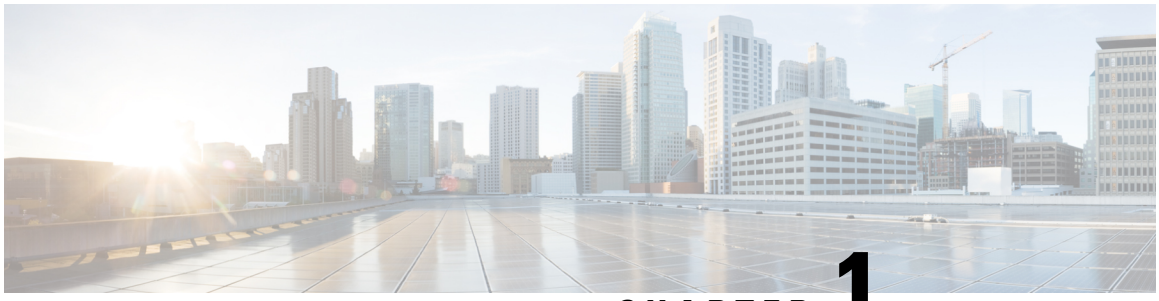
Release Change Reference, StarOS Release 21.15/Ultra Services Platform Release 6.9

First Published: 2019-08-29

Last Modified: 2021-09-27

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



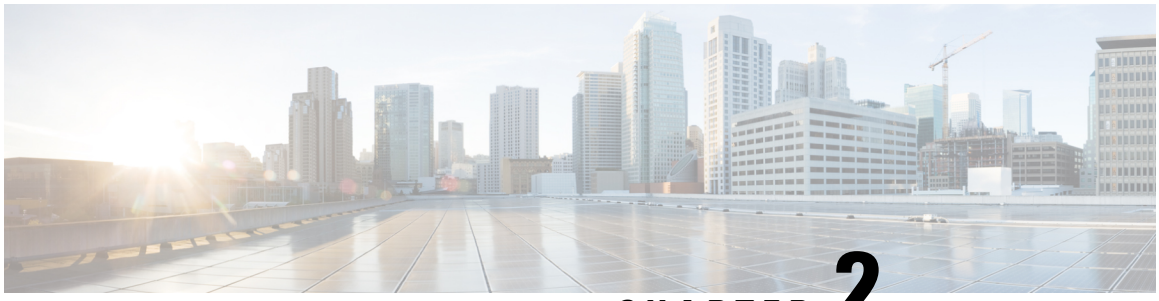
CHAPTER 1

Release 21.15/6.9 Features and Changes Quick Reference

Release 21.15/6.9 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Adding Discrete eNB IDs to eNB Group in MME, on page 9	MME	21.15
APN-OI based P-GW Selection, on page 13	MME	21.15
APN Rate Control for CIoT Devices, on page 15	C-SGN, P-GW	21.15
Deprecation of Manual Scaling, on page 25	UAS	6.0
ERAB Release if any ERAB Switch Fails, on page 27	MME	21.15
ERAB Setup Retry Handling, on page 31	MME	21.15
IPv4/IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW, on page 35	P-GW	21.15.52
HSS and AuC Interworking Configuration Enhancement, on page 37	MME	21.15
ICMPv6 Response for Fragmented Packets, on page 39	P-GW	21.15.x
Inner Fragmentation with VPP Non-CUPS Deployment, on page 41	P-GW	21.15.x
MEC Location Management, on page 43	MME	21.15

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
MME Handling of Purge Procedure, on page 51	MME	21.15.1
Migrating 3G to 4G Context , on page 53	P-GW	21.15.51
S-GW Address Based Combined SPGW Selection, on page 55	MME	21.15
TCP Reset with Invalid Sequence Number should not Trigger Connection Close, on page 57	P-GW	21.15.60
TAI-based Routing for 20-bit and 28-bit eNB ID, on page 59	MME	21.15



CHAPTER 2

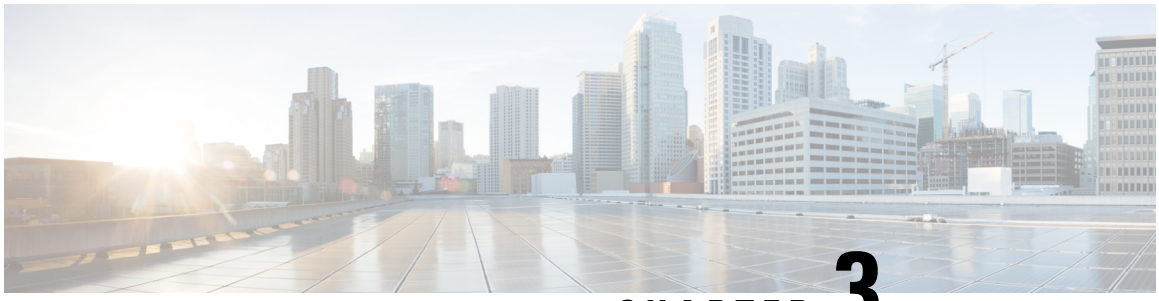
Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
Adding Discrete eNB IDs to eNB Group in MME	Disabled - Configuration Required
APN-OI Based PGW Selection	Disabled - Configuration Required
APN Rate Control for CIoT Devices	Disabled - License Required
Deprecation of Manual Scaling	Disabled - Configuration Required
ERAB Release if any ERAB Switch Fails	Enabled - Always-on
ERAB Setup Retry Handling	Disabled - Configuration Required
IPv4 or IPv6 Address Encoding Change in Flow-Description AVP for APPLICATION-START Event Trigger from P-GW	Disabled - Configuration Required
HSS and AuC Interworking Configuration Enhancement	Enabled - Always-on
ICMPv6 Response for Fragmented Packets	Enabled - Configuration Required
Inner Fragmentation with VPP non-CUPS deployment	Enabled - Configuration Required
MEC Location Management	Enabled - Always-on
MME Handling of Purge Procedure	Enabled - Configuration Required
Migrating 3G to 4G Context	Enabled - Configuration Required
S-GW Address Based Combined SPGW Selection	Disabled - Configuration Required
TCP Reset with Invalid Sequence Number should not Trigger Connection Close	Disabled - Configuration Required

Feature	Default
TAI-based Routing for 20-bit and 28-bit eNB ID	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.15 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 21.15 include:

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.15.

APN Schema

The following bulk statistics are added in the APN schema in support of the APN Rate Control for CIoT Devices feature.

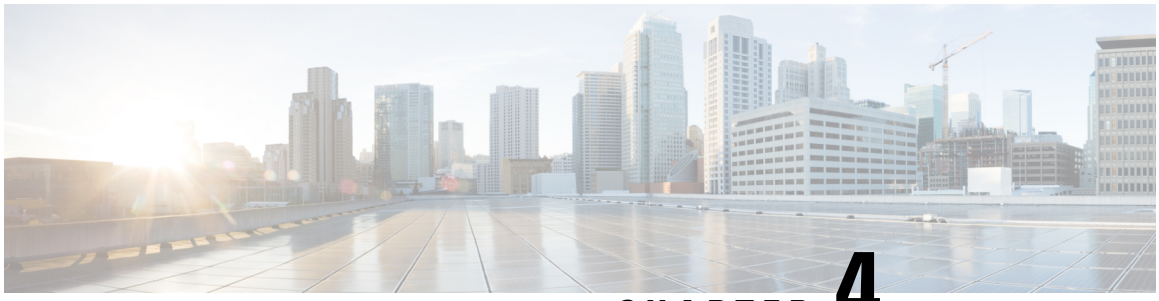
Bulk Statistics	Description
apn-rate-control-ul-pkt-drop	Indicates the total number of APN Rate Control uplink packets that are dropped.
apn-rate-control-dl-pkt-drop	Indicates the total number of APN Rate Control downlink packets that are dropped.
apn-rate-control-ul-bytes-drop	Indicates the total number of APN Rate Control uplink bytes that are dropped.
apn-rate-control-dl-bytes-drop	Indicates the total number of APN Rate Control downlink bytes that are dropped.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.16 and USP 6.10

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.16 and Ultra Services Platform (USP) 6.10 software releases.

SNMP MIB Object Changes for 21.15

This section provides information on SNMP MIB alarm changes in release 21.15.

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 21.15.

The following alarms are new in this release:

- starCFGSyncAbortReason
- starCFGSyncForUPlaneRedundancyAbort

Modified SNMP MIB Object

None in this release.

Deprecated SNMP MIB Object

None in this release.

SNMP MIB Alarm Changes for 21.15

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

SNMP MIB Conformance Changes for 21.15

This section provides information on SNMP MIB alarm changes in release 21.15.

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

New SNMP MIB Conformance

None in the release.

Modified SNMP MIB Conformance

None in the release.

Deprecated SNMP MIB Conformance

None in the release.

SNMP MIB Object Changes for 6.9

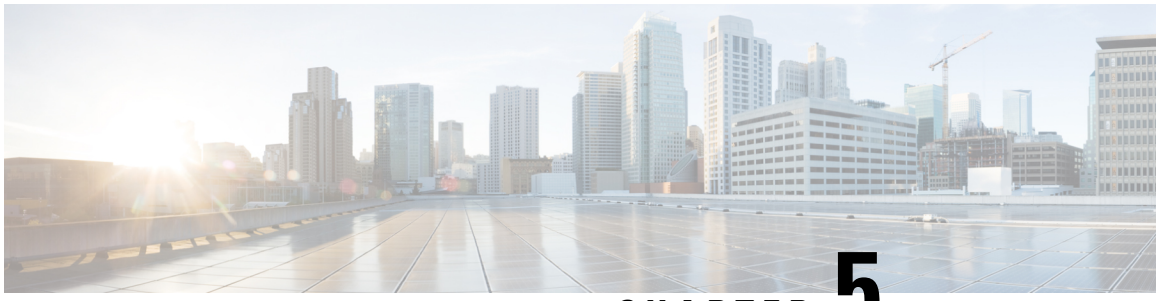
There are no new, modified, or deprecated SNMP MIB object changes in this release.

SNMP MIB Alarm Changes for 6.9

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

SNMP MIB Conformance Changes for 6.9

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



CHAPTER 5

Adding Discrete eNB IDs to eNB Group in MME

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
eNB Group configuration recommendation note is added.	21.15
First introduced.	21.14

Feature Description

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.

When the discrete eNB IDs are added to the eNB group, the MME sends the relative MME capacity value, which is configured in that eNB group, in the S1 setup response to those eNBs. Whenever the relative MME capacity for that eNB group is changed, the MME sends the MME Configuration Update message to those eNBs configured in that eNB group.

Adding Discrete eNB IDs to eNB Group in MME

This section provides information on the newly introduced CLI commands to configure discrete eNB IDs to the eNB Group in MME.

Adding the eNB Group

Use the following configuration to configure discrete eNB IDs in the eNB group.

```
configure
  lte-policy
    enb-group enb_group_name
      global-enb-id  [ enbid-list enbid_list_name |  prefix
network_identifier_name bits bits ]
      end
```

NOTES:

- **enbid-list** *enbid_list_name* : Specifies the eNB ID list with discrete eNB IDs. *enbid_list_name* must be a string of size 1 to 64.

  Important In an eNB Group, it is recommended to configure either Global eNB ID prefix or discrete eNB IDs, it is not recommended to configure both.

- **global-enb-id prefix** *network_identifier_name* **bits** *bits* : Specifies the Global eNB ID prefix that contains a bit string which should be matched with Hexadecimal value.*network_identifier_name* , This must be a hexadecimal number between 0x0 and 0xFFFFFFF.

  Important A maximum of 20 eNB groups can be configured at a time.

Adding the eNB ID List in the eNB Group

Use the following commands to configure discrete eNB IDs to be used in the eNB group.

```
configure
  lte-policy
    [ no ]enbid-list enbid_list_name
      [ no ]  enb-id discrete_eNB_id | enb-id-range from starting_eNB_id  to
ending_eNB_id
      end
```

NOTES:

- **no** : Disables the configuration of discrete eNB IDs.
- **enbid-list** *enbid_list_name* : Specifies eNB ID list with discrete eNB IDs.*enbid_list_name* must be a string of size string of size 1 to 64.
- **enb-id** *discrete_eNB_id*: Specifies the discrete eNB IDs. *discrete_eNB_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFF.

Important A maximum of 200 eNB IDs can be configured in an eNB id list. The enb-id-range can be a maximum of 64 per configured eNB ID list. However, if 200 eNB IDs are already configured, further enb-id-range configurations are not allowed. Duplicate eNB IDs per eNB ID list and across eNB ID list cannot be configured. Only two eNB ID lists can be configured such that discrete eNB IDs can be configured only in two eNB groups.

- **enb-id-range** : Specifies the range of discrete eNB IDs.
- **from** *starting_eNB_id* : Specifies the starting eNB ID in the range. *starting_eNB_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFF.
- **to** *ending_eNB_id* : Specifies the last eNB ID in the range. *ending_eNB_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFF.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the Adding Discrete eNB IDs to eNB Group in MME feature.

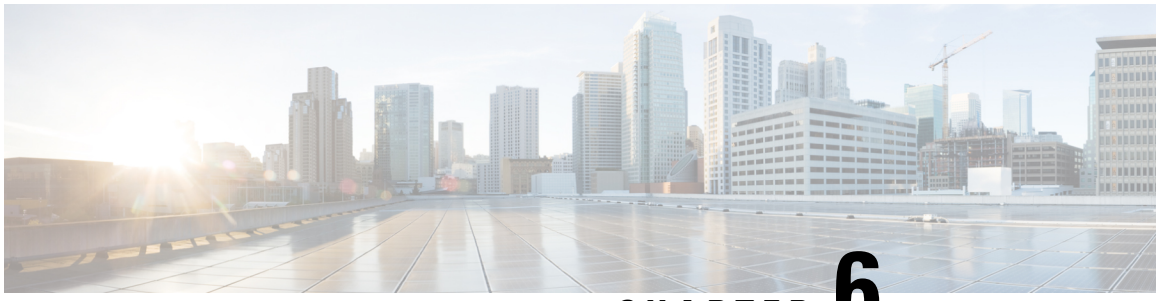
Show Commands and Outputs

show lte-policy enb-group name *enb_group_name*

The output of this command includes the following fields:

- eNB ID List Name
- Number of eNB IDs in the list

- List of eNB IDs



CHAPTER 6

APN-OI based P-GW Selection

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.15

Feature Description

The MME accepts a new format for the operator-identifier. When the configured APN matches with the APN that gets constructed with APN operator identifier (APN-OI), then the corresponding APN profile with the

P-GW address is selected. APN-OI-Replacement string from the ULA is in the format of ABCD.XYZ.MNCXXX.MCCYYY.GPRS or ABCD.MNCXXX.MCCYYY.GPRS.

MME selects P-GW based on the APN-OI-Replacement in the ULA message from HSS. MME is configured with ipv6.mnc009.mcc262.gprs/ KT5G.B2B.MNC009.MCC262.GPRS as the operator identifier. If this string matches with the APN-OI in the ULA message from HSS, then the configured P-GW is selected.

APN-OI Based P-GW Selection Configuration

This section describes how to configure APN-OI based P-GW Selection.

Modifying Operator Identifier

Use the following configuration to modify the operator identifier.

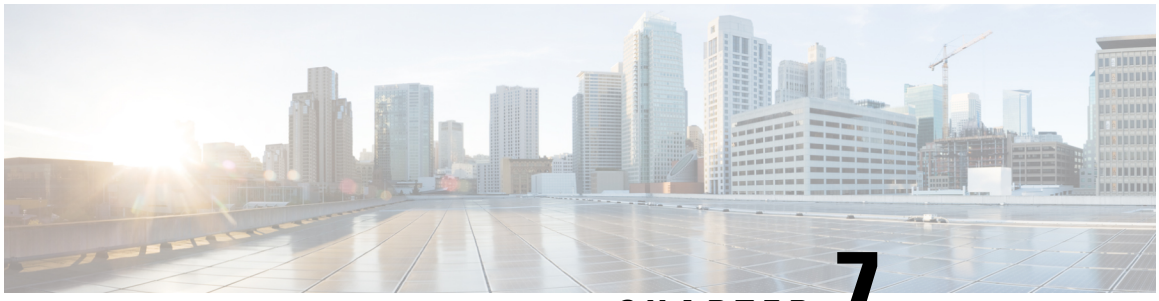
```
configure
   operator-policy name operator_policy_name
   apn{ network-identifier apn_net_id operator-identifier apn_op_id |
operator-identifier apn_op_id }[ apn-profile apn_profile_name ]
   end
```

NOTES:

- **apn** : Specifies the Access Point Name.
- **network-identifier***apn_net_id* : Links the specified APN network ID with the specified APN profile. *apn_net_id* must be an alphanumeric string of 1 through 63 characters, including dots (.) and dashes (-).
- **operator-identifier***apn_op_id* : Specifies the Operator identifier. *apn_op_id* must be a string of 1 to 39 characters in length 1 to 39, in format of [MNCxxx.MCCyyy.GPRS] / [ABCD.DEF.MNCxxx.MCCyyy.ZZZZ].

  Note With release 21.15, Operator Identifier can be configured in [ABCD.DEF.MNCxxx.MCCyyy.ZZZZ] format in addition to existing [MNCxxx.MCCyyy.GPRS] format.

- **apn-profile** *apn_profile_name*: Associates APN Profile. *apn_profile_name* must be a string of size 1 to 64 characters in length.



CHAPTER 7

APN Rate Control for CIoT Devices

This chapter contains the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• C-SGN • P-GW
Applicable Platform(s)	• UGP • VPC-DI • VPC-SI
Feature Default	Disabled - License Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference* • *Ultra IoT C-SGN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.15

Feature Description

In usual scenarios, CIoT-enabled UE send data packets infrequently. However, in unusual scenarios, UE can send data packets frequently during a short period resulting in network congestion and affecting services. APN Rate Control is one of the 3GPP standards-compliant mechanisms for rate limiting when UEs send data packets.

APN Rate Control allows Home Public Land Mobile Network (HPLMN) operators to control the amount of user data sent in Downlink (DL) and Uplink (UL). This is done with help of policing the user data on a maximum number of user data packets per time-unit, and/or maximum number of user data octets per time-unit, for both DL and UL.

How it Works

APN Rate Control policing for DL is done in the P-GW or the SCEF, and the APN Rate Control policing for UL is done in the UE. The P-GW or SCEF can also do APN Rate Control UL policing. For more information on:

- APN Rate Control UL in the UE, see 3GPP TS 24.301.
- APN Rate Control in the SCEF, see 3GPP TS 29.128.

Note The existing AMBR mechanisms are not suitable for APN Rate Control for CIoT Devices considering radio efficiency and UE battery-life. For example, an AMBR greater than 100 Kbps translates to a potentially large daily data volume.

The P-GW or Service Capability Exposure Function (SCEF) sends an APN Uplink Rate Control command to the UE using the PCO information element (IE). The APN Uplink Rate Control applies to data PDUs sent on that APN by either Data Radio Bearers (S1-U) or Signaling Radio Bearers (NAS Data PDUs). The UE complies with this uplink rate control instruction. The UE considers the rate control instruction as valid until it receives a new one from either P-GW or from SCEF. The P-GW or SCEF enforces the Uplink Rate Control by discarding or delaying packets that exceed the rate as indicated to the UE.

APN Rate Control Indications

APN Rate Control Indication Status is sent as part of Protocol Configuration Options (PCO)/Extended Protocol Configuration Options (ePCO). If P-GW/MME supports the ePCO as part of its capability exchange, the P-GW/S-GW sends the APN Rate Control parameters as part of ePCO. If ePCO is not supported by these entities, the P-GW/S-GW sends the APN Rate Control parameters as part of PCO.

As part of PCO/ePCO, the APN Rate Control parameters are sent as “additional parameters list”. A specific “container identifier” identifies the type of the parameter that is carried in a container. The “container identifier” related to the APN Rate Control are:

- Mobile Station (MS) to network direction:
  - 0016H (APN rate control support indicator)
  - 0019H (Additional APN rate control for exception data support indicator)
- Network to MS direction:
  - 0016H (APN rate control parameters)
  - 0019H (Additional APN rate control for exception data parameters)

When the “container identifier” indicates APN Rate Control support indicator, the “container identifier contents” field is empty and the “length of container identifier contents” indicates a length equal to zero. If the “container identifier contents” field is not empty, it is ignored. This information indicates that the MS supports APN Rate Control functionality.

When the “container identifier” indicates APN Rate Control parameters, the “container identifier contents” field contains parameters for APN Rate Control functionality.

When the “container identifier” indicates Additional APN Rate Control for exception data support indicator, the “container identifier contents” field is empty and the “length of container identifier contents” indicates a length equal to zero. If the “container identifier contents” field is not empty, it is ignored. This information indicates that the MS supports additional APN Rate Control for exception data functionality.

When the “container identifier” indicates Additional APN Rate Control for exception data parameters, the “container identifier contents” field contains parameters for additional APN Rate Control for exception data functionality.

APN Rate Control Status

APN Rate Control Status is the new IE, added as part of Create Session Request (CSReq), Delete Bearer Request (DBReq), and Delete Session Response (DSRes), which holds information of APN Rate Control Value. This IE is encoded as part of CSReq on the UR reattach to denote the P-GW about the remaining limits available for the subscriber on the current timeout period.

P-GW includes this IE when the DBReq is sent only for the default bearer, so that it can be used when the UE is attaching again. In addition, the P-GW includes this IE when the DSRes is sent to MME through S-GW.

	Bits								
Octets	8	7	6	5	4	3	2	1	
1	Type = 204 (decimal)								
2 to 3	Length = n								
4	Spare				Instance				
5 to 8	Number of Uplink packets allowed								
9 to 12	Number of additional exception reports								
13 to 16	Number of Downlink packets allowed								

17 to 24	APN Rate Control Status validity Time	
25 to (n+4)	These octet(s) is/are present only if explicitly specified	

Octets 17 to 24 are coded as time in seconds relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where the binary encoding of the integer part is in the 32 most significant bits, and binary encoding of the fraction part in the 32 least significant bits. The fraction part is expressed with a granularity of 1/2**32 second.

The APN Rate Control Status information is sent by P-GW to MME through S-GW to store the APN Rate control parameters in Mobility Management (MM) context. This helps in restoring the rate control for the same subscriber when it is reestablished again after some time. The parameters are treated as the remaining messages on the remaining time period of the time-unit.

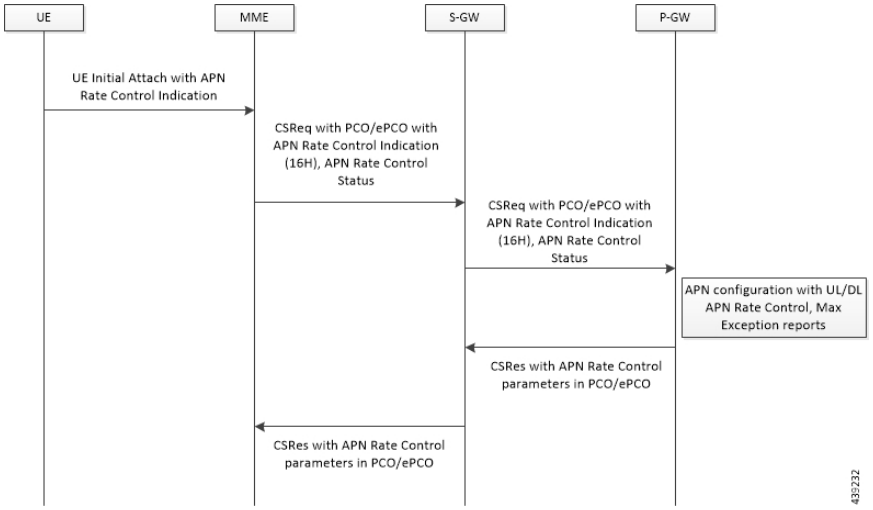
On reestablishment of the same subscriber (on first PDN for the same APN), the MME provides the information back to P-GW in PCO/ePCO. While processing, P-GW considers the values received from MME instead of its local configuration until the first timeout is complete.

Call Flows

This section describes the features' key call flows.

APN Rate Control Handling at P-GW on CSReq

On establishment or re-establishment of the subscriber for the APN, the MME sends the Indication Flags of APN Rate limit, Addition Exception indication, and APN Rate Control status in the CSReq.



Steps	Description
1	UE Initial Attach with APN Rate Control Indication is sent from UE to MME.
2	On receiving CSReq, the P-GW considers the APN Rate Control Status while encoding the APN Rate Control parameters in PCO, and while enforcing the APN Rate Control.
3	P-GW has two options to enforce the APN Rate Control:

Steps	Description
	1. On subsequent establishment of the first PDN connection for the given APN, the P-GW/SCEF receives the previously stored APN Rate Control Status, and if the first APN Rate Control validity period has not expired, it applies the received APN Rate Control Status and provides the related parameters to the UE in the PCO (instead of the configured APN Rate Control parameters). 2. If the initially applied parameters differ from the configured APN Rate Control parameters, the P-GW/SCEF uses the configured APN Rate Control parameters after the first APN Rate Control validity period expires, and sends an update to the UE with the configured APN Rate Control parameters.
4	P-GW sends CSRes to S-GW. P-GW prepares and encodes the APN Rate Control parameter into PCO/ePCO and sends back to S-GW in CSRes message with APN Rate Control parameters and Additional APN rate control parameters for exception data.
5	S-GW forwards the information (received from P-GW in Step 4) to MME.

APN Rate Control Parameter encodes information about Uplink time-unit and the Uplink rate supported.

8	7	6	5	4	3	2	1	
Spare				AER	Uplink time-unit			Octet 1
Maximum uplink rate								Octet 2 to Octet 4

Additional APN Rate control parameter for exception data encodes information about Uplink time-unit and the Uplink rate that is supported for the additional exception data.

8	7	6	5	4	3	2	1	
Spare					Uplink time-unit			Octet 1
Additional uplink rate for exception data								Octet 2 to Octet 3

Where Uplink Time-unit can take the value of any one as shown in the following format.

Uplink time-unit (Octet 1)	
Bit	
3 2 1	
0 0 0	Unrestricted
0 0 1	Minute
0 1 0	Hour
0 1 1	Day

1 0 0	Week

Maximum uplink rate (Octet 2 to Octet 4) is a binary coded representation of the maximum number of messages the UE is restricted to and sent per time-unit. If the uplink time-unit is set to "unrestricted", the maximum uplink data volume the UE can send is not restricted.

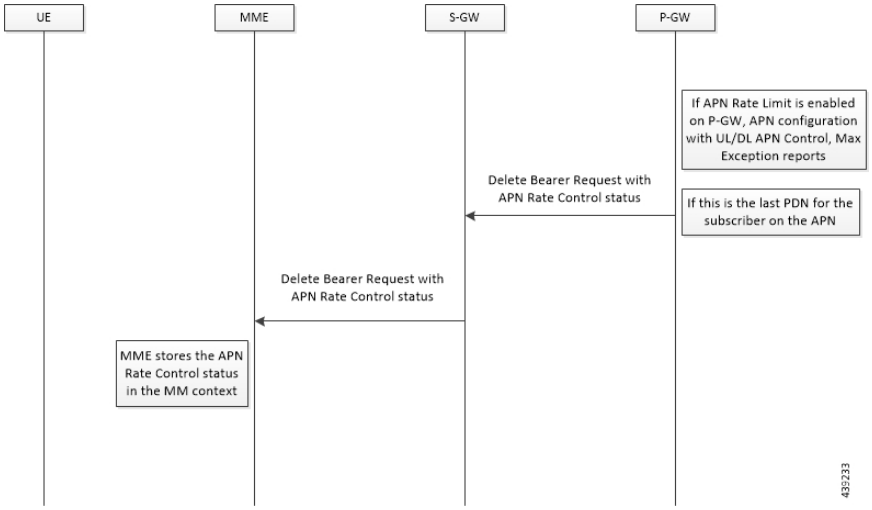
P-GW informs MME about UL APN Rate Control information in APN Rate Control Parameter, which is later stored by MME in MM context.

P-GW side APN Rate Control is based on “Maximum Allowed Rate” per direction. If P-GW provided the “number of additional allowed exception report packets per time unit” to the UE, then the "maximum allowed rate" is equal to the “number of packets per time unit” plus the “number of additional allowed exception report packets per time unit”. Otherwise, the “maximum allowed rate” is equal to the “number of packets per time unit”.

The P-GW enforces the uplink rate by discarding or delaying packets that exceed the “maximum allowed rate”. The P-GW enforces the downlink rate by discarding or delaying packets that exceed the downlink part of the “maximum allowed rate”.

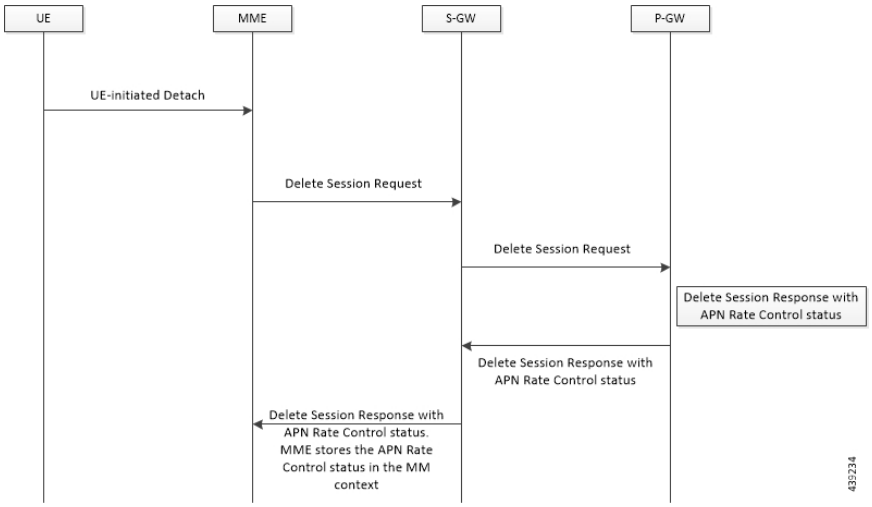
APN Rate Control Handling at P-GW on DBReq

On bearer deletion, if P-GW detects the current bearer is going to be the last bearer in the PDN for that specified APN, then it includes the APN Rate control status to MME through S-GW with the current quota of the rate limiting values (remaining messages on the remaining time-unit).



APN Rate Control Parameters on DSRes

On receiving the DSReq, P-GW clears the subscribers and sends the APN Rate Control status in CSRes with the remaining quota of the time and the messages for the subscriber to MME to update its MM context.



Licensing

The APN Rate Control for CIoT Devices is a license-controlled feature. Contact your Cisco Account representative for more information.

Standards Compliance

The APN Rate Control for CIoT Devices feature complies with the following standards:

- 3GPP TS 29.274 v15.8.0 - 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 23.401 v15.7.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

Limitations and Considerations

The APN Rate Control for CIoT Devices feature has the following limitations and restrictions:

- This feature takes highest priority and checks if the rate limit is done before checking for any other feature.
- Both uplink and downlink rate limit take same time-unit (unlimited, minute, hour, day, or week) value. It never accepts different values.
- Applicable for P-GW and Collapsed calls.
- Applicable only for CIoT subscribers; check on RAT Type is done to identify the CIoT subscribers.
- Applicable only for the CIoT IP PDNs. This feature is not applicable for Non-IP PDNs.
- In case of reattach, P-GW sends the CSRes with APN Rate Control parameters which are remaining for the subscriber to UE to perform Uplink Rate control operation. On time-unit expiry, P-GW renews its quota, but it never shares the updated quota values to UE. UE gets the P-GW configured APN Rate Control values only at initial attach.

- If Virtual-APN concept is applied on the subscriber, the Gi-APN Rate Control parameters are considered.

Configuring the APN Rate Control for CIoT Devices Feature

Use the following configurations to enable the feature.

```
configure
  context context_name
    apn apn_name
      iot-rate-control time-unit { unrestricted | mins | hours | days |
 week } downlink packet-count dl_packet_count uplink packet-count ul_packet_count
 aer aer_value
      end
```

NOTES:

- **time-unit { unrestricted | mins | hours | days | week }**: Specifies the mode of time-unit.
- **downlink**: Applies the APN Rate Control in the downlink direction.
- **packet-count** *dl_packet_count*: Specifies the allowed number of downlink packets. The *dl_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on the downlink direction.
- **uplink**: Applies the APN Rate Control in the uplink direction.
- **packet-count** *ul_packet_count*: Specifies the allowed number of uplink packets. The *ul_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on the uplink direction.
- **aer** *aer_value*: Specifies the number of Additional Exception Reports (AER) in the uplink direction. The *aer_value* must be an integer ranging from 1 through 65535.
- If previously configured, use the **no iot-rate-control** CLI command to disable the feature.

Monitoring and Troubleshooting the APN Rate Control for CIoT Devices Feature

This section describes the CLI commands available to monitor and/or troubleshoot the feature.

Show Command Support

The following show CLI commands are available in support of the feature.

show apn statistics

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control:
  - Dropped UL packets: Displays the total number of APN Rate Control uplink packets that are dropped.

- Dropped DL packets: Displays the total number of APN Rate Control downlink packets that are dropped.
- Dropped UL bytes: Displays the total number of APN Rate Control uplink bytes that are dropped.
- Dropped DL bytes: Displays the total number of APN Rate Control downlink bytes that are dropped.

show session subsystem facility sessmgr all debug-info

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control
  - Dropped UL packets: Displays the total number of APN Rate Control uplink packets that are dropped.
  - Dropped DL packets: Displays the total number of APN Rate Control downlink packets that are dropped.
  - Dropped UL bytes: Displays the total number of APN Rate Control uplink bytes that are dropped.
  - Dropped DL bytes: Displays the total number of APN Rate Control downlink bytes that are dropped.

show subscriber full all

The output of this CLI command has been enhanced to display the following feature-specific parameters.

- CIoT APN Rate Control:
  - Allowed UL limit: Displays the number of packets allowed for uplink direction.
  - Allowed DL limit: Displays the number of packets allowed for downlink direction.
  - Remaining UL limit: Displays the number of packets remaining for uplink direction.
  - Remaining DL limit: Displays the number of packets remaining for downlink direction.
  - Allowed Time unit: Displays the time-unit configured in either unrestricted, minutes, hours, days, or week mode.
  - Status Validity Time: Displays the validity time in YYYY-MM-DD HH:MM:SS format.

Bulk Statistics

This section provides information on the bulk statistics for the APN Rate Control for CIoT Devices feature.

APN Schema

The following bulk statistics are available in the APN schema in support of the APN Rate Control for CIoT Devices feature.

Bulk Statistics	Description
apn-rate-control-ul-pkt-drop	Indicates the total number of APN Rate Control uplink packets that are dropped.

Bulk Statistics	Description
apn-rate-control-dl-pkt-drop	Indicates the total number of APN Rate Control downlink packets that are dropped.
apn-rate-control-ul-bytes-drop	Indicates the total number of APN Rate Control uplink bytes that are dropped.
apn-rate-control-dl-bytes-drop	Indicates the total number of APN Rate Control downlink bytes that are dropped.

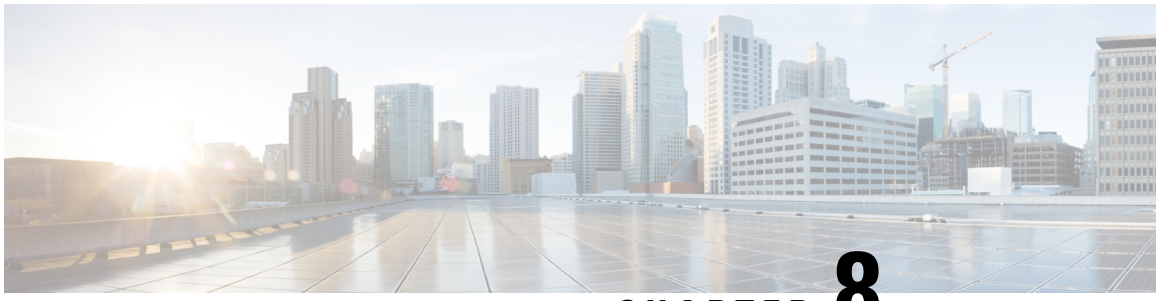
Accounting Support

The following table provides details of the GTPP dictionary available in support of the APN Rate Control for CIoT Devices feature.

CDR Dictionaries/Fields	
Type of dictionary change (New/Modified):	Modified
Dictionary name:	P-GW custom24 GTPP dictionary
Based on (3GPP specification):	3GPP TS 32.299
Applicable record type(s):	G-CDR
Applicable product:	P-GW

The following CDR fields are introduced in the P-GW custom24 GTPP dictionary:

1. Field name: datapacketsFBCDownlink
   - Description: Downlink Packets count
   - Format: Integer
   - CLI command to configure the field: **gtpp fbc-downlink-pkt-cnt**
   - Default value for field: 0
2. Field name: datapacketsFBCUplink
   - Description: Uplink Packets count
   - Format: Integer
   - CLI command to configure the field: **gtpp fbc-uplink-pkt-cnt**
   - Default value for field: 0



CHAPTER 8

Deprecation of Manual Scaling

Feature Summary and Revision History

Summary Data

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

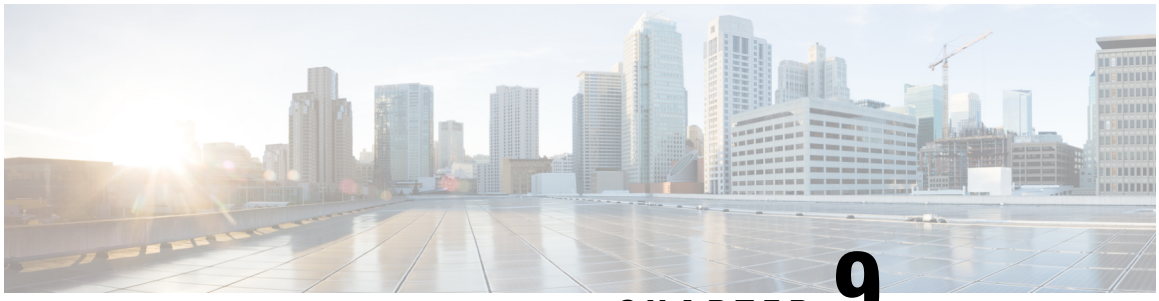
Revision History

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

Feature Changes

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

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



CHAPTER 9

ERAB Release if any ERAB Switch Fails

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.15

Feature Description

With Release 21.15, MME includes ERAB to "To Be Released List" IE in PATH SWITCH REQUEST ACKNOWLEDGE during X2 handover collision scenarios.

How It Works

This section describes how the ERAB release if any ERAB Switch Fails.

Flows

Figure 1: X2 handover without SGW Relocation

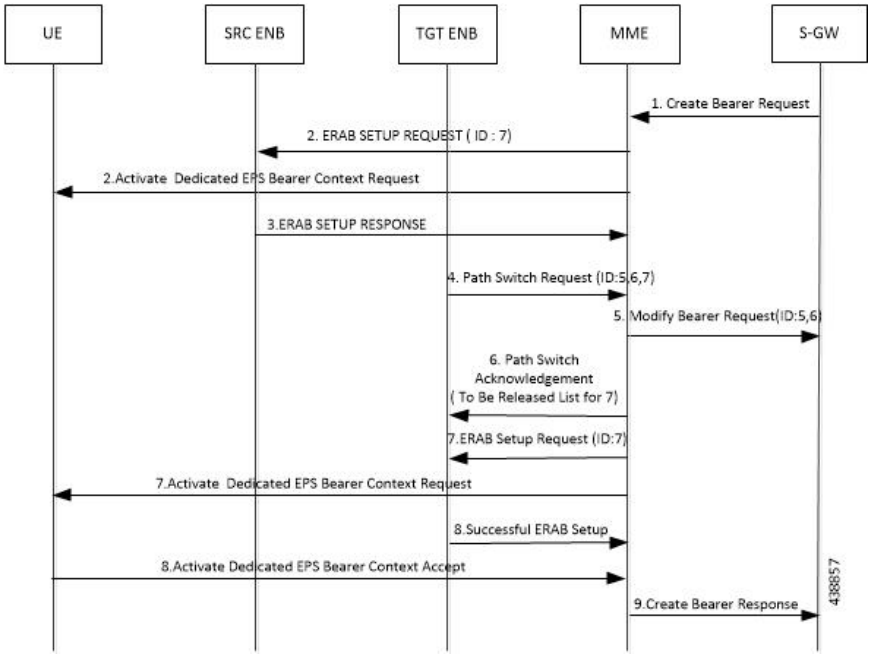


Table 1: Scenario 1

Steps	Description
1.	MME receives create bearer request for the dedicated bearer.
2.	MME sends eRAB setup and activate dedicated EPS bearer (ID: 7).
3.	ENB1 accepts eRAB setup.
4.	ENB2 sends path switch request with ID 5, 6, and 7.
5.	MME sends modify for 5 and 6, but 7 is not sent as setup is completed.
6.	MME responds with path switch acknowledge with "To Be Released List" for 7.
7.	MME sends Activate Dedicated EPS Bearer over E-RABSetup request for erab id 7.
8.	ENB2 sends E-RAB setup response.
9.	MME sends Create bearer response to S-GW.

Figure 2: X2 Handover with SGW Relocation:

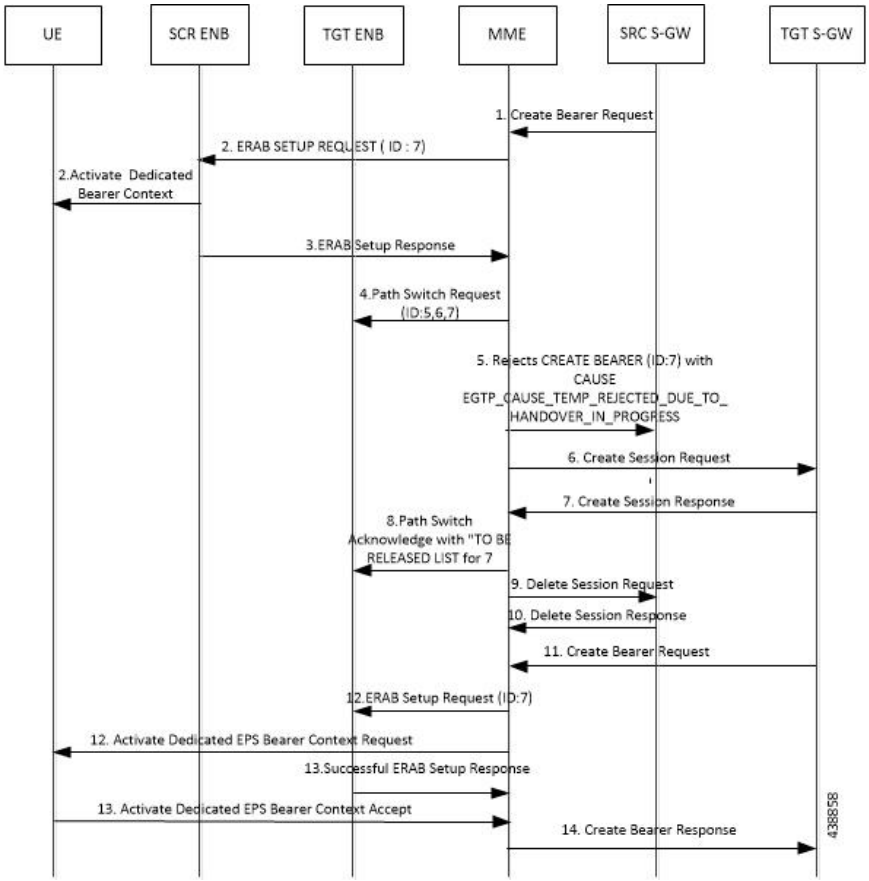
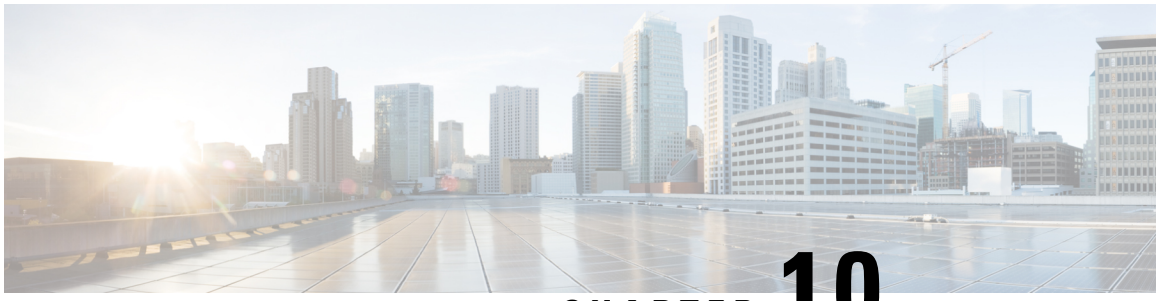


Table 2: Scenario 2

Steps	Description
1.	MME receives create bearer request for dedicated bearer.
2.	MME sends eRAB setup and activate dedicated EPS bearer (ID: 7).
3.	ENB1 accepts eRAB setup.
4.	ENB2 sends path switch request with ID 5, 6, and 7.
5.	MME rejects create bearer with cause: “EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS” to source S-GW (SGW1).
6.	MME sends create session request to target S-GW (SGW2).
7.	SGW2 responds with create session response.
8.	MME responds with path switch acknowledge to target enode B (ENB2), with bearer ID 5 and 6. ERAB Id 7 will be added under “To be released List”.

Steps	Description
9.	MME sends delete session request to SGW1.
10.	SGW1 responds with delete session response.
11.	If target S-GW retries to rejected bearer, then a create bearer is sent from SGW2 to MME.
12.	MME sends eRAB setup and activate dedicated EPS bearer (ID: 7).
13.	ENB ENB2 sends E-RAB setup response.
14.	Create bearer will be successful.

Note If MME did not get an acknowledgement from UE for NAS message (ACTIVATE_DEDICATED_EPS_BEARER_CONTEXT_REQUEST) or if MME has rejected that create bearer due to handover after successful ERAB establishment, then that ERAB ID is added to “To Be Released List” which is ERAB ID 7 under path switch acknowledge. When MME tries again to set up a ERAB SETUP request for ERAB ID 7, MME receives a successful response from Enode B2.



CHAPTER 10

ERAB Setup Retry Handling

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

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

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

Feature Changes

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

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

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

Command Changes

erab-setup-rsp-fail retry-timer

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

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

NOTES:

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

Performance Indicator Changes

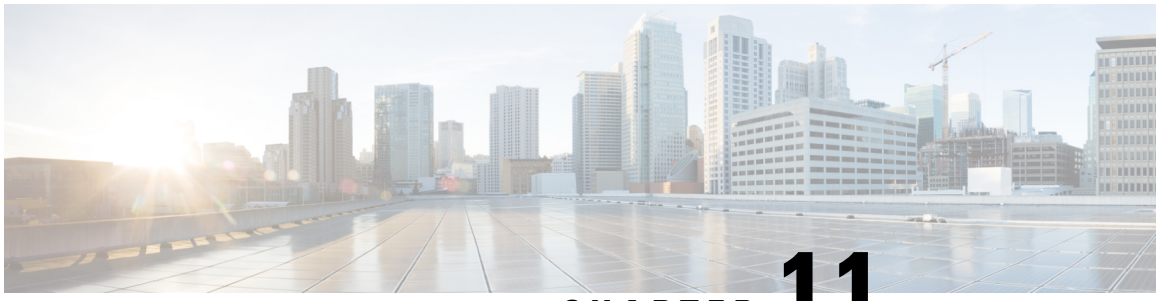
show mme-service name <mme_svc_name>

The output of this command includes the following fields:

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

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

show mme-service name <mme_svc_name>



CHAPTER 11

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

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 21.15.52 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

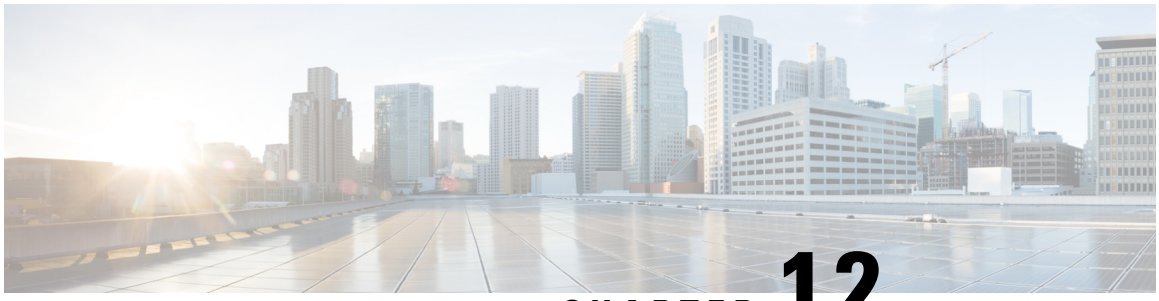
Previous Behavior: In CCR-U for APPLICATION-START event trigger from P-GW, Flow-Description AVP under Application-Detection-Information AVP towards PCRF was encoded as:

- 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 12

HSS and AuC Interworking Configuration Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

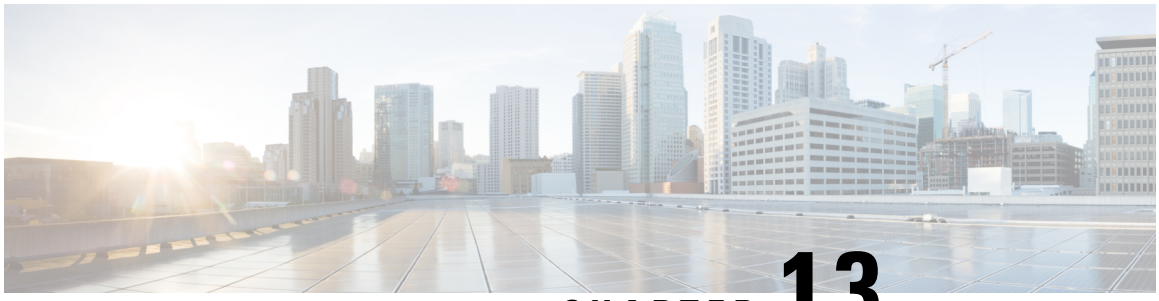
Revision Details	Release
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. This feature is fully qualified in this release.	21.20
The maximum number of HSS Peer Services that can be created and configured has been increased from 96 to 128. **Important**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

Feature Description

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

Note

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



CHAPTER 13

ICMPv6 Response for Fragmented Packets

Feature Summary and Revision History

Summary Data

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

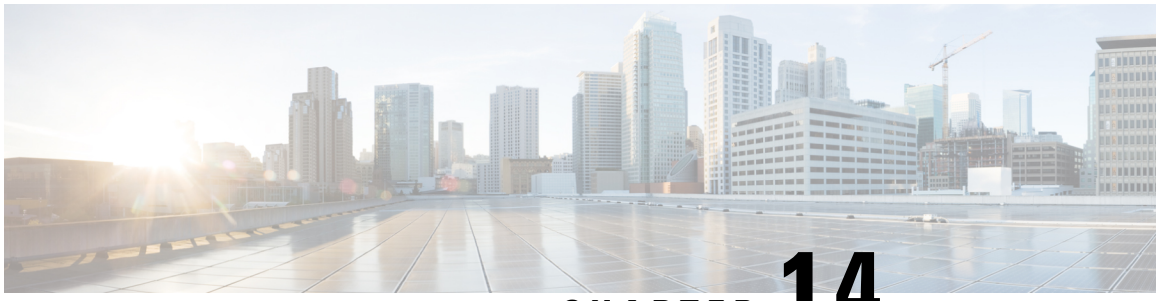
Revision Details	Release
In this release, P-GW supports Inner Fragmentation with VPP Non-CUPS Deployment.	21.15.x

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 14

Inner Fragmentation with VPP Non-CUPS Deployment

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

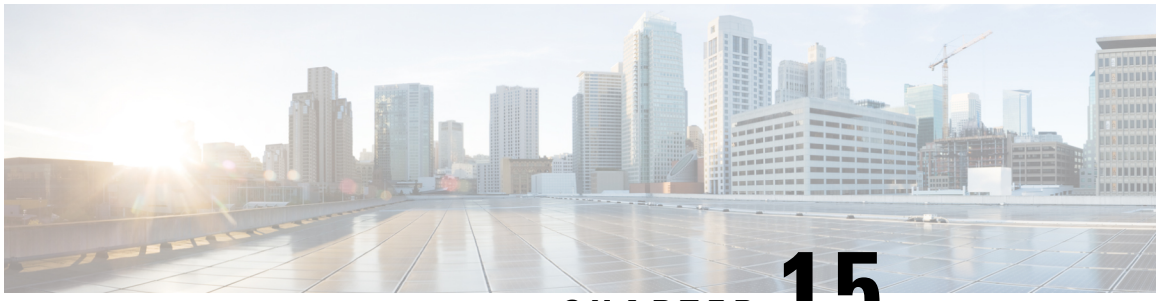
Revision Details	Release
In this release, P-GW supports Inner Fragmentation with VPP Non-CUPS Deployment.	21.15.x

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 15

MEC Location Management

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
PGW-U IP address is used for User Plane address.	21.15
First introduced.	21.14

Feature Description

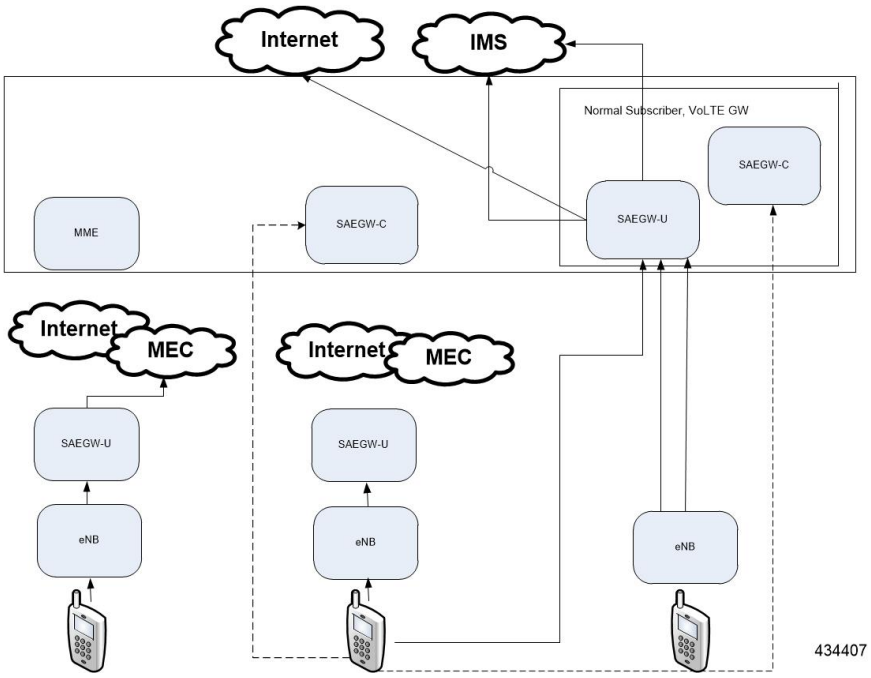
Mobile Edge Computing (MEC) Support is used to bring application with low latency requirements and capabilities to the carrier’s network in order to explore a wide range of new use cases and applications. This feature enables selection of proper Edge User Plane nodes for MEC user sessions.

How It Works

Architecture

This section describes the MEC architecture.

Figure 3: MEC Architecture



Flows

This section describes the call flow procedures related to MEC support.

Whenever the user moves to idle mode, each PDN's default bearer is checked to see if the GW-U IP address matches the TAI List. If a mismatch is found, paging is initiated.

When the user connects back again either by TAU or Service Request based on the new tracking area from where the TAU or Service Request is received, each PDN's default bearer is checked to see if the GW-U IP address matches the TAI List. If mismatch is found and if the PDN and UE Usage is marked Re-connect in APN Profile, the PDNs are deleted with Re-Activation cause code. TAI List will be taken from TAI Management DB or MEC TAI Group based on the configuration of TAI List and UP address".

Figure 4: Attach in TA-1, TAU from TA-2, IDLE Mode and SR in TA-2

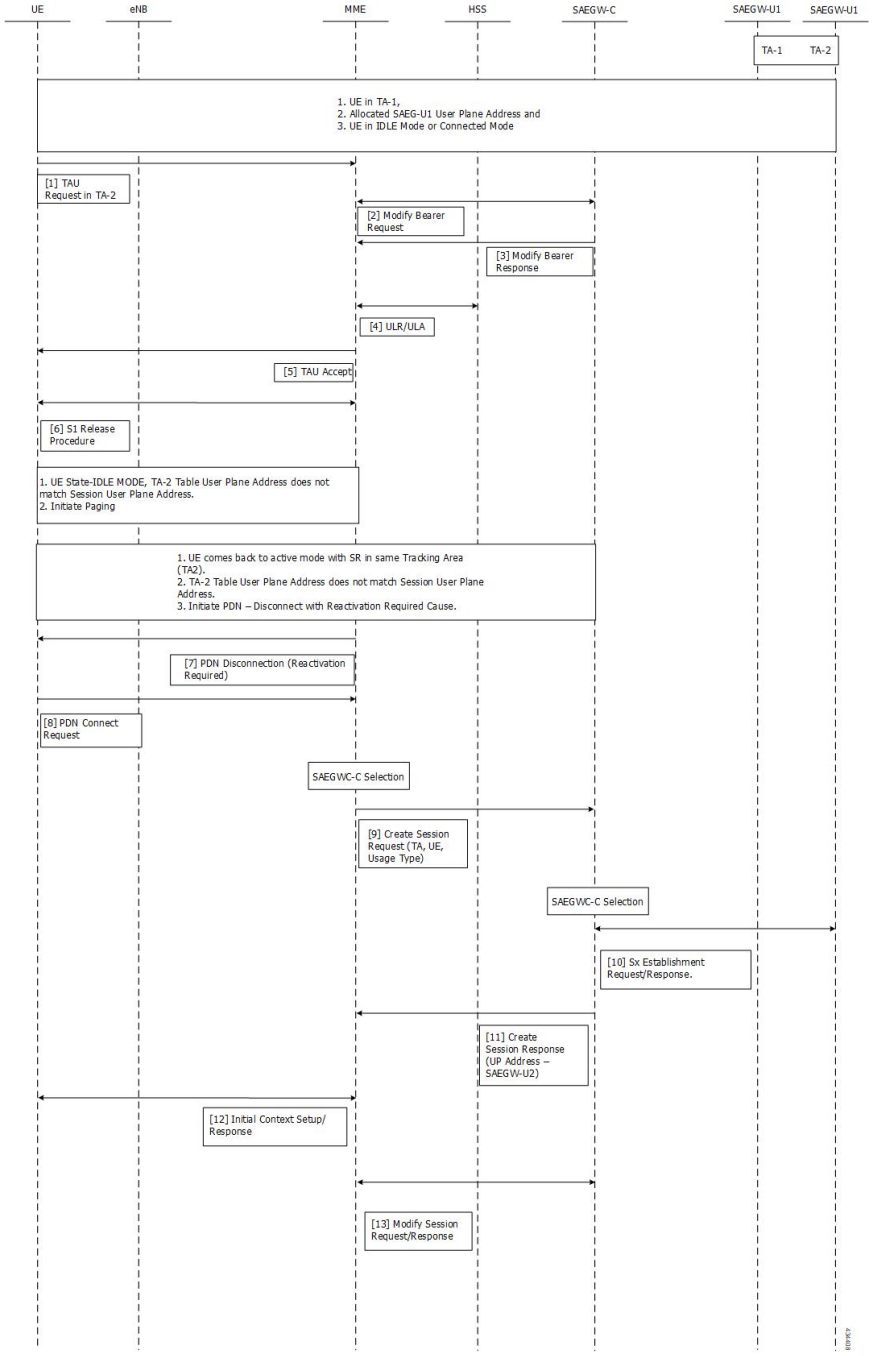
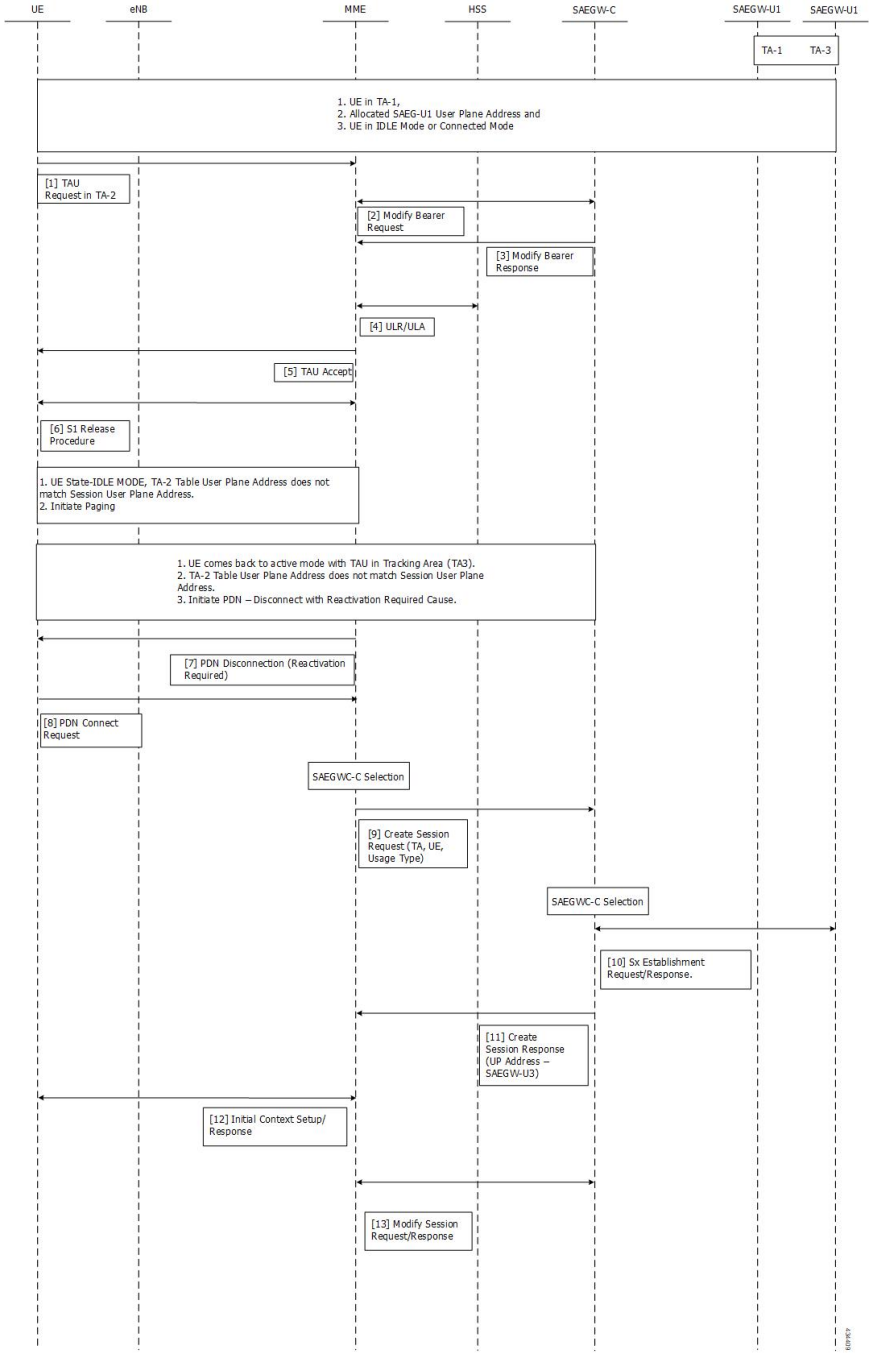


Figure 5: Attach in TA-1, TAU from TA-2, IDLE Mode and TAU in TA-3



Configuring MEC Support

This section provides information on the CLI commands to configure MEC Support in the MME.

Configureing up-address in TAI Management DB

Use the following configuration to configure the addresses of User Plane Nodes Serving all TAIs in this object.

```
configure
  lte-policy
    tai-mgmt-db tai_mgmt_db_name
      tai-mgmt-obj tai_mgmt_obj_name
        [ no ] up-address ( IP-ADDRESS | IP-ADDRESS/MASK }
        end
```

NOTES:

- **no**: Removes the addresses of User Plane Nodes Serving all TAIs in this object.
- **[no] up-address (IP-ADDRESS | IP-ADDRESS/MASK }** Configures the addresses of User Plane Nodes Serving all TAIs in this Object. **IP-ADDRESS** must be an IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:####. Also supports :: notation **IP-ADDRESS/MASK** must be an IPV4 ##.##.##.##/x or IPV6 ####:####:####:####:####:####:####:####/x.

Configuring up-address in MEC TAI Group

Use the following configuration to configure the up-address of User Plane Nodes Serving all TAIs in this object.

```
configure
  lte-policy
    mec-tai-grp mec_tai_grp_name
        [ no ] up-address ( IP-ADDRESS | IP-ADDRESS/MASK } mef-address
 iPV4/iPV6_address
        end
```

NOTES:

- **no**: Removes the addresses of User Plane Nodes Serving all TAIs in this object.
- **up-address (IP-ADDRESS | IP-ADDRESS/MASK }** Configures the addresses of User Plane Nodes Serving all TAIs in this Object. **IP-ADDRESS** must be an IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:####. Also supports :: notation **IP-ADDRESS/MASK** must be an IPV4 ##.##.##.##/x or IPV6 ####:####:####:####:####:####:####:####/x.
- **mef-address** *iPV4/iPV6_address*: Configures the peer MEF server address for MEF signalling.*iPV4/iPV6_address* must be IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:#### (IPV6 also supports :: notation).

Configuring tai in MEC TAI Group

Use the following configuration to configure the Tracking Area Identity.

```
configure
  lte-policy
    mec-tai-grp mec_tai_grp_name
      [ no ] tai mcc mcc_value mnc mnc_value { tac value1... value20  | tac-range
```

```
from tac_value_from to tac_value_to }
        [ no ] up-address ( IP-ADDRESS | IP-ADDRESS/MASK }
        end
```

NOTES:

- **no**: Removes the configuration of tai.
- **mec-tai-grp** *mec_tai_grp_name*: Configures MEC TAI Group.*mec_tai_grp_name* must be a string between 1 to 64. Maximum of 50 MEC TAI Groups can be configured.
- **tai**: Specifies the Tracking Area Identity.
- **mcc** *mcc_value*: Specifies the Mobile Country Code.*mcc_value* must be a three digit integer between 0 to 999.
- **mnc** *mnc_value*: Specifies the Mobile National Code.*mnc_value* must be a two / three digit integer between 00 to 999.
- **tac** *value1... value20*: Specifies the Tracking Area Code. Upto 20 Tracking Area Codes can be entered on one line. It can be configured by entering TAC directly or using range. *value1... value20* must be an integer between 0 to 65535.
- **tac-range from** *tac_value_from* **to** *tac_value_to* : Specifies the Range of Tracking Area Code. Maximum of 5 ranges in a MEC TAI group can be configured. *tac_value_from* and *tac_value_to* must be an integer between 0 to 65535.

Configuring up-service-area-change

Use the following configuration to configure action for User-Plane Service Area Change for MME.

```
configure
   context context_name
      apn-profile apn_profile_name
        up-service-area-change disconnect-pdn [ ue-usage-type ]
ue_usage_type_values
        end
```

NOTES:

- **up-service-area-change**: Configures action for User-Plane Service Area Change for MME.
- **disconnect-pdn**: Enables reselection of User Plane Node by PDN disconnection.
- **ue-usage-type** *ue_usage_type_values*: Configures UE usage type for disconnecting PDN for UP service area. *ue_usage_type_values* must be an integer 1 through 255.

Important Release 21.15 onwards, PGW-U IP address is used for User Plane address.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor this feature.

Show Commands and Outputs

show mme-service statistics

The output of this command includes the following fields:

Paging Initiation for SIGNALING PDN RECONN Events:

- Attempted
- Success
- Failures
  - Success at Last n eNB
  - Success at TAI List
  - Success at Last TAI

Bulk Statistics

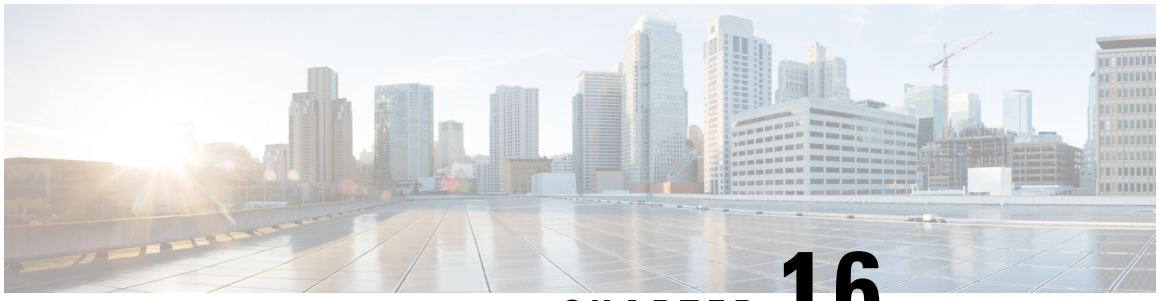
The following statistics are added in support of the MEC Location Management feature:

Table 3: MME Schema

Bulk Statistics	Description
signalling-pdn-reconn-paging-init-events-attempted	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were attempted.
signalling-pdn-reconn-paging-init-events-success	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were successful.
signalling-pdn-reconn-paging-init-events-failures	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that failed.
signalling-pdn-reconn-paging-last-enb-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known eNodeB.
signalling-pdn-reconn-paging-last-tai-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known Tracking Area Identifier.
signalling-pdn-reconn-paging-tai-list-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE.

Table 4: TAI Schema

Bulk Statistics	Description
tai-signalling-pdn-reconn-paging-init-events-attempted	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were attempted.
tai-signalling-pdn-reconn-paging-init-events-success	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were successful.
tai-signalling-pdn-reconn-paging-init-events-failures	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that failed.
tai-signalling-pdn-reconn-paging-last-enb-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known eNodeB.
tai-signalling-pdn-reconn-paging-last-tai-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known Tracking Area Identifier.
tai-signalling-pdn-reconn-paging-tai-list-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE.



CHAPTER 16

MME Handling of Purge Procedure

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
MME Handling of Purge Procedure support added.	21.12.15
First introduced.	21.15.1

Feature Changes

Previous Behavior: The MME sends Purge-UE-Request (PUR) to HSS during deletion of subscriber information in the old session manager initiated by IMSI manager.

New Behavior: MME can be configured to stop sending Purge-UE-Request (PUR) to HSS during the deletion of subscriber information in the old session manager initiated by the IMSI manager with the help of newly introduced CLI.

Command Changes

This section describes the CLI configuration required to configure MME handling of Purge procedure.

Configuring hss-purge-ue-request

Use the following configuration to configure HSS purge UE request.

```
configure
     context context_name
       mme-service mme_service_name
          [ default | no ] hss-purge-ue-request imsimgr-initiated
          end
```

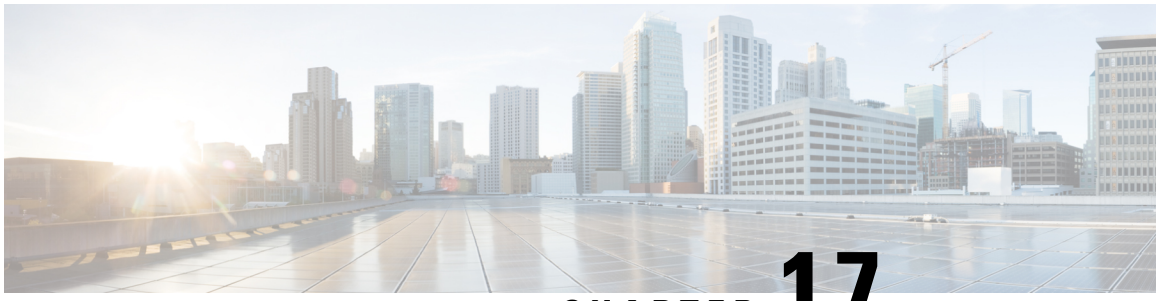
NOTES:

- **default**: MME sends Purge-UE-Request (PUR) to HSS during deletion of subscriber information in old session manager initiated by IMSI manager.
- **no**: Disables sending Purge-UE-Request (PUR) to HSS during deletion of subscriber information in old session manager initiated by IMSI manager.
- **hss-purge-ue-request**: Configure to enable/disable sending Purge-UE-Request (PUR) to HSS.
- **imsimgr-initiated**: Purge-UE-Request (PUR) to HSS during deletion of subscriber information in old session manager.

Performance Indicator Changes

show mme-service all

The output of this command includes "IMSIMGR HSS Purge UE Request" field to indicate IMSI manager HSS Purge UE request is enabled or not.



CHAPTER 17

Migrating 3G to 4G Context

Feature Summary and Revision History

Summary Data

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

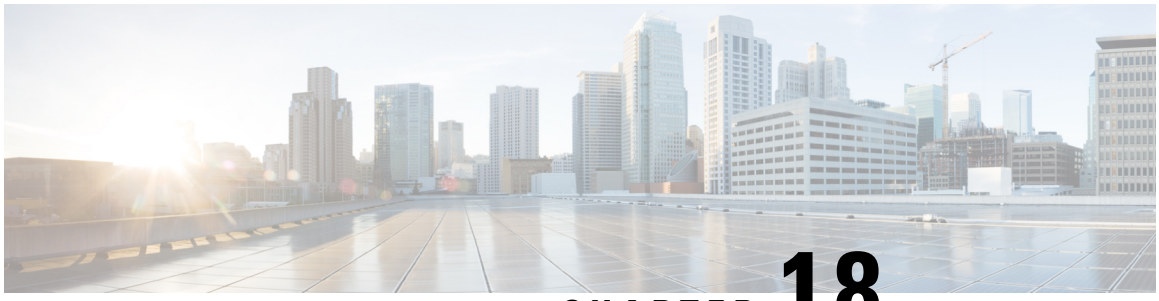
Revision History

Revision Details	Release
First Introduced	**21.15.51**

Feature Changes

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

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



CHAPTER 18

S-GW Address Based Combined SPGW Selection

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.15

Feature Description

The MME allows to configure the Gateway selection priority when priority is configured as S-GW. MME selects S-GW first, and P-GW will be selected based on the co-location string from the selected S-GW. For the additional PDN, P-GW is selected based on the colocation string from the selected S-GW. When this feature is not configured, by default P-GW is selected first.

Important This behavior is applicable only to the initial attach and PDN connectivity.

Configuring S-GW Address Based Combined SPGW Selection

Select S-GW as Priority

Use the following configuration to select S-GW priority.

```
configure
  apn-profile apn_profile_name
  [ remove ] gateway-selection priority sgw
  end
```

NOTES:

- **priority sgw**: Configures S-GW to be selected first.
- **remove**: Removes the configured priority S-GW.

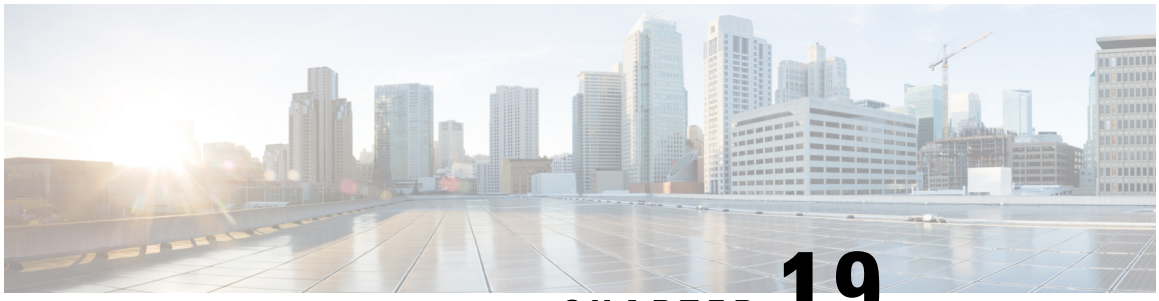
Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the S-GW Address Based Combined SPGW Selection feature.

Show Commands and Outputs

show apn-profile full all

The output of this command includes "Gateway Selection Priority" to inidcate gateway selection priority is configured or not.



CHAPTER 19

TCP Reset with Invalid Sequence Number should not Trigger Connection Close

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.	21.15.60

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.

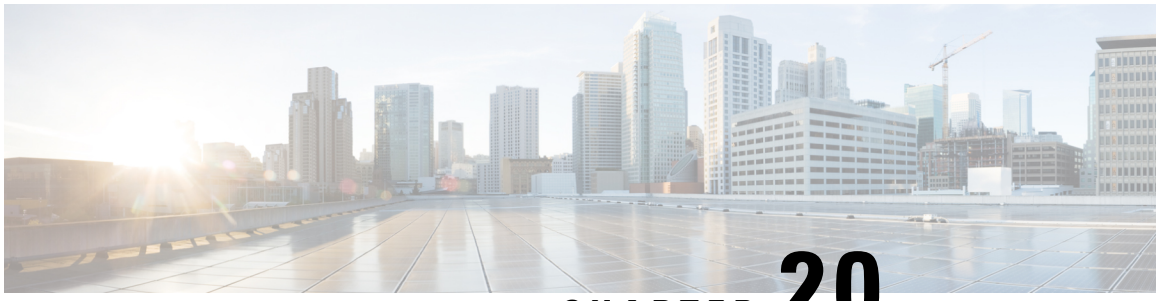
New Behavior: If a TCP RST Segment is received and the TCP FSM is in SYN-RCVD state, the TCP RST Segment is sequence number validated. Refer to RFC793 for more information.

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 20

TAI-based Routing for 20-bit and 28-bit eNB ID

This feature enables MME to perform TAI-based routing for both 20-bit and 28-bit eNB IDs.

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
HeNBGW Selection Enhancement in MME.	21.18
HeNBGW Selection Enhancement in MME.	21.15

Revision Details	Release
First introduced.	21.1

Feature Description

MME supports TAI-based routing of handover (HO) and configuration transfer messages towards Pico controller/HeNBGW when the target eNB ID is 28 bits, but it could not support TAI-based routing when the target Pico eNB ID is 20 bits.

Pico controller can transfer the target Pico eNB ID to 28 bits from 20 bits if the handover is Pico-to-Pico, but it could not handle Macro-to-Pico handover as there is no Pico Controller for Macro.

In releases 21.1 and beyond, the behavior of MME is modified so that it can perform TAI-based routing even if target home-eNB ID is 20 bits.

This feature provides a configurable option within MME service to configure target HeNB type (home or macro or both) behind HeNBGW. Based on this configuration, MME allows TAI-based lookup of target eNB, if target eNB ID is not found by MME during handover. By default, TAI-based lookup is performed only for home eNB ID (28-bits).

This feature is also introduced to support identification of target eNB using target TAI for target eNB type Macro or Pico nodes or both so that handover to such eNB can be supported if it is connected to MME through Pico controller/HeNBGW. From MME point of view, Pico controller is a Macro eNB which is using 20 bit eNB ID to support multi-cell.

Along with S1 based intra-MME HO, this feature can be applied to inter MME S1 HO procedures (inbound S10, S3 and Gn handovers). Please note that, in Gn case, MME converts target RNC ID to macro eNB ID so target TAI-based lookup for macro eNB works fine.

This feature allows operators to configure the global eNodeB IDs of HeNBGWs in the MME service. The MME uses this information to perform HeNBGW related functions. In case of S1-based handovers to home eNodeBs served by a HeNBGW, the lookup at MME for the target eNodeB based on global eNB ID will fail, as MME is aware of only the HeNBGW. In those cases, additional lookup needs to be done based on TAI to find the HeNBGW serving the home eNodeB.

Since TAI-based lookup for home or macro eNBs is supported for HeNBGWs, all such HeNBGWs should be defined in HeNBGW management database (HeNBGW-mgmt-db). The HeNBGW-mgmt-db should be associated within mme-service.

In this release, the number of HeNBGW entries in the HeNBGW-mgmt-db has been increased from 8 to 512.

HeNBGW Selection Enhancement

TAI is unique and it is not shared across multiple HeNBGWs. If the TAIs are shared, then any one of the target eNBs sharing the TAC under consideration will be selected during TAI-based target eNB selection and handed over to the eNB may fail. To overcome this failure, HeNBGW matched with MSB 10 bits of Target HeNB ID (macro-enb 20 bit or home-enb 28 bits) and eNB ID of HeNBGW must be selected. If no match is found, then any one of the target eNBs sharing the TAC under consideration is selected during the TAI-based target eNB selection and handover to the eNB may ultimately fail.

Note If there are several HeNBGW with same TAI, CISCO MME supports selection of HeNBGW with MSB 10 bits (macro-enb 20 bit or home-enb 28 bits)) of HeNB ID.

Limitations

The following are the limitations of this feature:

- TAI-based lookup is performed only for home eNB.
- TAI should be unique and should not be shared across multiple HeNBGWs. If the TAIs are shared, then any one of the target eNBs sharing the TAC under consideration will be chosen during TAI-based target eNB selection and handover to the eNB might fail.

Configuring TAI-based Lookup of eNB

The following section provides the configuration commands to enable the TAI-based lookup of eNB.

Configuring Target eNB Type for TAI-based Lookup

Use the following configuration commands to configure the target eNB type or target henb-type as home or macro.

```
configure
   context context_name
      mme-service service_name
         henbgw henb-type { macro-enb | home-enb | all }
         end
```

Notes:

- The **henbgw henb-type { macro-enb | home-enb | all }** is a new CLI command introduced in 21.1 release to support TAI-based lookup functionality.
- **henbgw**: Configures Home eNodeB gateway options.
- **henbgw-type**: Configures HeNB type. TAI-based lookup depends on HeNB type.
  - **home-enb**: Configures HeNB type home-enb (28-bits)
  - **macro-enb**: Configures HeNB type macro-enb (20-bits)
  - **all**: Configures HeNB type both macro-enb (20-bits) and home-enb (28-bits)
- By default, when the **henbgw henb-type** command is not applied explicitly, target eNB type is set as home-enb.
- Use the **no henbgw henb-type** command to delete the existing configuration, if previously configured.

- The target eNB type configuration is effective only when the **henbgw henb-type** CLI command is configured within mme-service and the HeNBGW-mgmt-db is associated with HeNBGWs inside mme-service.

Verifying the Target eNB Type Configuration

Use the following commands to verify the configuration status of this feature.

```
show mme-service all
```

- or -

```
show mme-service name service_name
```

service_name must be the name of the MME service specified during the configuration.

This command displays all the configurations that are enabled within the specified MME service.

The following is a sample configuration of this feature.

```
configure
   lte policy
      mme henbgw mgmt-db db_name
         henbgw-global-enbid mcc 123 mnc 456 enbid 12345
         henbgw-global-enbid mcc 123 mnc 456 enbid 12543
         end
configure
   context context_name
      mme-service service_name
         henbgw henb-type macro-enb
         associate henbgw-mgmt-db henbdb
         end
```

NOTES:

- By default, when the **henbgw henb-type** command is not configured, target eNB type is set as **home-enb**.

Configuring HeNBGW msb-10-bits Selection

Use the following commands to configure HeNBGW selection using HeNB MSB 10 bits for the same TAI.

```
configure
   context context_name
     mme-service service_name
        henbgw selection msb-10-bits
        no henbgw selection
        end
```

NOTES:

- **no** : Removes the configured HeNBGW selection for the same TAI.
- **henbgw**: Configures HeNBGW options.
- **selection**: Configures HeNBGW selection for same TAI.

- **msb-10-bits** Configures HeNBGW selection using HeNB MSB 10 bits for same TAI. By default this is disabled.

Note HeNBGW selection using HeNB MSB 10 bits is performed only when TAIs are shared across multiple HeNBGWs.

The TAI lookup happens only in the following instance:

- When henb-type {all | macro-enb} for handover to target Henbgw macro 20 bits.
- When henb-type **{all | home-enb}** is configured for handover to target HeNBGW home 28 bits. However, when henb-type {macro} is configured for handover to target HeNBGW home 28 bits, the lookup at MME for the target eNodeB will fail in handover preparation.

Monitoring and Troubleshooting the TAI-based Lookup

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show mme-service all** CLI command. If not enabled, configure the **henbgw henb-type** CLI command in MME service Configuration mode and check if it works.
- Collect and analyze the output of **show configuration**, **show support details**, **show mme-service name** *service_name* and **show mme-service statistics handover** commands. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.
- Check and analyze the debug logs for mme-app, s1ap, mmemgr, and mmedemux facilities to determine if TAI-based lookup fails for a particular TAI.

show mme-service all

The following field is added to the output of the **show mme-service all** command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

Table 5: show mme-service all Command Output Descriptions

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

Field	Description
HeNBGW selection using HeNodeB MSB 10 bits for same TAI	• Enabled • Disabled

show mme-service name *service_name*

The following field is added to the output of the **show mme-service name** *service_name* command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

Table 6: show mme-service name service_name Command Output Descriptions

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

show mme-service statistics handover

The following fields are added to the output of the **show mme-service statistics handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
  EUTRAN<-> EUTRAN using S10 Interface:
    .
    .
    Inbound relocation using Target TAI based S1 HO procedure:
      Attempted:       0
      Success:         0
      Failures:        0
```

*Table 7: **show mme-service statistics** Command Output Descriptions*

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

show mme-service statistics peer-id

The following fields are added to the output of the **show mme-service statistics peer-id** *peer_id* **handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
  EUTRAN<-> EUTRAN using S10 Interface:
    .
    .
    Inbound relocation using Target TAI based S1 HO procedure:
      Attempted:       0
      Success:         0
      Failures:        0
```

*Table 8: **show mme-service statistics** Command Output Descriptions*

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

Bulk Statistics

MME Schema

The following bulk statistics have been added to the MME schema to track the TAI-based lookup attempts, successes and failures during intra-MME S1 and inter-MME inbound S10 handovers:

- emmevent-s1ho-target-tai-attempt
- emmevent-s1ho-target-tai-success
- emmevent-s1ho-target-tai-failure
- in-s1-ho-4gto4g-s10-target-tai-attempted
- in-s1-ho-4gto4g-s10-target-tai-success
- in-s1-ho-4gto4g-s10-target-tai-failures

For detailed information on these bulk statistics, refer to the **BulkstatStatistics_documentation.xls** spreadsheet that is included as part of the software companion package for this release.