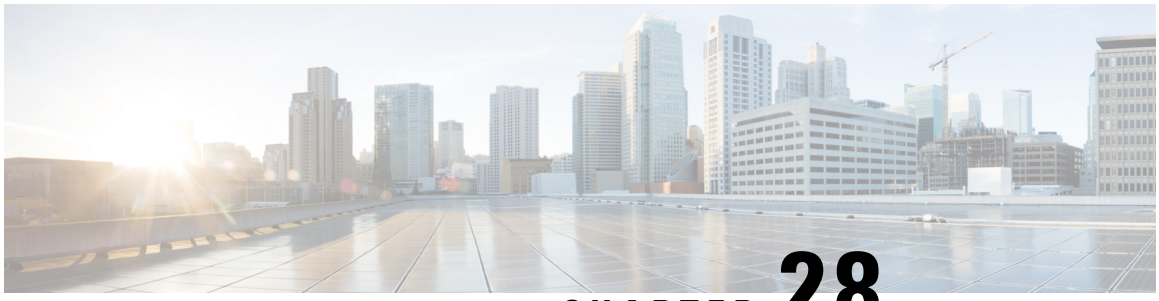
Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
With this release, the UP now restricts random source port range from 32768 to 33791.	21.20
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: In releases earlier to 21.20.x, the VPP-based port randomization did not prevent randomizing well-known ports when the source port and destination were different. The allowed port range previously supported was from 1 to 65535.

New Behavior: From this release onwards, the VPP-based port randomization prevents randomizing into well-known ports when the source port and destination are different. The UP now restricts the random source port range from 32768 to 33791.



CHAPTER 28

Printing APN Field in EDR Record

- Feature Summary and Revision History, on page 161
- Feature Changes, on page 161

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME SGSN
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

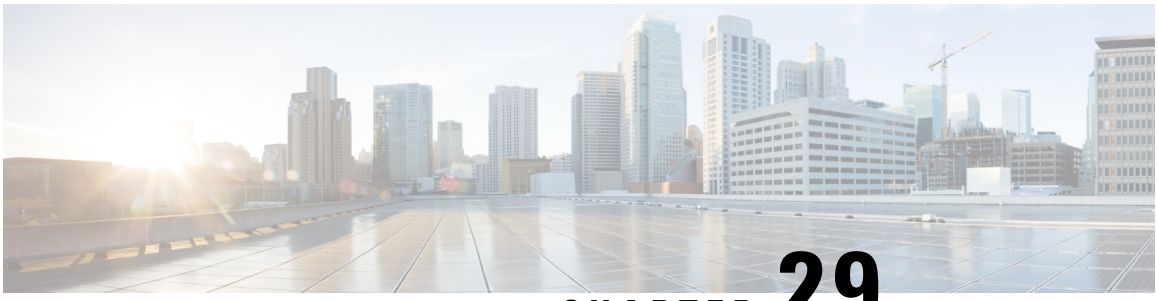
Revision History

Revision Details	Release
First Introduced	21.20

Feature Changes

Previous Behavior:: In the MME EDR log files, when the APN field contained special characters (Line break(\n), comma (,), double quotes(")), the APN field was printed without escape characters, APN was not enclosed with double quotes.

New Behavior:: If the APN field contains special characters, the APN field is enclosed with double quotes. If double quotes are available within the APN field, then it precedes another double quote.



CHAPTER 29

Revised Marking for Subscriber Traffic

- Feature Summary and Revision History, on page 163
- Feature Description, on page 164
- How It Works, on page 164
- Configuring Revised Marking for Subscriber Traffic, on page 165
- Configuring 802.1p and MPLS EXP Marking for User Data Traffic, on page 166
- Monitoring and Troubleshooting Revised Marking for Subscriber Traffic, on page 169

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* • *P-GW Administration Guide*

Revision History

Revision Details	Release
P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. This feature is fully qualified in this release.	21.20.2

Revision Details	Release
In this release P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. **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

Feature Description

802.1p/MPLS EXP marking helps in providing QoS treatment by prioritizing traffic at L2 level.

Currently, data traffic for different access types, such as GGSN, eHRPD, P-GW, and S-GW, refer to the QCI-QoS table and configure the appropriate 802.1p or MPLS-EXP (L2 QoS) markings based on the internal-qos value associated with particular row. However, the usage of internal-qos from the QCI-QoS table is not configurable and uses the default values. In addition, L2 QoS (802.1p/MPLS EXP) marking is not supported in GGSN, SAEGW, and GTPv1/eHRPD calls on P-GW.

With this feature, you can:

- Configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls.
- Mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. A new CLI command has been introduced to support service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Limitations

- This feature does not control the behavior of the control packets. The control packets (GTP-C) continue to get L2 marked based on DSCP derived L2 marking.
- This feature is not supported on standalone GGSN. It is supported on GnGp-GGSN node.

How It Works

You can configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. You can also mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Behavior Changes for Different Services

This section describes behavior of this feature for different services. Please see the *Command Changes* section for more information on the CLI command options and its behavior:

GGSN/P-GW GTPv1 Calls:

Previous Behavior: Earlier, the traffic was not marked for data path. This was default behavior for GGSN.

New Behavior: A new CLI command has been introduced to mark the traffic based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked. When the feature is not enabled, traffic is not marked.

P-GW GTPv2, S-GW, SAEGW Calls:

Previous Behavior: The QCI-QoS mapping feature used internal-QoS for L2 marking, which in turn uses QCI-Derived marking for data traffic. This was the default behavior for P-GW, S-GW, and SAEGW calls.

New Behavior: With this feature, the traffic is marked based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked and the default behavior is executed. When the feature is not enabled, traffic is not marked.

Configuring Revised Marking for Subscriber Traffic

By default, the traffic data path is supported with GGSN.. The internal priority can be configured in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. Subscriber traffic can also be marked with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Configuring Internal Priority

To configure internal priority in the QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls, use the following service specific configuration. This command in the GGSN service configuration overrides the behavior of QCI-QOS-mapping for data packets only.

```
configure
     context context_name
        ggsn-service service_name
           internal-qos data { dscp-derived | none | qci-derived }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           end
```

Notes:

- **no:** Disables the specified functionality.
- **default:** Disables the functionality.

- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.
- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show** *service-type* **{ all | name** *service_name* **}**

Please see the *Monitoring and Troubleshooting Revised Marking for Subscriber Traffic* section for the command output.

Configuring 802.1p and MPLS EXP Marking for User Data Traffic

This section describes how to configure the 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. Configuring the feature consists of the following tasks:

1. Configure ip-dscp-iphb-mapping.
2. Configure L2-mapping
3. Configure qci-qos-mapping.
4. Associate the l2-mapping in Egress context.
5. Associate the l2-mapping in Igress context.
6. Associate internal-qos data in P-GW and S-GW service

Configure ip-dscp-iphb-mapping

Use the following example to access *QOS Profile Configuration Mode* and configure ip-dscp-iphb-mapping.

```
configure
  qos ip-dscp-iphb-mapping dscp Value  internal-priority cos  value
  end
```

Notes:

- *qos ip-dscp-iphb-mapping dscp* : Creates a QOS profile.
- **dscp** : Specify dscp mapping with Hexadecimal value between 0x0 and 0x3F.
- **internal-priority cos** : Define the Class of Service (cos) value between 0x0 and 0x7.

Configure L2-mapping

Use the following example to access *QOS L2 Mapping Configuration Mode* and configure L2 mapping.

```
configure
  qos l2-mapping-table name  { name map_table_name | system-default }
    internal-priority cos class_of_service_value color color_value [ 802.1p-value
 802.1p_value ] [ mpls-tc mpls_tc_value ]
      end
```

Notes:

- **qos l2-mapping-table name** : Maps qos from internal qos to l2 values.
- **internal-priority cos** : Maps internal QoS priority with Class of Service (COS) values.
  - *class_of_service_value*: Specify a Hexadecimal number between 0x0 and 0x7.
  - **802.1p-value** : Maps to a 802.1p value and *.802.1p_value* must be a Hexadecimal number between 0x0 and 0xF.
  - **mpls-tc** *mpls_tc_value*: Maps to an MPLS traffic class. *mpls_tc_value* must be a Hexadecimal number between 0x0 and 0x7.

Configure qci-qos

Use the following commands to configure qci-qos mapping.

```
Configure
  qci-qos-mapping  name
    qci  num [ arp-priority-level arp_value ] [ downlink [ encaps-header
 { copy-inner | dscp-marking  dscp-marking-value } ] [ internal-qos
priority  priority ] [ user-datagram dscp-marking  dscp-marking-value  ]
 ]  [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking
dscp-marking-value } ] [ internal-qos priority  priority ]  [ user-datagram
 dscp-marking  dscp-marking-value  ] ]
     end
```

Notes:

- **qci-qos-mapping** : Maps internal QoS priority with Class of Service (CoS) value.
- **quci num**: Specifies the non-standard, operator-defined QCI value to be enabled.
- **arp-priority-level** : Specifies the address retention priority (ARP) priority level.
- **downlink**: Configures parameters for downlink traffic.
- **encaps-header { copy-inner | dscp-marking** *dscp-marking-value}*: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
  - **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
  - **dscp-marking** *dscp-marking-value*: Specifies that the DSCP marking is to be defined by this keyword.

dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

- **uplink**: Configures parameters for uplink traffic.
- **internal-qos priority** *priority* : Sets the internal QoS. These get resolved in L2 values.
- **user-datagram dscp-marking** *dscp-marking-value*: Specifies that the IP DSCP marking is to be defined by this keyword.*dscp-marking-value* is expressed as a hexadecimal number from 0x00 through 0x3F.

Associate L2-mapping table

Use the following commands to associate L2 mapping table in egress context and ingress context.

```
configure
   context egress context_name | ingress context_name
   associate l2-mapping-table { name table_name
   exit
   context ingress context_name
   associate l2-mapping-table { name table_name
   end
```

- **associate l2-mapping-table**: Maps qos from internal qos to l2 values.
- **{ name** *table_name* : Specifies the name of table to map qos from internal qos to l2 values. *table_name* must be a alphanumeric string of size 1 to 80.

Associate internal-qos-data in a P-GW and S-GW Service

Use the following commands to associate internal-qos-data in a P-GW and S-GW service.

```
configure
     context context_name
       pgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          exit
        sgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          end
```

Notes:

- **no:** : Disables the specified functionality.
- **default** : Disables the functionality.
- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.

- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Monitoring and Troubleshooting Revised Marking for Subscriber Traffic

The following section describes commands available to monitor Revised Marking for Subscriber Traffic.

Internal Priority Show Commands

The following section describes commands available to monitor Internal Priority.

show configuration

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
internal-qos data none
```

- When **internal-qos data** is configured as **qci-derived**:

```
internal-qos data qci-derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
internal-qos data dscp-ds-derived
```

- When **internal-qos data** is **not configured**:

```
no internal-qos data
```

show *service-type* { all | name *service_name* }

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:         None
```

- When **internal-qos data** is configured as **qci-derived**:

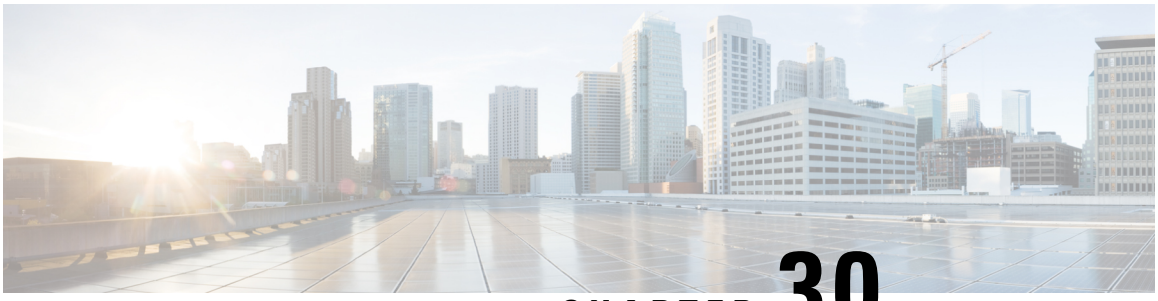
```
Internal QOS Application:   Enabled
Internal QOS Policy:        QCI Derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
 Internal QOS Application:    Enabled
 Internal QOS Policy:         DSCP Derived
```

- When **internal-qos data** is **not configured**:

```
                Internal QOS Application:     Backward-compatible
```



CHAPTER 30

Roaming Support for Monitoring Events

- Feature Summary and Revision History, on page 171
- Feature Description, on page 172
- How it Works, on page 172
- Configuring Monitoring Events Profile , on page 176
- Monitoring and Troubleshooting, on page 180

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
This release supports Roaming feature for monitoring events:	21.20

Feature Description

MME supports Roaming functionality for monitoring events through Interworking (IWK) SCEF by communicating monitoring information to the SCEF.

How it Works

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

Figure 12: Monitoring Events Call Flow through Interworking (IWK) SCEF

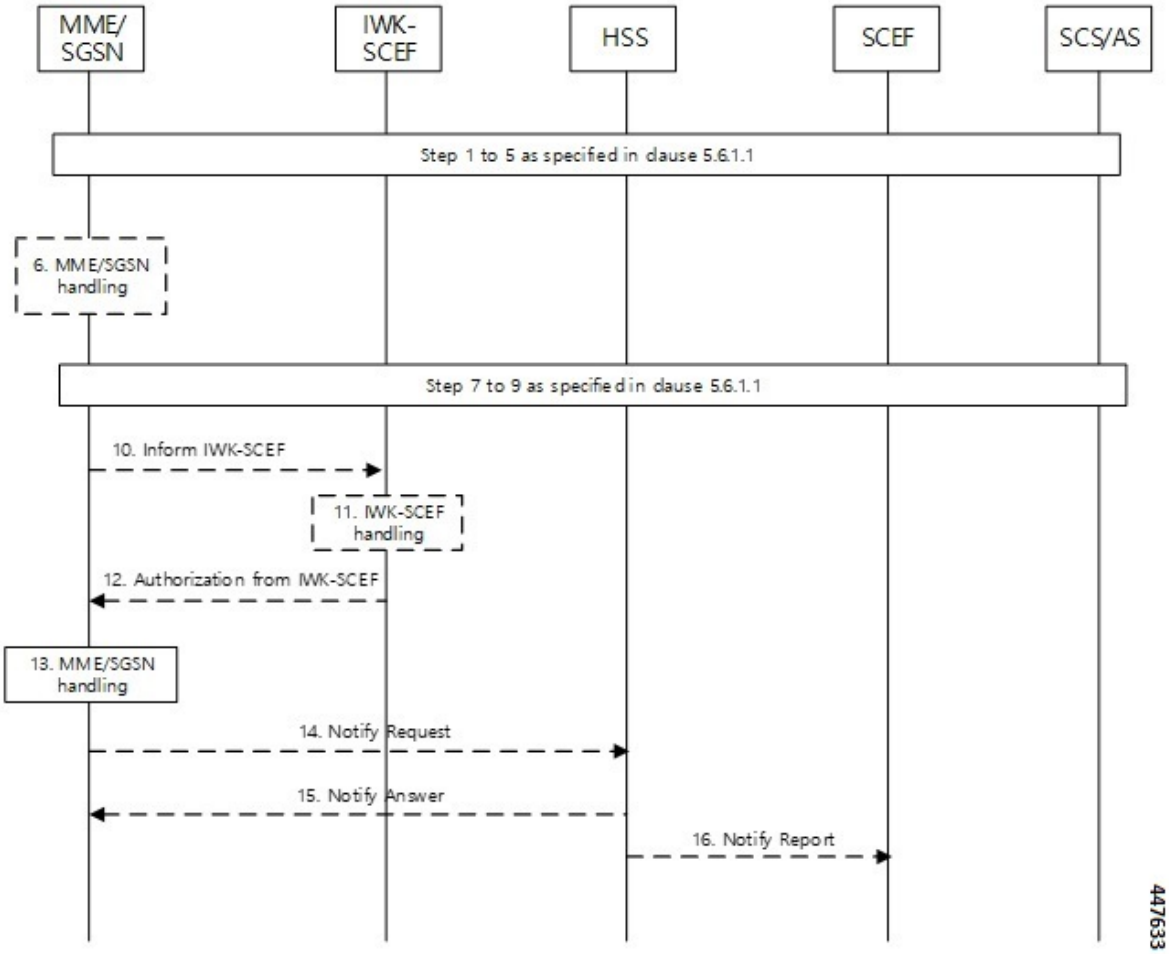


Table 20: Monitoring Event Configuration through IWK-SCEF Procedure

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.
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.

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.

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 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.

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.

Note In the StarOS 21.20 and later releases, After the UE Detach procedure, **Total Terminated** and **Total Current Sessions** counters in Statistics are updated only after purge timeout (purge time out + 10% of purge timeout) seconds. Whereas for releases on or before StarOS 21.19, **Total Terminated** and **Total Current Sessions** counters are updated immediately after the successful UE Detach Procedure.

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.

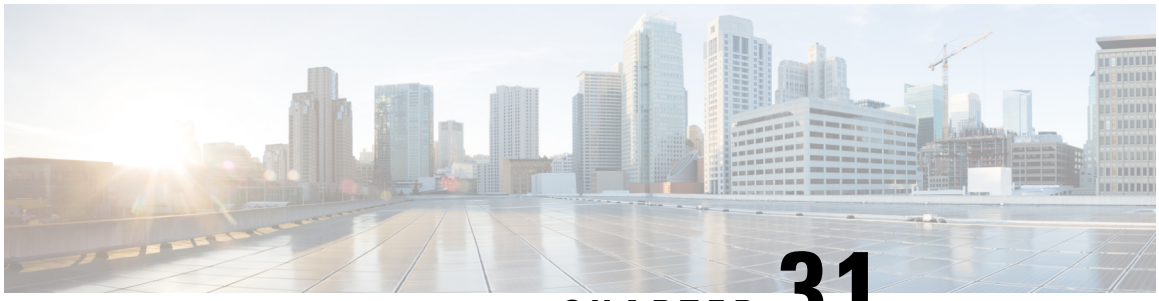
Monitoring Event Configuration Deleted Count: The output includes the following fields:

- 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.



CHAPTER 31

RedHat Software Version Update

- Feature Summary and Revision History, on page 185
- Feature Description, on page 185

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	VPC-DI
Feature Default	Enabled - Always-on
Related Features in this Release	Not Applicable
Related Documentation	Not Applicable

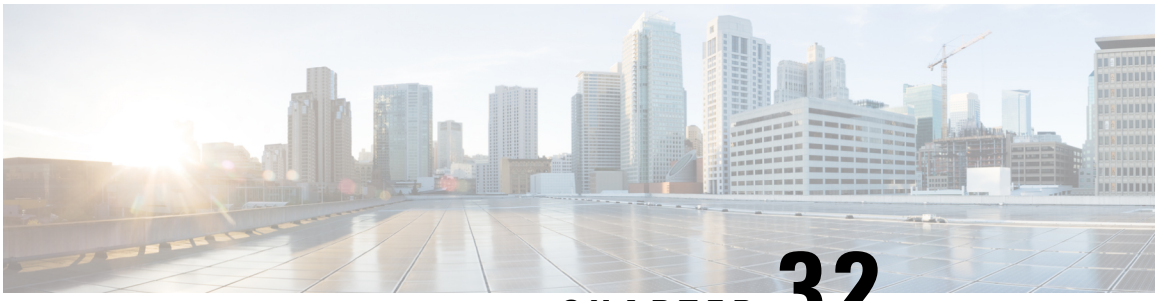
Revision History

Revision Details	Release
First introduced.	21.20.12

Feature Description

This release includes support for RedHat OpenStack Platform (OSP) version 16.1 (Train). The RedHat OSP 16.1 (Train) has been validated and is recommended for use with all the VPC-DI based deployments.

For more information, contact your Cisco Account representative.



CHAPTER 32

Secondary RAT Usage Report in CDR Records

- Feature Summary and Revision History, on page 187
- Feature Description, on page 188
- Configuring Secondary RAT Usage Report through GTPP, on page 191
- Monitoring and Troubleshooting, on page 194

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
P-GW and S-GW supports secondary RAT usage reports and CDRs processing through GTPP Group Configuration CLIs.	21.20.31

Feature Description

Reporting issues pertaining to 5G **RANSecondaryRATUsageReport** occur due to lack of:

- Control in identifying whether the **RANSecondaryRATUsageReport** must be processed in CDRs or not. This allows the S-GW, P-GW, and SAEGW to either include these reports in the SGW-CDR or PGW- CDR or to simply ignore them.
- Number of available reports inside a CDR, if the control is active.
- Control in identifying whether Zero-volume reports must make it inside the CDR or not.

This results in billing loss of data. To overcome these reporting issues, you can trigger CLI controls using GTPP group configuration to:

- Allow the S-GW, P-GW, and SAEGW to either include the RANSecondary RAT Usage reports in the SGW-CDR or PGW-CDR or to simply ignore them.
- Identify the number of secondary RAT usage reports available inside the SGW-CDR or the PGW- CDR.

Note This limit must be in accordance with the system capability and ensure to consider the File-Format of the CDRs. If the configured limit exceeds, the system closes the SGW-CDR or PGW-CDR with the appropriate change-condition. For example, **max-change-condition** CDR is reused for further reports.

- Add or ignore Zero-volume reports inside the CDR.
- The CLI **gtpp limit-secondary-rat-usage** or hardcoded limit will be removed and the CLI **gtpp limit-secondary-rat-usage** is reused to control the number of records within the range 1-100.
- Provides logging when the CDR size reaches the maximum size. Through PGW-CDR counter, you can monitor the number of occurrences when the CDR exceeds its size limit.

Behavior Matrix

The following table explains the new behavior of P-GW and S-GW for this feature.

CLI	P-GW New Behavior	S-GW New Behavior
gtpp attribute secondary-rat-usage By default, this CLI command is enabled in gtpp group.	P-GW sends secondary RAT usage records in CDR including zero volume records.	S-GW sends secondary RAT usage records in CDR including zero volume records.
[no] gtpp attribute secondary-rat-usage	P-GW does not send secondary RAT usage records in CDR.	S-GW does not send secondary RAT usage records in CDR.
gtpp suppress-secondary-rat-usage zero-volume By default, this CLI command is disabled in gtpp group.	P-GW does not include and send zero volume secondary RAT records in CDR. P-GW sends only secondary RAT records with non-zero volumes.	S-GW does not include and send zero volume secondary RAT records in CDR. S-GW sends only secondary RAT records with non-zero volumes.
[no] gtpp suppress-secondary-rat-usage zero-volume	P-GW sends secondary RAT usage records including zero volume records in CDR.	S-GW sends secondary RAT usage records including zero volume records in CDR.
gtpp limit-secondary-rat-usage *range_1–100*. If not configured, the default value is 32. By default, this CLI command is enabled in gtpp group. **Example: gtpp limit-secondary-rat-usage 32** **Note** This CLI is the modification of the existing CLI command **gtpp limit-secondary-rat-usage** with range between 1– 100.	P-GW generates CDR immediately when total received secondary RAT records exceeds 32 and reported cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 32. **Example**: If P-GW receives 100 RAT records between two triggers, P-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.	S-GW generates CDR immediately when total received secondary RAT records exceeds 32 and the reported cause value is *maximum change condition*. S-GW generates multiple CDRs if the total received secondary RAT records are multiples of 32. **Example**: If S-GW receives 100 RAT records between two triggers, S-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.
Example:gtpp limit-secondary-rat-usage 40	P-GW generates CDR immediately when total received secondary RAT records exceeds 40 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 40. **Example**: If P-GW receives 100 RAT records between two triggers, it will generate 2 CDRs and will keep remaining 20 RAT records for the next CDR trigger.	If the configured value is greater than 32 and sends 32 secondary RAT records in every CDR, Ignores **gtpp limit-secondary-rat-usage 40** CLI command.

CLI	P-GW New Behavior	S-GW New Behavior
Example:gtpp limit-secondary-rat-usage 20	P-GW generates CDR immediately when total received secondary RAT records exceed 20 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 20. **Example:** If P-GW receives 100 RAT records between two triggers, P-GW generates 2 CDRs and will store the remaining 20 RAT records for the next CDR trigger.	S-GW generates CDR immediately when the total received secondary RAT records exceeds 20 and cause value is *maximum change condition*. S-GW generates multiple CDRs if total received secondary RAT records are in multiples of 20. **Example**: If S-GW receives 100 RAT records between two triggers, it will generate 5 CDRs.
[no] gtpp limit-secondary-rat-usage	Generates CDR immediately when the total received secondary RAT records exceed 255 and cause value is *maximum change condition*. Generates multiple CDRs if the total received secondary RAT records are multiples of 255. **Example**: If 1000 RAT records between two triggers are received, then 3 CDRs are generated. The remaining 235 RAT records are stored for the next CDR trigger.	Ignores the **[no] gtpp limit-secondary-rat-usage** CLI and sends 32 secondary RAT records in every CDR. Behavior is similar to the **gtpp limit-secondary-rat-usage** *32* CLI implementation. Counter and debug logs are not required as it will never exceed the CDR size of 64k.
	Service-specific unit limit is sent in the **serviceConditionChange** file.	Record Closure

Relationship to Other Features

- Sessmgr Restart While Processing Secondary RAT Usage CDR Records in the *P-GW Administration Guide*.
- Secondary RAT Usage IE during GnGp handover, S-GW, and P-GW support of Secondary RAT Data Usage Report in Gz CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.
- P-GW support of Secondary RAT Data Usage Report in Rf CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.

Limitations

This feature has the following limitations:

- S-GW allows a maximum number of 16 secondary RAT records per bearer during session recovery and checkpointing.
- P-GW allows a maximum number of 142 secondary RAT records across all bearers during session recovery and checkpointing.
- Anything beyond these numbers gets lost during session recovery.

Configuring Secondary RAT Usage Report through GTPP

Use the following GTPP configurations to close Secondary RAT Usage CDR records before exceeding a buffer size.

Enabling or Disabling the Secondary RAT Usage Report

Use the following configuration to enable or disable secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute secondary-rat-usage
      default gtpp attribute secondary-rat-usage
      no gtpp attribute secondary-rat-usage
      end
```

NOTES:

- **gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records.
- **default gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records by default.
- **no gtpp attribute secondary-rat-usage**: Does not send the optional attribute Secondary RAT usage records.

Controlling the Maximum Number of Entries

When the Secondary RAT usage record reaches the maximum configured value within a CDR, the CDR closure cause occurs and uses **maxChangeCond**. The **gtpp limit-secondary-RAT-usage** CLI command controls the maximum number of Secondary RAT usage record entries in the P-GW and S-GW CDRs. If the limit is configured with a value more than 32, the partial CDRs get generated with a maximum of 32 for S-GW CDR.

Note The existing behaviour of S-GW has a limit of 32 Secondary RAT Usage records.

The following table explains the behavior of Secondary RAT records and CDR, and the maximum limit.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
1	P-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 secondary RAT records.
					Remaining 15 secondary RAT records sent in the next trigger.
	S-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 Secondary RAT records.
					Remaining 15 Secondary RAT records sent in the next trigger.
2	P-GW	32	32	35	Partial CDR is generated with 32 Secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.
	S-GW	32	32	35	Partial CDR is generated with 32 secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
3	P-GW	Greater than 32 Example: 100	100	100	Partial CDR is generated with 100 secondary RAT records.
	S-GW	Greater than 32 Example: 100	32	100	Three partial CDRs are generated with 32 secondary RAT records each.
					Remaining 4 secondary RAT records sent in the next trigger.
4	P-GW	Not configured	255	1000	Three partial CDRs are generated with 255 secondary RAT records each.
					Remaining reported Secondary RAT records become a part of CDR in the next trigger.
	S-GW	Not configured	32	1000	No partial CDR is generated.
					32 Secondary RAT records become part of the CDR in the next trigger.

Use the following configuration to control the maximum number of entries.

```
configure
  context context_name
    gtpp group group_name
      gtpp limit-secondary-rat-usage usage_limit
      default gtpp limit-secondary-rat-usage
```

```
no gtpp limit-secondary-rat-usage
end
```

NOTES:

- **gtpp limit-secondary-rat-usage** *usage_limit*: Enter a maximum number of secondary RAT reports. *usage_limit* must be an integer in the range of 1-100. The recommended value for S-GW CDR is 32.

  For example, if the limit is set to 10, then the CDR is generated once the configured value is reached.

- **default gtpp limit-secondary-rat-usage**: Specifies a default value of 32.
- **no gtpp limit-secondary-rat-usage**: Disables the CDR generation with limited number of secondary RAT usage information.

Suppressing Zero-Volume Secondary RAT Usage Report

Use the following configuration to suppress zero-volume Secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp suppress-secondary-rat-usage zero-volume
      default gtpp suppress-secondary-rat-usage zero-volume
      no gtpp suppress-secondary-rat-usage zero-volume
      end
```

NOTES:

- **gtpp suppress-secondary-rat-usage zero-volume**: Suppresses either Secondary RAT records or zero volume Secondary RAT records.
- **default gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume secondary RAT usage records.
- **no gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume Secondary RAT usage records.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show config

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Specify this option to include the Secondary RAT reports field in the CDR.
gtpp suppress-secondary-rat-usage zero-volume	Enables the exclusion of the zero volume Secondary RAT reports in the CDR.
gtpp limit-secondary-rat-usage	Enables limiting the number of Secondary RAT Usage reports in CDR with the configured value.

show config verbose

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Displays the Secondary RAT usage records.
gtpp suppress-secondary-rat-usage zero-volume	Displays only Secondary RAT records that is having non-zero volumes from P-GW and S-GW.
gtpp limit-secondary-rat-usage	If total received Secondary RAT records are multiples of 10, displays multiple CDR generated by P-GW and S-GW. The reported cause value will be the maximum change condition.
no gtpp limit-secondary-rat-usage	Displays Secondary RAT records for unconfigured cause.

show gtpp group

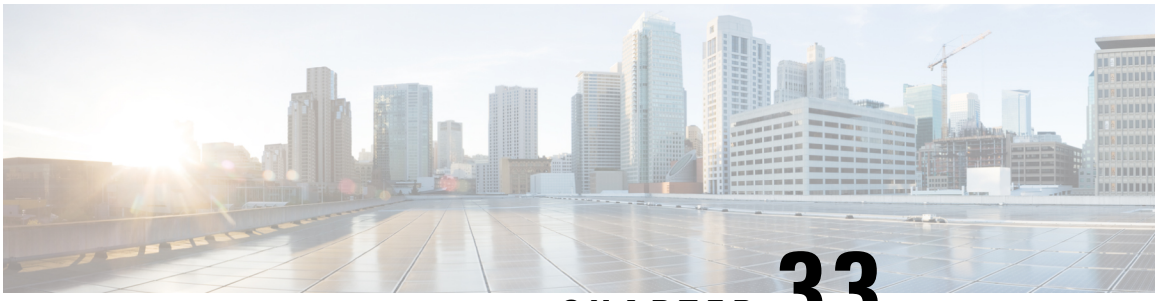
The output of this CLI command displays the following parameters.

Field	Description
Secondary RAT records present	Specifies whether the Secondary RAT record is present or not. The available options are: • no • yes
Limit-secondary-rat-usage	Specifies a limit for Secondary RAT usage report.

show gtpp statistics group

The output of this CLI command displays the following parameter.

Field	Description
Total PGW-CDR exceed size limit	Displays the total number of CDRs that exceeded size limit in P-GW.



CHAPTER 33

Supporting Larger Source to Target Container IE in Handover

- Feature Summary and Revision History, on page 197
- Feature Changes, on page 198
- Monitoring and Troubleshooting, on page 198

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.	21.20.3
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.

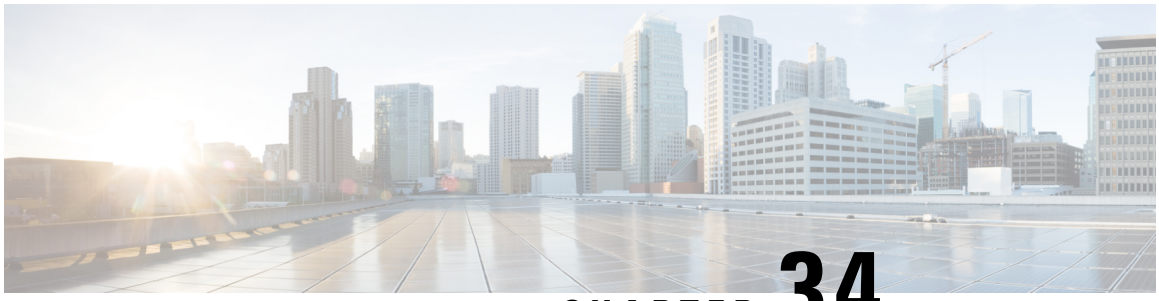
Show Commands and Outputs

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 34

Show Fabric Status

- Understanding Fabric Hardware Architecture, on page 201
- Terminology, on page 201
- Support for show fabric-status Command at Operator Level, on page 202
- Verify Fabric Device Status, on page 202

Understanding Fabric Hardware Architecture

The fabric hardware is made up of Fabric Access Processor (FAP) devices on the MIO/DPC/DPC2 cards, and Forwarding Engine (FE) devices on the Fabric and Storage Cards (FCS). Each FAP has three Serializer/Deserializer (SERDES) links to each FE device.

A separate process named ARES Fabric IO (AFIO) configures and manages each individual fabric device. The AFIO process is a standalone executable and not a boxer proclet. This is primarily because the Control plane must be initialized and configured before Boxer is started. The FE devices are managed by AFIO processes running on the Active MIO, one for each FE device. This is because the AFIO process or processes, which run on the local CPU of the MIO/DPC/DPC2 card and the FSC cards do not have a local CPU.

Within Boxer, running on the CPU of the Active MIO, there is a fabric-related controlling proclet named Ares Fabric Controller (AFCtrl). Also within Boxer, on the CPU on each card, there is a process named Ares Fabric Manager (AFMgr). Each AFMgr has an IPC connection to all AFIO processes on the same CPU.

All CLI requests are sent to the AFCtrl proclet on the Active MIO. Depending on the command, AFCtrl forwards the request to one or more AFMgr(s). AFMgr in turn forwards the request to one or more appropriate afios. The AFIO process receives and processes the request, then sends a reply to AFMgr. AFMgr coordinates the individual afio responses by aggregating them into a single reply, which is then sent to AFCtrl. AFCtrl waits for all AFMgr responses, and displays the results.

Terminology

This section defines important terms:

- Ares Fabric IO (AFIO) – Name of process that controls a FAP or FE device.
- Fabric Access Device (FAP) – Hardware device found on MIO, DPC and DPC2 cards on which packets enter and exit the fabric. It performs segmentation/reassembly, queueing and traffic engineering.

- Forwarding Entity (FE) – Hardware device found on FSC card which receives a fabric cell from the source FAP and forwards it to the destination FAP.
- Fabric and Storage Card (FSC) – FSC is a front-mounted card. The FE devices on the FSC provide a crossbar switch architecture. The ASR 5500 supports up to 6 FSC cards.
- Serializer/Deserializer (SERDES) – SERDES converts parallel data from multiple interfaces into serial data, in both directions, that is sent over a link.

Support for show fabric-status Command at Operator Level

Currently, the “show fabric status” command is a debug level show command, which allows the Cisco TAC personnel to check and verify the high-level summary of the SERDES lanes in all fabric devices. This high-level summary includes fabric links between the FSC, DPC/DPC2 and MIO cards, and serdes links to an NPU or FPGA. The "show fabric status" checks and displays the current state of all SERDES lanes. In this StarOS 21.21 and later releases, the network operators or anyone with higher login access can run this show fabric status command without Cisco TAC assistance.

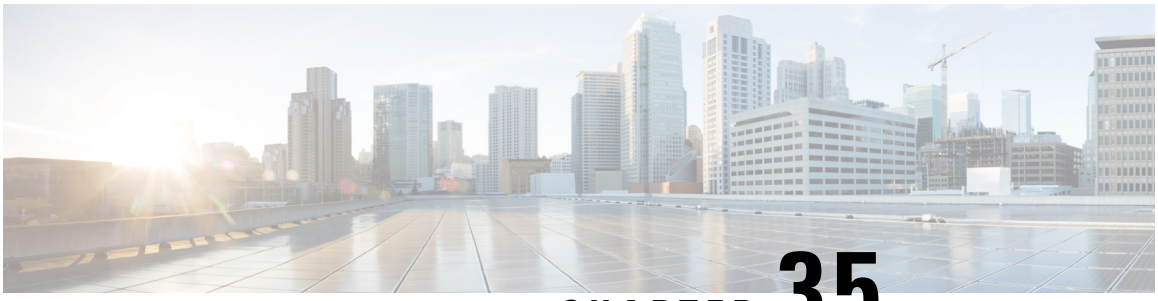
The CLI command is sent from the CLI proclet to the AFCtrl proclet. It essentially probes all SERDES lanes on each FAP an FE device by sending the request to all AFMgrs and all AFIOs. Determining the SERDES status of each lane requires reading multiple registers in the FAP and FE devices, because each FAP has up to 60 active SERDES lanes, and each FE has up to 96 SERDES lanes. This results in many device access operations, which can be CPU intensive. To prevent unnecessary CPU load by executing this command at a high frequency, it probes the device no more than once every 30 seconds. If the command is run at an interval less than 30 seconds, it returns the previous results. Once 30 seconds has passed, the next request will probe the devices.

Verify Fabric Device Status

Use the **show fabric status** command to verify the fabric device status.

Field	Description
Total number of FAPs	The Fabric status report displays the total number of FAP devices in the chassis.
Total number of FEs	The Fabric status report displays the total number of FE devices in the chassis..
Total number of SERDES links	Displays total number of SERDES lanes, broken down into Network Interface (NIF) and Fabric. **Note** NIF serdes lanes are between the FAP and another device, such as the NPU or FPGA. Fabric lanes are between FAP and FE devices.
Total number of active SERDES links	Displays total number of active SERDES links.
Total number of Fabric SERDES with errors	Displays total number of fabric SERDES with errors.

Field	Description
Total number of NIF SERDES with errors	Displays total number of NIF SERDES with errors.
Devices last Probed	Displayed only if cached values are returned because it has been less than 30 seconds since the command was last run.



CHAPTER 35

Short Message Service

- Feature Summary and Revision History, on page 205
- Feature Description, on page 206
- How It Works, on page 206
- Configuring SMS Support, on page 215
- Monitoring and Troubleshooting, on page 221

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The supports for SMS over SGd interface for EPS only Attach feature is introduced.	21.20.19

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

Feature Description

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

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

SMS is delivered over LTE through the following methods:

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

  For more information, see the *Configuring MME Preference for SMS section*.

How It Works

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

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

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

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

Limitations

This section lists the known limitations for the SMS feature:

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

Flows

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

Obtaining UE capability for SMS

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

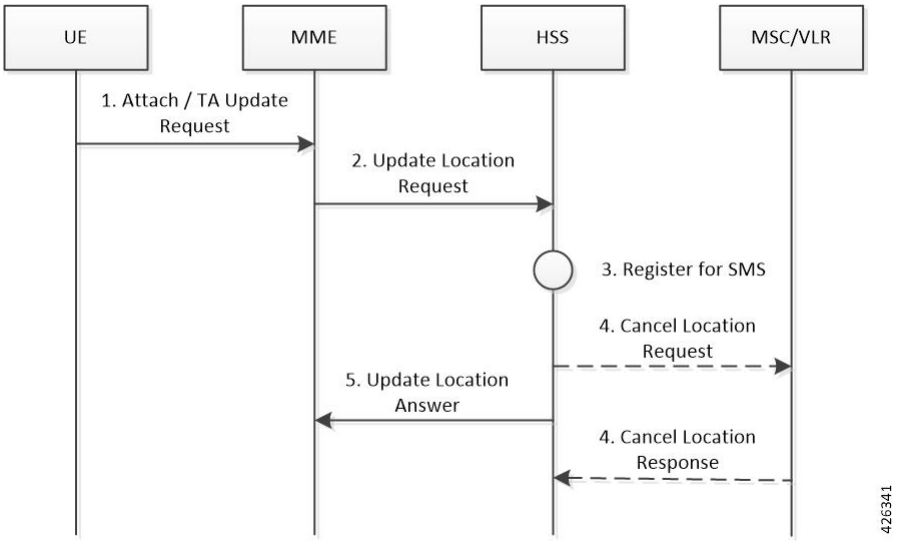
EPS Attach:To support the SMS-only handling option for NBIOT users, the MME must accept the Attach Request. The Attach Request must be associated with an Attach Type of "EPS Attach", or a "TAU Request" with an Update Type of "TA Updating" with an SMS-only indication in the Additional Update IE.

SMS Capability with HSS

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

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

Figure 13: SMS Capability with HSS

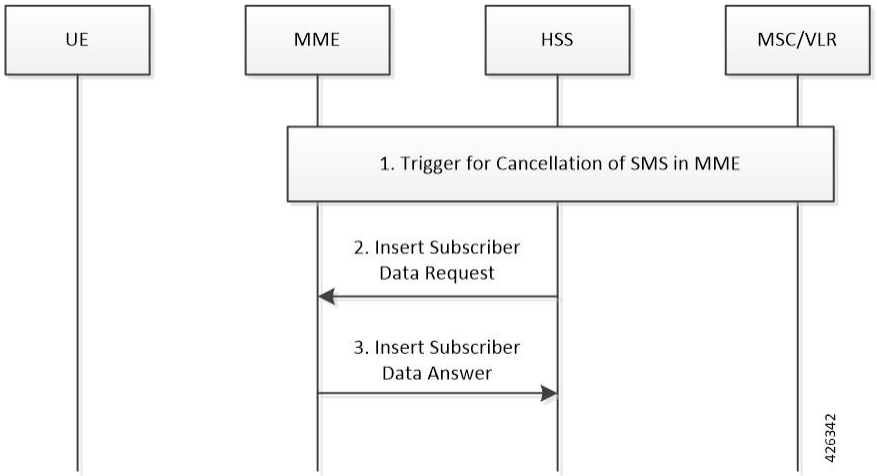


Step	Description
1	The UE initiates combined Attach Update or combined TAU/LAU to an MME.
2	The MME sends an Update Location Request message to the HSS with the following data: • SMS bit set in Feature-List in Supported-Features AVP. The Feature-List ID will be set to 2. • "SMS-only" indication bit set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

HSS-initiated Removal of Registration for SMS

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

Figure 14: Removal of Registration for SMS

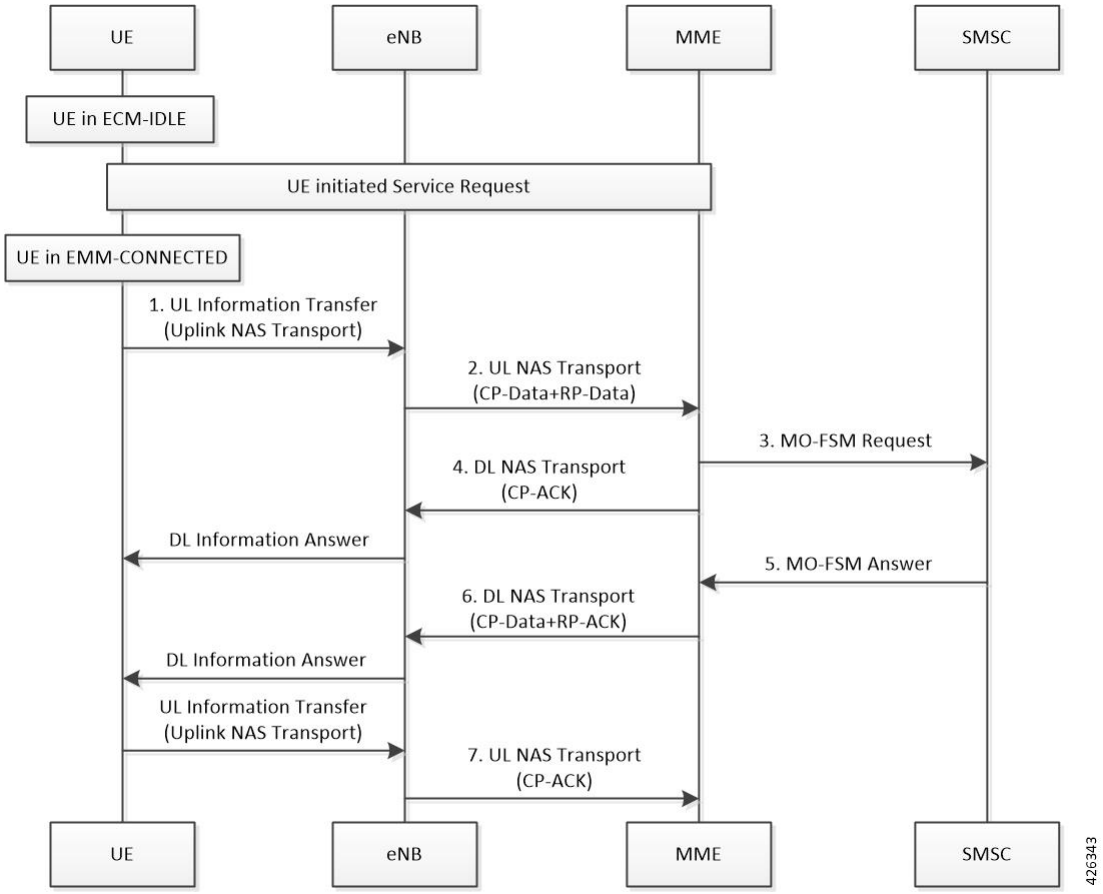


Step	Description
1	An event will trigger the cancellation of the MME being registered for SMS. For example, removal of the SMS subscription for the UE, CS location update, and so on.
2	The HSS sends an Insert Subscriber Data Request (Remove SMS registration) message to the MME to inform that it is no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

MO Forward Short Message Procedure

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

Figure 15: MO Forward Short Message Procedure



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

MT Forward Short Message Procedure

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

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

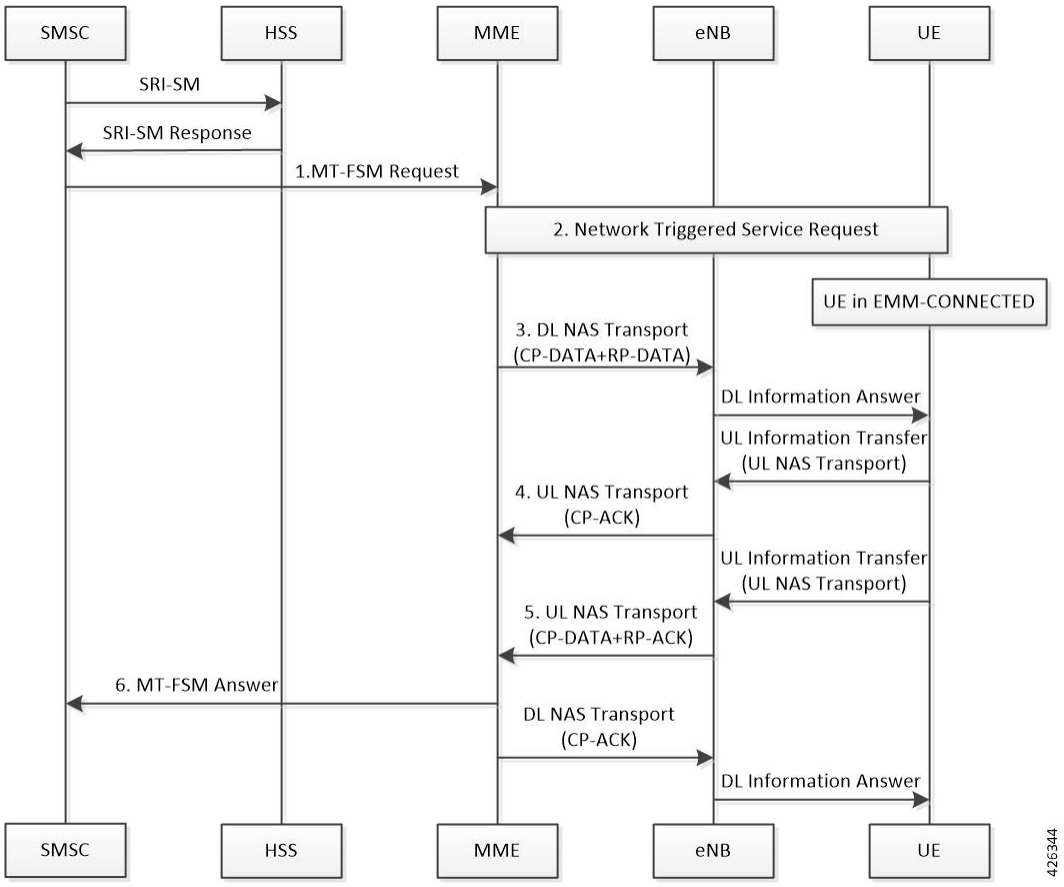
  If it is an unknown user, an Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN is returned.

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

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

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

Figure 16: MT Forward Short Message

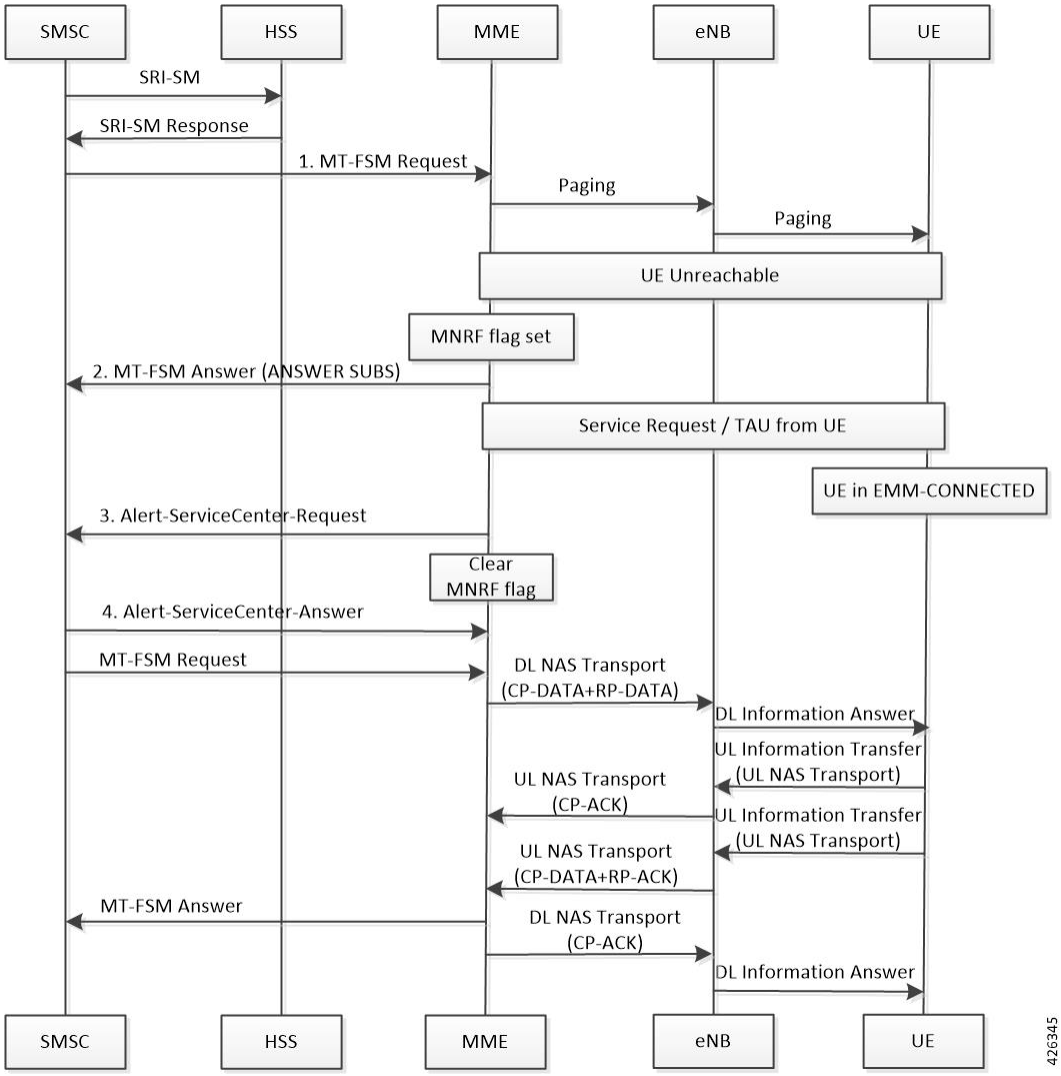


Step	Description
1	The SMSC sends mobile terminated SMS to MME in the MT-Forward-Short-Message-Request (TFR) message.
2	If the UE is in IDLE mode then MME initiates paging and establishes an S1AP connection provided UE replies with paging response.
3	Once the UE is in CONNECTED mode, MME forwards the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

MT Forward Short Message Procedure (UE Unreachable)

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

Figure 17: MT Forward Short Message Procedure (UE Unreachable)



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

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

MT Forward Short Message Procedure (UE Memory Unavailable)

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

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

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

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

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

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

Important This procedure has the following limitations:

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

Standards Compliance

The SMS feature complies with the following standards:

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

Configuring SMS Support

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

Creating and Configuring SMSC Service

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

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

NOTES:

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

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

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

Verifying the Configuration

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

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

Configuring MME Preference for SMS

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

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

     end
```

Note When the **sms-in-mme subscribe eps-only-attach** command is enabled, the SC Address AVP between the MME and SMSC is handled as per 3gpp release 15.

NOTES:

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

Associating SMSC Service with MME Service

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

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

NOTES:

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

Configuring Alert SC Request on SGd interface

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

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

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

NOTES:

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

Verifying the Configuration

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

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

Configuring Notify Request on S6a Interface

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

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

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

NOTES:

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

Verifying the Configuration

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

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

Configuring Queue Timers

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

```
configure
  context context_name
    mme-service mme_svc_name
      emm { mt-queue-timeout mtq_timer | tc1n-timeout tc1n_timer |
```

```
tr1n-timeout tr1n_timer | tr2n-timeout tr2n_timer }
       default emm { mt-queue-timeout | tc1n-timeout | tr1n-timeout |
tr2n-timeout }
       end
```

NOTES:

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

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

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

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

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

Verifying the Configuration

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

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

Configuring CP Data Retransmissions

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

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

NOTES:

- **context** *context_name*: Creates or specifies an existing context and enters the Context Configuration mode. *context_name* specifies the name of a context entered as an alphanumeric string of 1 to 79 characters.

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service as an alphanumeric string of 1 to 63 characters.
- **cp-data-max-retransmissions** *num_retrans*: Configures the number of times CP Data for SMS is retransmitted. *num_retrans* must be an integer from 1 to 10.
- **default**: Sets the default value to 2.

Verifying the Configuration

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

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

Configuring Heuristic paging for PS-SMS traffic via MME

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

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

NOTES:

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

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

Monitoring and Troubleshooting

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

Show Commands and/or Outputs

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

show call-control-profile full all

The output of this command includes the following fields:

- SMS in MME — Displays the configured value (preferred / not-preferred) for SMS in MME.
- SMSC Address — Displays the configured SMSC address.

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

show mme-service all

The output of this command includes the following fields:

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

show mme-service session full all

The output of this command includes the following fields:

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

show mme-service statistics

The output of this command includes the following fields:

- Paging Initiation for PS SMS Events:

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

- NB-IoT with SMS:
  - Attach Requests Rcvd — The total number of EPS Attach Requests received for NB-IoT subscribers with SMS option.

show smsc-service name <smsc_svc_name>

The output of this command includes the following fields:

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

show smsc-service statistics all

The output of this command includes the following fields:

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

- Message Stats:
  - Total Messages Rcvd — Displays the total number of messages received.
  - Total Messages Sent — Displays the total number of messages sent.
  - OF Request — Displays the total number of OF requests.
  - OF Answer — Displays the total number of OF answers.
  - OFR Retries — Displays the total number of OFR retries.
  - OFR Timeouts — Displays the total number of OFR timeouts.
  - OFA Dropped — Displays the total number of OFA dropped.
  - TF Request — Displays the total number of TF requests.
  - TF Answer — Displays the total number of TF answers.
  - TFR Retries — Displays the total number of TFR retries.
  - TFA Timeouts — Displays the total number of TFA timeouts.
  - TFA Dropped — Displays the total number of TFA dropped requests.
  - AL Request — Displays the total number of AL requests.
  - AL Answer — Displays the total number of AL answers.
  - ALR Retries — Displays the total number of ALR retries.
  - ALR Timeouts — Displays the total number of ALR timeouts.
  - ALA Dropped — Displays the total number of ALA dropped.
- Message Error Stats:
  - Unable To Comply — Displays the total number of message errors containing the result code "Unable To Comply".
  - User Unknown — Displays the total number of message errors containing the result code "User Unknown".
  - User Absent — Displays the total number of message errors containing the result code "User Absent".
  - User Illegal — Displays the total number of message errors containing the result code "User Illegal".
  - SM Delivery Failure — Displays the total number of message errors containing the result code "SM Delivery Failure".
  - User Busy for MT SMS — Displays the total number of message errors containing the result code "User Busy for MT SMS".
  - Other Errors — Displays the total number of message errors containing the result code "Other Errors".
- Bad Answer Stats:
  - Auth-Application-Id — Displays the absence or unexpected value in Auth-Application-Id AVP.

- Session-Id — Displays the absence or unexpected value in Session-Id AVP.
- Origin-Host — Displays the absence of Origin-Host AVP.
- Origin Realm — Displays the absence of Origin-Realm AVP.
- Parse-Message-Errors — Displays the total number of parse errors in the message.
- Parse-Mscc-Errors — Displays the total number of parse errors in MSCC AVP.
- Miscellaneous — Displays the total number of other miscellaneous errors.

show smsc-service statistics summary

The output of this command includes the following fields:

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

show sms statistics mme-only verbose

The output of this command includes the following fields:

SMS Statistics:

Session Statistics:

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

- SMMA Attempted — The total number of procedures for retrieval of available SMS memory attempted.
- SMMA Successful — The total number of procedures for retrieval of available SMS memory successful.

Message Statistics:

- CP Layer Messages:
  - CP Data (Tx) — The total number of protocol data units sent during connection setup.
  - CP Data (Rx) — The total number of protocol data units received during connection setup.
  - CP Ack (Tx) — The total number of Ack messages sent during connection setup.
  - CP Ack (Rx) — The total number of Ack messages received during connection setup.
  - CP Error (Tx) — The total number of protocol errors during connection setup in Tx message.
  - CP Error (Rx) — The total number of protocol errors during connection setup in Rx message.
- CP Error Cause Stats:
  - Network Failure (Tx)/(Rx) — The total number of protocol errors during connection setup due to network failure in Tx/Rx message.
  - Congestion (Tx)/(Rx) — The total number of protocol errors during connection setup due to congestion in Tx/Rx message.
  - Invalid TID (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid transaction ID (TID) in Tx/Rx message.
  - Invalid Semantic (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid semantics in Tx/Rx message.
  - Invalid Mand Info (Tx)/(Rx) — The total number of protocol errors during connection setup as mandatory information in Tx/Rx message is invalid.
  - Invalid Msg Type (Tx)/(Rx) — The total number of protocol errors during connection setup due to invalid Tx/Rx message type.
  - Invalid Prot State (Tx)/(Rx) — The total number of protocol errors during connection setup as protocol state in Tx/Rx message is invalid.
  - Invalid IE (Tx)/(Rx) — The total number of protocol errors during connection setup as information element in Tx/Rx message is invalid.
  - Protocol Error (Tx)/(Rx) — The total number of protocol errors during connection setup as protocol error in Tx/Rx message.
  - Undefined Cause (Tx)/(Rx) — The total number of protocol errors during connection setup due to unspecified error in Tx/Rx message.
- Message Drop Counters:
  - CP Data — The total number of CP data packets dropped during connection setup.
    - Retransmission Drops — The total number of data packets dropped during retransmission.
    - Unknown TID Drops — The total number of data packets dropped during connection setup due to unknown transaction ID (TID).

        - Invalid TID Drops — The total number of data packets dropped during connection setup due to invalid transaction ID (TID) received.

    - CP Ack — The total number of CP acknowledgement messages dropped during connection setup.
        - CP-ACK Drop for Invalid TID Rcvd — The total number of CP-Ack messages dropped during connection setup due to invalid transaction ID (TID) received.

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

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

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

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

- Message Drop Counters:
  - RP Data — The total number of RP data packets dropped during message relay.
  - RP Ack — The total number of RP acknowledgement messages dropped during message relay.
  - RP Error — The total number of RP data packets dropped during message relay due to error in connection.

- RP Decode Failures — The total number of messages dropped during message relay due to invalid transaction ID (TID) received.

General Statistics:

- Concatenated MO SMS — The total number of concatenated mobile originated SMS messages.
- CP Timer Expiry — The total number of events when timer expired during connection setup.
- TR1N Timer — The total number of events when TR1N timer expired during mobile terminated SMS is in wait state for RP-ACK.
- TR2N Timer — The total number of events when TR2N timer expired during mobile terminated SMS is in wait state to send RP-ACK.
- CP Data Retrans — The total number of protocol data units retransmitted during connection setup.
- RP Msg Encode Fail — The total number of message encoding failures during message relay.
- CP Data Tx Fail — The total number of protocol data units with Tx messages failed during connection setup.
- CP Data Inv TID — The total number of protocol data units with invalid transaction ID (TID) during connection setup.
- Max Retrans Reached — The total number of events when retransmission limit is exhausted during connection setup.
- SMSC Addr Restricted — The total number of SMSC addresses restricted.
- MO SMSC Addr Restricted — The total number of mobile originated SMSC addresses restricted.
- MT SMSC Addr Restricted — The total number of mobile terminated SMSC addresses restricted.
- CP-DATA No Cp Ack Rx — The total number of mobile terminated messages failed as no acknowledgement is received during connection setup.
  - Release Indication Waiting MO CP-ACK Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol acknowledgement messages that are being delivered.
  - Release Indication Waiting MO CP-DATA Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol data messages that are being delivered.
  - Release Indication Waiting MO CP-ERR Delivery — The total number of release indications waiting to be transferred between network and MS for mobile originated control protocol error messages that are being delivered.
  - Release Indication Waiting MT CP-DATA Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol data messages that are being delivered.
  - Release Indication Waiting MT CP-ACK Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol acknowledgement messages that are being delivered.

- Release Indication Waiting MT CP-ERR Delivery — The total number of release indications waiting to be transferred between network and MS for mobile terminated control protocol error messages that are being delivered.

- MT-SMS Failures:
  - IMSI Record Not Found — The total number of mobile terminated messages failed as IMSI record is not available.
  - Busy Subscriber — The total number of mobile terminated messages failed due to busy subscriber.
  - Detached Subscriber — The total number of mobile terminated messages failed due to detached subscriber.
  - MT Queue Full — The total number of mobile terminated messages failed as messaged queue was full.

Bulk Statistics

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

MME Schema

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

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

MME-SMS Schema

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

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

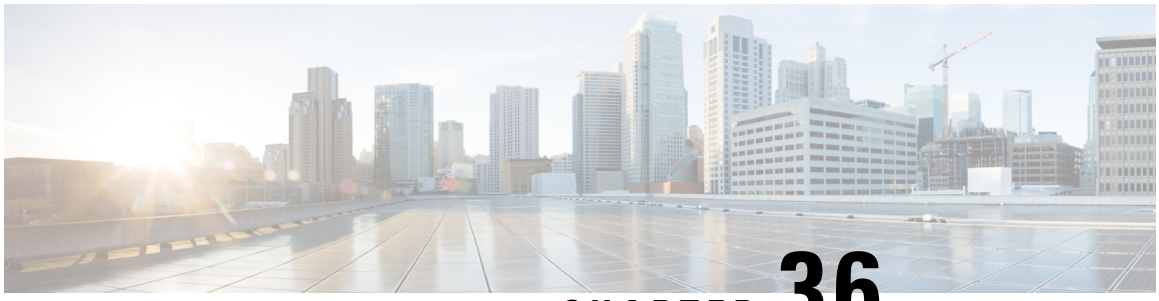
Bulk Statistics	Description
conn-prot-error-congestion-tx	The total number of protocol errors during connection setup due to congestion in Tx message.
conn-prot-error-congestion-rx	The total number of protocol errors during connection setup due to congestion in Rx message.
conn-prot-error-invalid-tid-tx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

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

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

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

Bulk Statistics	Description
conn-prot-timer-expiry	The total number of events when timer expired during connection setup.
tr1n-timer-expiry	The total number of events when TR1N timer expired during mobile terminated SMS is in wait state for RP-ACK.
tr2n-timer-expiry	The total number of events when TR2N timer expired during mobile terminated SMS is in wait state to send RP-ACK.
conn-prot-data-retrans	The total number of protocol data units retransmitted during connection setup.
relay-prot-msg-encode-fail	The total number of message encoding failures during message relay.
conn-prot-data-tx-fail	The total number of protocol data units with Tx messages failed during connection setup.
conn-prot-data-inval-tid	The total number of protocol data units with invalid transaction ID (ID) during connection setup.
conn-prot-max-retrans-reached	The total number of events when retransmission limit is exhausted during connection setup.
mt-fail-no-db-rec	The total number of mobile terminated messages failed as database record is not available.
mt-fail-conn-prot-data-no-ack-rcvd	The total number of mobile terminated messages failed as no acknowledgement is received during connection setup.
mt-fail-fwd-busy-subs	The total number of mobile terminated messages failed due to busy subscriber.
mt-fail-fwd-detached-subs	The total number of mobile terminated messages failed due to detached subscriber.
mt-fail-mt-queue-full	The total number of mobile terminated messages failed as messaged queue was full.



CHAPTER 36

show ip vrf CLI Syntax Changes

- Feature Summary and Revision History, on page 237
- Feature Changes, on page 237

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	All
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*Command Line Interface Reference, Modes E - F*

Revision History

Revision Details	Release
In this release, the syntax for **show ip vrf** CLI command has been changed across all platforms.	21.20.19

Feature Changes

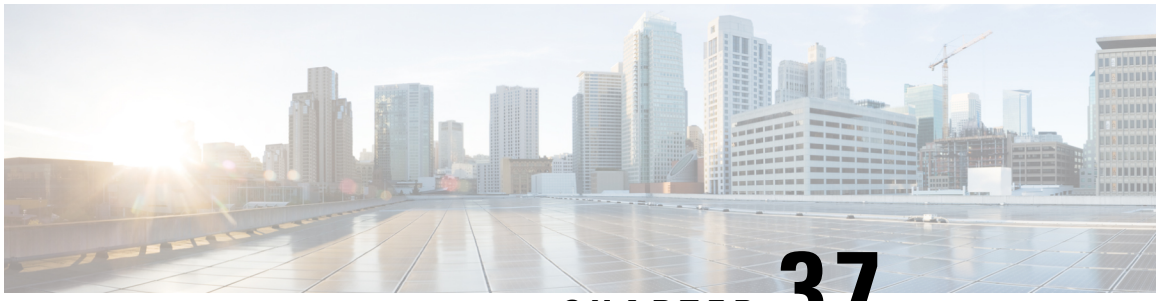
The syntax for **show ip vrf** CLI command has been changed across all platforms. However, there's no change in output of the CLI commands.

In releases prior to 21.20.19:

```
show ip vrf [  vrf_name [ mpls-map-dscp-exp ] ] ] | { grep grep_options | more
 ]
```

In 21.20.19 and 21.24 later releases:

show ip vrf [name *vrf_name* **[mpls-map-dscp-exp]]] | { grep** *grep_options* **| more]**



CHAPTER 37

show port npu counter Ouput Command Changes

- Feature Summary and Revision History, on page 239
- Bulk Statistics Command Output Changes, on page 240

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, **IPv4 MRU exceeded** counter is changed to **MRU exceeded** in the **show port npu counters** command output. Also, **ipv4-mru-excd-rx-frames** and **ipv4-mru-excd-rx-bytes** bulk statistics variable names are modified to **mru-excd-rx-frames** and **mru-excd-rx-bytes** in the schema file.	21.20.19

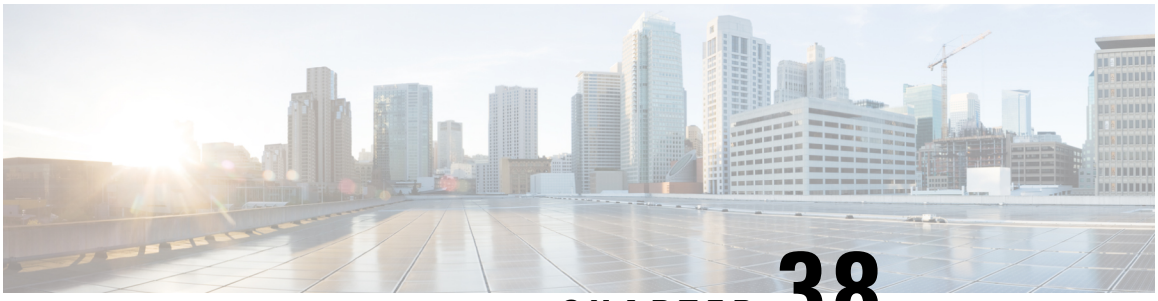
Bulk Statistics Command Output Changes

Previous Behavior: The **IPv4 MRU exceeded** counter that was displayed in the **show port npu counters** CLI command was specific to IPv4 packets.

New Behavior: The **IPv4 MRU exceeded** counter has been changed to **MRU exceeded** counter in the **show port npu counters** CLI command. This counter is a generic counter for all types of packet. The following Bulkstats variable names are changed:

- **ipv4-mru-excd-rx-frames** to **mru-excd-rx-frames** : The total number of received frames for packets where the Maximum Receive Unit (MRU) has been exceeded.
- **ipv4-mru-excd-rx-bytes** to **mru-excd-rx-bytes**: The total number of received bytes for packets where the MRU has been exceeded.

Customer Impact: Show command output and schema file changes are introduced to use new variable names.



CHAPTER 38

Support for Presence Reporting Area and Extended QOS on Offline Charging Interface for P-GW and SAEGW

- Feature Summary and Revision History, on page 241
- Feature Description, on page 242
- Handling Single and Multi-Presence Reporting Area on Rf Interface, on page 242
- Configuring IMS Authorization Service at Context Level, on page 245
- Configuring AAA Group, on page 246

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
This release supports Diameter offline charging on Rf interface for P-GW and SAEGW.	21.20.5

Feature Description

P-GW and SAEGW supports the following Attribute Value Pairs (AVP) and functionalities in diameter offline charging (RF) interface.

- **Originating-User-Location-Info** –This AVP holds value of 3GPP **User-Location-Info** AVP at the Packet Switch (PS) Information AVP in the Rf accounting (ACR) message for Long-Term Evolution (LTE) and General Packet Radio Service (GPRS).
- **Originating BSID** –This AVP holds value of 3GPP2-BSID AVP for Enhanced High-Rate Packet Data (eHRPD) at the PS Information AVP in the Rf accounting (ACR) message.
- **Grouped QoS-Information AVP with 5G-related sub-AVPs**– This AVP is enhanced with extended bit rates using 5G related sub AVP's. The 5G related sub AVP's are available at Service Data Container (SDC) level and **APN-AMBR** AVP values at PS level.
- **Presence Reporting Area Information** –P-GW and SAEGW supports the core network of signle and Multi Presence Reporting Area (PRA) information for only LTE and GPRS at Service Data Container (SDC) level in Rf accounting (ACR) message.
- **Change-Condition** –This AVP holds value of 24 for **Change of UE Presence in Presence Reporting Area** at SDC level in Rf accounting (ACR) message.

Limitations

The following are the limitations:

- User Equipment (UE) Dedicated Presence Reporting Area is not supported.
- Presence-Reporting-Area-Element-List AVP not supported. This AVP is applicable only for UE-Dedicated PRA support.

Handling Single and Multi-Presence Reporting Area on Rf Interface

During an IP-CAN session, the Policy and Charging Rules Function (PCRF) determines whether the reports for change of the UE presence in the Presence Reporting Area (PRA) are required for an IP-CAN session. If the reporting is required for the IP-CAN session, the PCRF provides PRA information AVP, which contains the PRA identifier within the **Presence-Reporting-Area-Identifier** AVP to the P-GW. The PCRF activates the reporting changes of the UE presence in the PRA by subscribing to the**CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT** event trigger at the P-GW at any time during the entire IP-CAN session.

When the UE enters or leaves the PRA, P-GW reports the **CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA** change condition in Rf messages (ACR-Interim). In addition, the P-GW reports the PRA identifier within **Presence-Reporting-Area-Identifier** AVP included in `Presence-Area-Information` AVP when UE is inside the PRA.

Handling both single and multiple Presence Reporting Area

To handle both single and multiple PRA:

- Add the **Change of UE Presence in Presence Reporting Area** value in **Change-Condition** AVP at SDC level every time when change of UE presence in PRA is received from access side along with other change conditions.
- P-GW includes:
  - extended MBR, GBR and APN-AMBR AVP values, if it received from PCRF or access side, to send in the accounting messages at SDC level
  - extended APN-AMBR AVP values, if it received from access or PCRF side, to send in the accounting messages at PS level
- Set the **Originating-User-Location-Info** AVP value during session creation for LTE/S4-SGSN RAT type when ULI IE received from access side and send value in ACR-Start message over Rf interface. Once Originating-User-Location-Info value is set, same value is sent in subsequent messages irrespective of any type of Hand Over (HO) for P-GW service.
- Set the **Originating-BSID** AVP value during session creation for eHRPD RAT type and send value in the ACR-Start message over Rf interface. Once Originating-BSID value is set, same value is sent in subsequent messages irrespective of any type of HO for P-GW service.

Note Originating-User-Location-Info AVP and Originating-BSID AVP values are not supported during session creation for 3G and WI-FI RAT types.

PRA Information IE are present in following messages:

- Create Session Request
- Create Bearer Response
- Modify Bearer Request
- Update Bearer Response

Behavior Matrix

The following table describes message type behavior for E-UTRAN.

Table 21: E-UTRAN

Message Type	Presence-Reporting-Area-Information AVP	Originating-User-Location-Info AVP	Originating-BSID AVP
Create-Session-Request	-	ACR-Start	ACR-Start
Modify-Bearer-Request	ACR-Interim	ACR-Interim	ACR-Interim
Create-Bearer-Response	ACR-Interim .	ACR-Interim	ACR-Interim
Delete-Session-Request	ACR-Stop	ACR-Stop	ACR-Stop
Delete-Bearer-Command	ACR-Interim/Stop	ACR-Interim/Stop	ACR-Interim/Stop
Update-Bearer-Response	ACR-Interim	ACR-Interim	ACR-Interim
Delete-bearer-Request	ACR-Interim/Stop	ACR-Interim/Stop	ACR-Interim/Stop

The following table describes RAT type behavior.

Table 22: RAT Type

RAT Type	Presence-Reporting-Area-Information AVP	Originating-User-Location-Info AVP	Originating-BSID AVP
3G/2G	Not Supported	Supported	Not Supported
E-UTRAN	Supported	Supported	Not Supported
NB-IOT	Not Supported .	Not Supported	Not Supported
Trusted-Wifi	Not Supported	Not Supported	Not Supported
Untrusted-Wifi	Not Supported	Not Supported	Not Supported
eHRPD	Not Supported	Not Supported	Supported

The following table describes Handoff expected behavior.

Table 23: Handoff

Handoff	Presence-Reporting-Area-Information AVP	Originating-User-Location-Info AVP	Originating-BSID AVP
E-UTRAN --> NB-IOT	Not Supported	Supported	Not Supported
NB-IOT --> E-UTRAN	Not Supported	Not Supported	Not Supported
E-UTRAN->3G/2G	Not Supported .	Supported	Not Supported

Handoff	Presence-Reporting-Area-Information AVP	Originating-User-Location-Info AVP	Originating-BSID AVP
E-UTRAN->3G/2G->E-UTRAN	Not Supported	Supported	Not Supported
3G/2G->E-UTRAN	Not Supported	Supported	Not Supported
3G/2G->E-UTRAN->3G/2G	Not Supported	Supported	NotSupported
E-UTRAN->WIFI	Not Supported	Supported	Not Supported
E-UTRAN->WIFI->E-UTRAN	Supported	Supported	Not Supported
WIFI->E-UTRAN	Supported	Not Supported	Not Supported
WIFI->E-UTRAN->WIFI	Not Supported	Not Supported	Not Supported
E-UTRAN --> eHRPD --> E-UTRAN	Supported	Supported	Not Supported
eHRPD --> E-UTRAN	Supported	Not Supported	Not Supported
eHRPD --> E-UTRAN --> eHRPD	Not Supported	Not Supported	Supported

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in LTE/ GPRS networks.

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter encode-supported-features
extended-bw-newradio multiple-pra cno-uli
                    diameter host-select table { 1 | 2 } algorithm
round-robin
                    diameter host-select row-precedence <precedence_value>
table { 1 | 2 } host <primary_host_name> [ realm <primary_realm_id> ] [ secondary
 host <secondary_host_name> [ realm <secondary_realm_id> ] ] [ -noconfirm ]
                    exit
```

Notes:

- <*context_name*> must be the name of the context where you want to enable IMSA service.

- *<imsa_service_name>* must be the name of the IMSA service to be configured for Rf interface authentication.
- **extended-bw-newradio**: Enables Extended Bandwidth with New-Radio feature.
- **multiple-pra** : Enables Multiple Presence Reporting Area Information Reporting feature.
- **cno-uli** : Enables Presence Reporting Area Information Reporting feature.

Configuring AAA Group

Use the following configuration commands to configure the Accounting group for Rf interface.

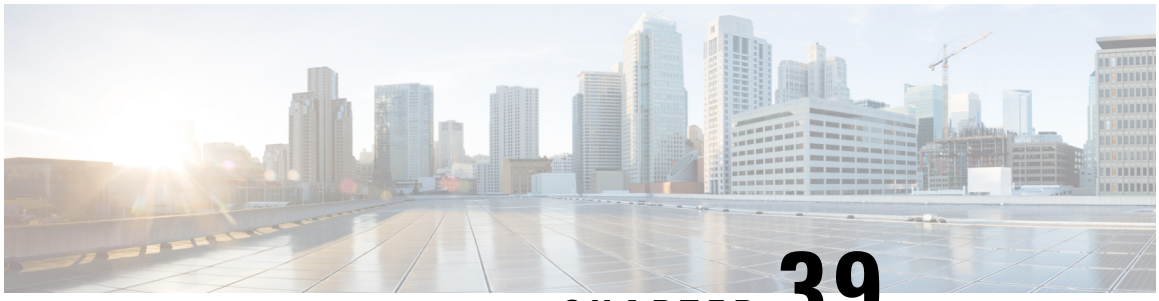
```
configure
   context context_name
         aaa group group_name
           diameter accounting dictionary {aaa-custom4 | aaa-custom3}
           diameter accounting endpoint rf
           diameter accounting server rf_server priority 1
         exit
```

Notes:

- **aaa group** *group_name*: Specifies the AAA server group. *group_name* must be an alphanumeric string of 1 through 63 characters.
- **diameter accounting dictionary** {*aaa-custom4* | *aaa-custom3}* : Enables aaaa-custom4 and aaa-custom3 diameter accounting dictionaries.

Note The Presence Reporting Area (PRA) and Extended QOS on Offline Charging Interface feature supports only {aaa-custom4 | aaa-custom3} dictionaries.

- **diameter accounting endpoint** : Enables diameter accounting endpoint on Rf interface.
- **diameter accounting server** *rf_server priority 1*: Enables multiple rf server priorities.



CHAPTER 39

Suppressing CCR-U Quota with Validity Timer

- Feature Summary and Revision History, on page 247
- Feature Description, on page 248
- Supressing CCR-U Quota with Validity Timer Running, on page 248

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First Introduced .	21.20.16

Feature Description

The Validity-Time Attribute Value Pair (AVP) is primarily used in the following conditions:

1. Granted-Service-Unit (GSU)
2. Final-Unit-Indication (FUI)

This feature deals only with Granted-Service-Unit (GSU). The validity time AVP contains the time for which the GSU is valid. After the expiry of Validity-Time, an update request is sent to the server to get a new GSU.

When the GSU is zero,then the P-GW sends an update request towards the Credit Control Server for every packet it receives, inspite the validity timer is still running in the existing behaviour.

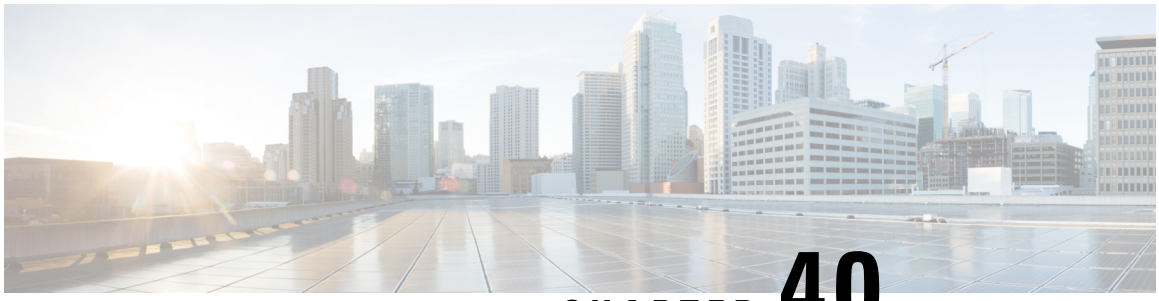
This existing behavior is enhanced, where there is no update request be sent towards Credit Control Server, even if GSU is zero and the validity timer is running. The new behavior is only valid when no Final-Unit-Indication AVP has come.

This is done by using the configuration command **suppress-ccru zero-gsu-with-validity-timer** to control the activity.

Supressing CCR-U Quota with Validity Timer Running

Use the following configuration commands to supress CCR-U quota with validity timer running:

```
configure
   active-charging-service service_name
     credit-control
      [ no ] diameter suppress-ccru-zero-gsu-with-validity-timer
         end
```



CHAPTER 40

Support for Tariff-Time-Change in Fast Path

- Feature Summary and Revision History, on page 249
- Feature Changes, on page 249

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

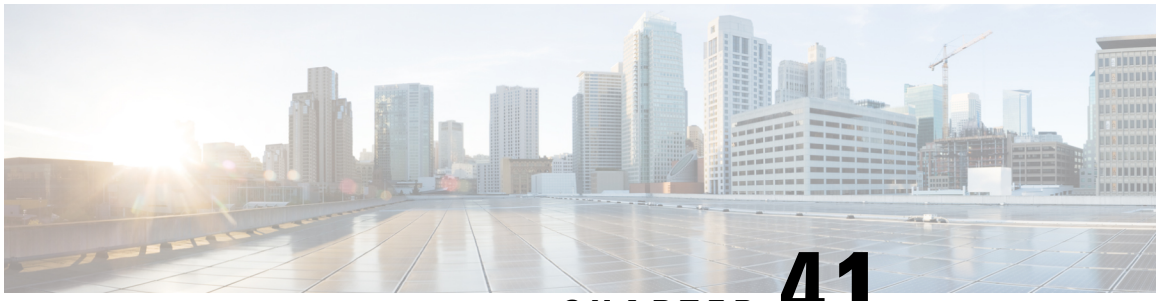
Revision Details	Release
Tariff-Time-Change AVP is supported in fast path.	• 21.25.4 • 21.20.22

Feature Changes

Previous Behavior: When the Tariff-Time-Change AVP was received from Gy for a Rating Group, traffic was switched to the slowpath and thus slowed down user's traffic.

New Behavior: When the Tariff-Time-Change AVP is received from Gy for a Rating Group, traffic continues to flow in the fast path and maintains the user's traffic rate.

Customer Impact: End-user will receive seamless traffic.



CHAPTER 41

TCP Reset with Invalid Sequence Number should not Trigger Connection Close

- Feature Summary and Revision History, on page 251
- Feature Changes, on page 252

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, the TCP RST segment will be sequence number validated.	• 21.25 • 21.20.25 • 21.15.60

Feature Changes

Previous Behavior: P-GW always accepted TCP RST Segments as valid and closed the TCP Data Connection Session on receiving a RST Segment.

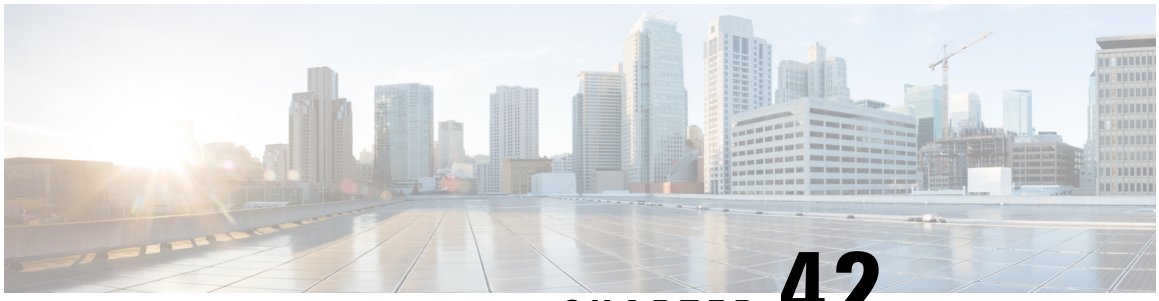
New Behavior: If a TCP RST Segment is received and the TCP FSM is in SYN-RCVD state, the TCP RST Segment is sequence number validated. Refer to RFC793 for more information.

If the validation fails (an invalid TCP RST segment), the TCP RST segment is not processed at P-GW and the TCP Data Connection is not closed. The TCP RST segment is passed on seamlessly to the destination.

If the TCP RST Segment is valid, then the normal TCP Data Connection teardown continues.

The new TCP RST Segment validation is only done in TCP FSM SYN-RCVD state. For other TCP FSM states, the behaviour has not changed.

Impact on Customer: TCP Data connection is not closed for invalid TCP RST Segment in SYN-RCVD state and flow at PDN-GW continues to be active.



CHAPTER 42

Writing Rf Charging Records to P-GW Hard Disk

- Feature Summary and Revision History, on page 253
- Feature Description, on page 253
- How it Works, on page 254
- Configuring aaa-group, on page 256

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release,writng Rf charging records to P-GW hard disk is supported.	21.20.5

Feature Description

The Rf charging record that gets transmitted from P-GW is an essential charging information. When you configure the system using Rf to write charging records, if there is a configuration error, for example,

misconfiguration of a diameter server or configured a wrong diameter accounting server and so on, loss of charging information and revenue loss can occur. To prevent charging record loss because of system errors, P-GW provides a function to write charging record ACR to P-GW local hard disk storage. Through CLI configuration, you can specify that on the ASR5500 chassis the hard disk on the DPC be used to store Diameter record storage. Diameter files are transferred from packet processing cards to the hard disk on the DPC.

How it Works

If the Diameter server used in the "aaa group" is not configured in the "diameter endpoint" or if no diameter server is configured, the Rf ACR record writes to local memory up to the number of configured maximum outstanding messages. If the system reboots, all message in the local memory will be lost.

The table below lists all the positive and negative cases after system writes charging ACR to diameter server.

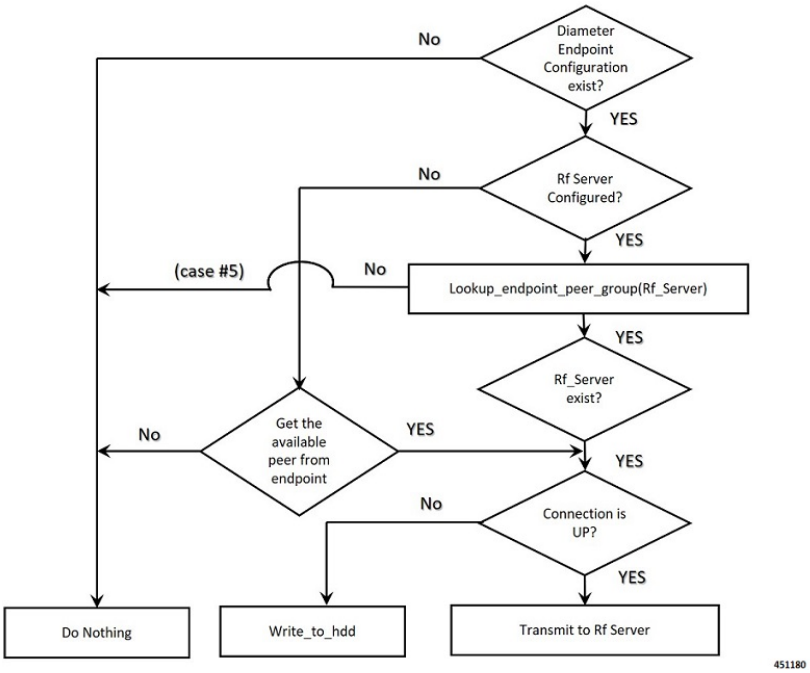
Table 24: Rf Record Writing Execution Cases in Current P-GW

Case#	Aaa group configuration	Diameter endpoint configuration	Server Connection States	Write to Hard Disk
1	Diameter accounting server A	Peer A	UP	NO, Everything right, Send to Rf server
2	Diameter accounting server A	Peer A	Down	YES
3	Diameter accounting server A	Peer A	Server A IP address does not exist (Server A exist in peer table, but the IP address is wrong)	YES
4	No accounting server configured	Peer A	UP or Down	• ACR is sent to the server if connection state is UP • ACR is written to HDD if the connection state is DOWN.

Case#	Aaa group configuration	Diameter endpoint configuration	Server Connection States	Write to Hard Disk
5	Diameter accounting server B	Peer A	Server B does not exist in peer table in endpoint	ACR is written to the archive list and pushed to the server when the connection is UP.

The following illustration shows the scenario when the Diameter accounting server B does not exist (case 5) and the P-GW Rf record writing logic scenario.

Figure 18: Call flow for Writing Rf Charging Record with Error



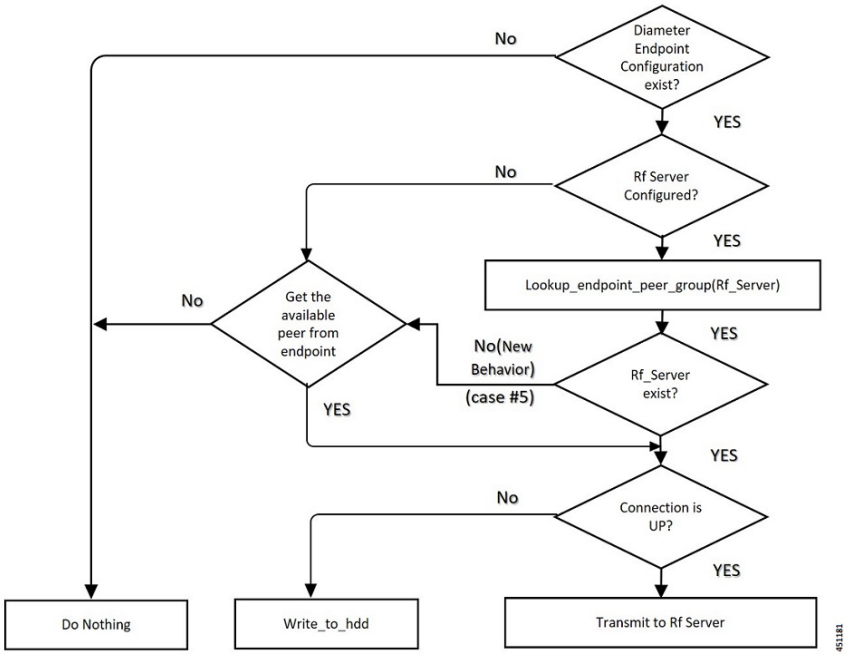
If the P-GW cannot find the server configured under **aaa group** within the diameter endpoint group, P-GW follows logic listed in the table:

Table 25: Writing Rf Charging Record Logic

Step	Description
1	P-GW receives the first available ACTIVE peer entry in the diameter endpoint and sends the ACR to the respective server.
2	If Step1 fails, none of the peer entries in the diameter endpoint are in ACTIVE state. The P-GW uses a random peer entry in the diameter endpoint and triggers the function to write ACR to local hard disk.

The following illustration shows the logic when the Diameter accounting endpoint is correctly configured under the aaa group.

Figure 19: Call Flow forWriting Rf Charging Record without Error



Note If multiple Diameter accounting servers are configured under the **aaa group**, the same logic (Step1 and Step2) applies for forwarding an ACR from P-GW.

Configuring aaa-group

Use the following commands to configure one or multiple diameter accounting servers as the CDF/CCF end points:

```
configure
   context context_name
      aaa group group_name
         diameter accounting endpoint endpoint_name
         diameter accounting serverhost_name
         exit
```

Notes

- **diamneter accounting endpoint**: Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use. *endpoint_name* must be a string of 1–63 characters.
- **diamter accounting server** : Configures Diameter host *host_name* from this AAA server group for Diameter accounting.

Writing Diameter Record to P-GW Local Hard Disk

The function of writing diameter record to local hard disk is disabled by default. To enable the function, configure the following commands under aaa group:

```
configure
   context context_name
      aaa group group_name
         diameter accounting hd-mode fall-back-to-local
         diameter accounting hd-storage-policy hd_policy
         exit
```

Notes

- **diamneter accounting hd-mode fall-back-to-local**: Specifies that records be copied to the local HDD if the Diameter server is down or unreachable. CDF/CGF pulls the records through SFTP.
- **diameter accounting hd-storage-policy** : Associates the specified HD Storage policy with the AAA group. *hd_policy* must be the name of a configured HD Storage policy, and must be an alphanumeric string of 1 through 63 characters. HD Storage policies are configured through the Global Configuration Mode. hd_policy and the hd-mode commands enable storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable