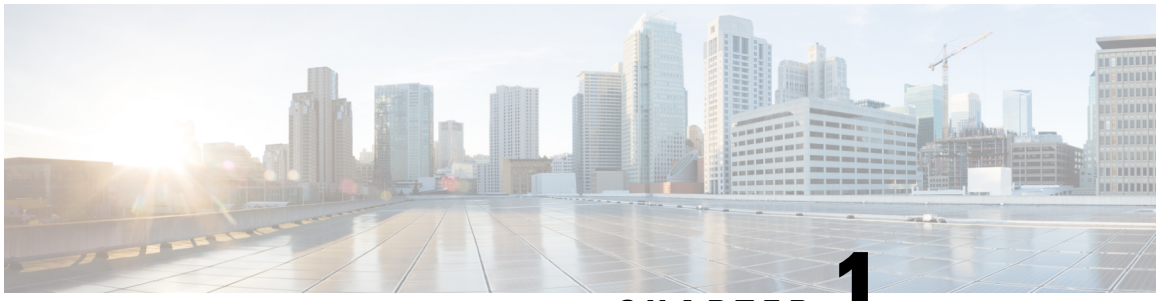
Release Change Reference, StarOS Release 21.17/Ultra Services Platform Release 6.11

First Published: 2019-12-20

Last Modified: 2021-02-05

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



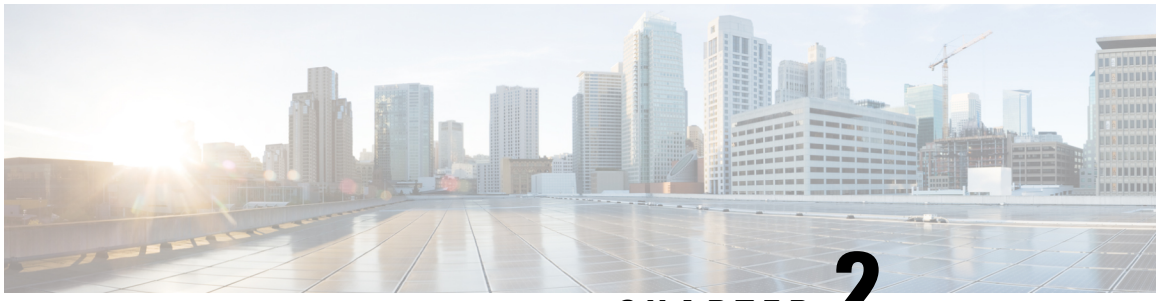
CHAPTER 1

Release 21.17/6.11 Features and Changes Quick Reference

Release 21.17/6.11 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5G NSA for MME, on page 9	MME	21.17
Co-Located SPGW Selection for Emergency Bearer, on page 37	SGSN	21.17
Configuring UE Radio Capability IE Size, on page 39	MME	21.17.6
Deprecation of Manual Scaling, on page 45	UAS	6.0
Diameter Pending Transaction, on page 47	SAEGW	21.17
Extraction of IPv4 Addresses Embedded in IPv6 Addresses, on page 49	ECS	21.17.16
GTPV1/V2 Echo Support for Peer MME and SGSN, on page 53	All	21.17
MME MDT Management Support, on page 59	MME	21.17
Maximum MTU Size Changes for Diameter Data Packets Fragmentation, on page 65	P-GW	21.17.17
NAS Notification for SRVCC Cancellation due to TAU Request, on page 67	MME	21.17.6
Origin-State-Id AVP Support on P-GW , on page 69	SGSN	21.17

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
RTLLI Management for 2G M2M Devices, on page 73	SGSN	21.17.9
SGSN Controlling Peer Status Based on Heartbeat Message, on page 77	SGSN	21.17
Support for DH group 5 Encryption under IKE and IPSEC Transform Set, on page 79	ePDG	21.17.12
UEM Interworking with Generic VNFM, on page 81	UEM	6.11



CHAPTER 2

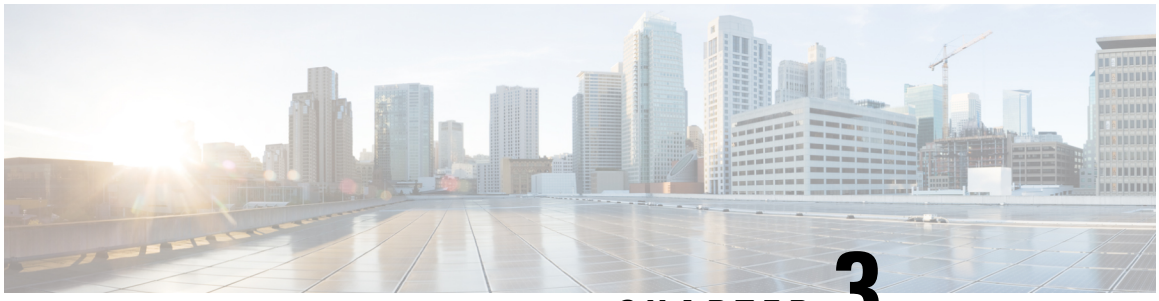
Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
5G NSA for MME	Disabled - Configuration Required
Co-Located SPGW Selection for Emergency Bearer	Disabled - Configuration Required
Configuration of UE Radio Capability IE Size	Enabled - Configuration Required
Controlling SGSN Receive Heartbeat from Peer	Disabled - Configuration Required
Deprecation of Manual Scaling	Disabled - Configuration Required
Diameter Pending Transaction	Enabled - Always-on
Extraction of IPv4 addresses Embedded in IPv6 Addresses	Disabled - License Required
GTPV1/V2 Echo Support for PeerMME and SGSN	Disabled - Configuration Required
MME Minimization Drive Test	Disabled - Configuration Required
MME Support for EN-DC SON Configuration Transfer IE on S1-AP	Enabled - Configuration Required
Maximum MTU Size Changes for Diameter Data Packets Fragmentation	Enabled- Always On
NAS Notification for SRVCC Cancellation due to TAU Request	Enabled- Always On
Origin-State-Id AVP Support on P-GW	Disabled - Configuration Required
RTLLI Management for 2G M2M Devices	Disabled - Configuration Required
SGSN Controlling Peer Status Based on Heartbeat Message	Disabled - Configuration Required

Feature	Default
Support for DH group 5 Encryption under IKE and IPSEC Transform Set	Disabled – Configuration Required
UEM Interworking with Generic VNFM	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 21.17 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 21.17 include:

New 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.

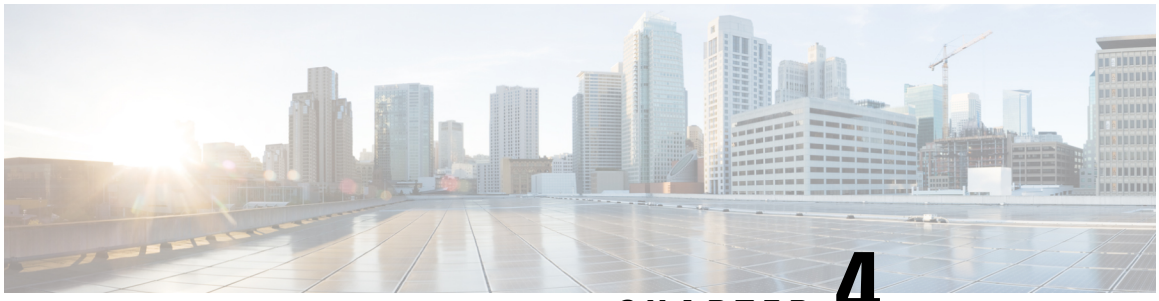
Bulk Statistics	Description
tai-emmcall-attach-currcall	Shows the total number of EPS Mobility Management call-line statistics on attached current calls for each TAI.
tai-emmcall-connect-currcall	Shows the total number of EPS Mobility Management call-line statistics on connected calls for each TAI.
tai-emmcall-idle-curcall	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.
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.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.17 and USP 6.11

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.17 and Ultra Services Platform (USP) 6.11 software releases.

SNMP MIB Object Changes for 21.17

This section provides information on SNMP MIB alarm changes in release 21.17.

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 21.17.

None in this release.

Modified SNMP MIB Object

None in this release.

Deprecated SNMP MIB Object

None in this release.

SNMP MIB Alarm Changes for 21.17

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

SNMP MIB Conformance Changes for 21.17

This section provides information on SNMP MIB alarm changes in release 21.17.

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 6.11

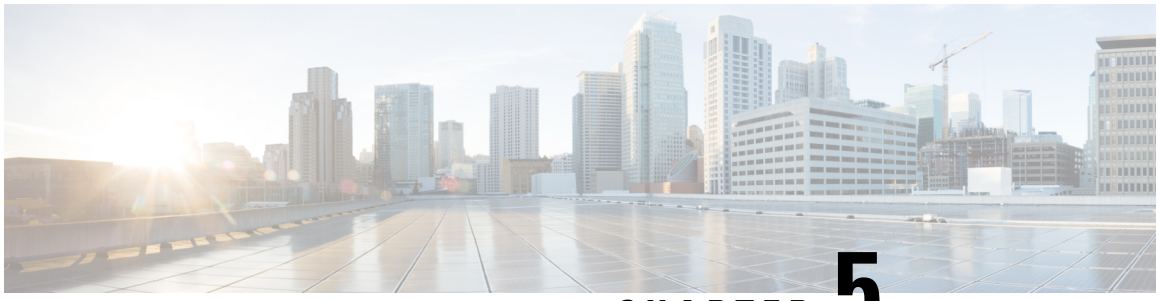
There are no new, modified, or deprecated SNMP MIB object changes in this release.

SNMP MIB Alarm Changes for 6.11

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

SNMP MIB Conformance Changes for 6.11

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



CHAPTER 5

5G NSA for MME

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	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release

The 5G NSA support for Secondary RAT Usage Reporting feature is qualified on the ASR 5500 platform.	21.17
The 5G NSA supports Secondary RAT Usage Reporting. **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.	21.16
The 5G NSA solution for MME supports the following functionality in this release: • Ultra-Low Latency QCI bearers handover from MME to Gn-SGSN • NR security algorithms for DCNR capable UEs to support 5G security	21.10
The 5G NSA solution for MME supports the following functionality in this release: • DCNR capability exchange with peer SGSN in MM context over S3 interface • MME support of statistics for DCNR PDNs • NR security algorithms for DCNR capable UEs to support 5G security **Important** Support for 5G security is not fully qualified in this release.	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
First introduced.	21.8

Feature Description

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

Overview

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

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

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

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

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

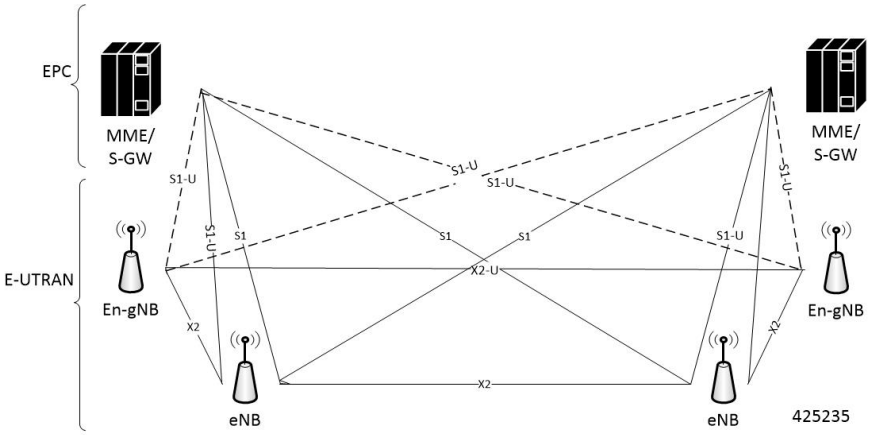
  Network Slicing, CUPS, Virtualization, Multi-Gbps support, Ultra low latency, and other such aspects will be natively built into the 5G SA Packet Core architecture.

Dual Connectivity

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

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

Figure 1: EN-DC Architecture



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

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

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

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

of the Attach Accept/Tracking Area Update Accept message. Accordingly, UE provides the indication that dual connectivity with NR is restricted to the upper layers.

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

The 5G NSA solution for MME supports the following functionalities:

- **E-RAB Modification Procedure:**

  When SCG (Secondary Cell Group) bearer option is applied to support DCNR, this procedure allows the Master eNodeB to switch a bearer to Secondary eNodeB without changing the S1-MME association.

- **NR Capable S-GW/P-GW Selection:**

  When DCNR capable UE attempts to register in MME and when all DCNR validations are successful (for example DCNR feature configuration on MME, HSS not sending access-restriction for NR, and so on), for dynamic S-GW and P-GW selection, MME uses the following service parameters received from DNS server (in NAPTR response) over other service parameters to select NR capable S-GW/P-GW.

  - x-3gpp-sgw:x-s5-gtp+nc-nr
  - x-3gpp-pgw:x-s5-gtp+nc-nr

  When the dynamic selection of S-GW/P-GW fails for any other reasons, MME falls back and selects the locally configured S-GW/P-GW.

- **Dynamic S-GW/P-GW Selection:**

  Dynamic S-GW and P-GW selection by MME for DCNR capable UE is supported. When a DCNR capable UE attempts to register in MME and when all DCNR validations are successful (DCNR feature configuration on MME, HSS not sending access-restriction for NR, and so on), the MME sets the "UP Function Selection Indication Flags" IE with DCNR flag set to 1 in "Create Session Request" message. This feature supports the CUPS architecture for SGW-C and PGW-C to select SGW-U and PGW-U and support dual connectivity with NR. When S-GW receives this IE over S11, it sends the IE over S5 to P-GW. If S-GW receives the IE in a non-CUPS deployment, it is ignored.

- **URLCC QCI Support:**

  For Ultra-Reliable and Low Latency Communications (URLCC), MME supports — QCI 80 (Non-GBR resource type), QCI 82 (GBR resource type), and QCI 83 (GBR resource type). MME establishes the default bearers with URLLC QCI 80, which is typically used by low latency eMBB applications. MME establishes the dedicated bearers with URLLC QCI 82 and QCI 83 (also with QCI 80 if dedicated bearers of non-GBR type to be established), which is typically used by discrete automation services (industrial automation).

- **PDNs with UP Function Selection Indication:**

  Based on the DCNR flag in the UP Function Selection Indication Flags IE, new statistics and bulk statistics are supported for the total number of current active, setup, and released DCNR PDNs on MME.

- **NR Support in GTP MM Context over S3 Interface:**

  MME supports the DCNR capability exchange with peer SGSN over the S3 interface. The DCNR restriction can be notified by the peer SGSN during handover to MME. The DCNR restriction information helps the target MME in performing the right S-GW selection.

During handovers, the target MME performs gateway selection before getting the subscription information from the HSS and hence MME may select the NR capable S-GW for DCNR restricted UE. To prevent this, the peer SGSN will notify the Restriction information (NRSRNA) through the GTP MM context in Identification-Response/Context-Response/Forward-Relocation-Request message to MME. The S3-DCNR support includes both GTPv2 and GTPv1 protocol for S4-SGSN and Gn-SGSN respectively.

- **5G Security:**

  The "UE Additional Security Capability" and "Replayed UE Additional Security Capability" IEs for MME are supported as per 3GPP TS 24.301.

  The MME supports handling of the "UE Additional Security Capability" IE for DCNR capable UEs. This information element is used by the UE in Attach Request and Tracking Area Update messages to indicate which additional security algorithms are supported by the UE.

  The MME includes the "Replayed UE Additional Security Capability" IE if the MME supports handling of UE additional security capabilities, if the MME is initiating a Security Mode Command during an Attach or Tracking Area Update procedure and the Attach Request or Tracking Area Update Request message included a "UE Additional Security Capability" IE.

  The "NR UE Security Capability" IE will be included by MME in the S1AP messages — INITIAL CONTEXT SETUP REQUEST, UE CONTEXT MODIFICATION REQUEST, HANDOVER REQUEST, PATH SWITCH ACKNOWLEDGE and DOWNLINK NAS TRANSPORT for MME as per 3GPP TS36.41.

  The eNode-B includes the "NR UE Security Capability" IE in PATH SWITCH REQUEST to be processed by the MME.

- **High Throughput:**

  5G NR offers downlink data throughput up to 20 Gbps and uplink data throughput up to 10 Gbps. Some interfaces in EPC have the support to handle (encode/decode) 5G throughput ranges. For example, NAS supports up to 65.2 Gbps (APN-AMBR) and S5/S8/S10/S3 (GTP-v2 interfaces) support up to 4.2 Tbps. The diameter interfaces such as S6a and Gx support only up to 4.2Gbps throughput, S1-AP supports only up to 10 Gbps and NAS supports up to 10 Gbps (MBR, GBR). New AVP/IE are introduced in S6a, Gx , S1-AP and NAS interfaces to support 5G throughput rates. See the *How It Works* section for more information.

- **Extended QoS:**

  MME supports the extended QoS values towards S-GW in legacy IEs - APN-AMBR, Bearer QoS, and Flow QoS.

- **Supported IEs:**

  S1-AP interface:

  - Extended UE-AMBR Downlink
  - Extended UE-AMBR Uplink
  - Extended E-RAB Maximum Bit Rate Downlink
  - Extended E-RAB Maximum Bit Rate Uplink
  - Extended E-RAB Guaranteed Maximum Bit Rate Downlink
  - Extended E-RAB Guaranteed Maximum Bit Rate Uplink

NAS interface:

- Extended EPS quality of service
- Extended APN aggregate maximum bit rate

- **ULL QCI bearers handover from MME to Gn-SGSN Support:**

  For Ultra-Low Latency (ULL) MME is configured to map the Ultra-Low Latency values 80, 82, and 83 to Pre-Release8 QoS during handover from MME. Maximum Bit Rate (MBR) and Guaranteed Bit Rate (GBR) limits are increased to 4Tbps. MME supports outbound handover on GnGp interface to Gn-SGSN with ULL-QCI values 80, 82, and 83.

- **UE additional Security Capability:**

  MME includes “UE additional security capability” IE in MM-Context over S10 interface during handover if it is available, otherwise includes the length of UE additional security capability as zero.

  MME processes “UE additional security capability” for NR received in MM-Context over S10 interface during Handover only if it is not available. If the received length of UE additional security capability is zero, then it is not present in MM-context.

Secondary RAT Usage Reporting

When a Secondary RAT is used in conjunction with E-UTRAN, operator may wish to record the data volume sent on the Secondary RAT. The PLMN locally activates the Secondary RAT Usage Data Reporting by E-UTRAN O & M. The E-UTRAN reports uplink and downlink data volumes to the EPC for the Secondary RAT on a per EPS bearer basis and per time interval. If E-UTRAN is also configured to make periodic reports, if there is no event to trigger a report before the period expires. MME handle these reports received from eNodeB in S1-AP messages and forwards it to S-GW / P-GW via GTPV2 messages.

Important MME behavior in Routing Area Update Procedure involving “MME and S3 SGSN”, will be similar to Routing Area Update Procedure involving “MME and Gn/Gp SGSN” where secondary RAT report will be sent over Change Notification to P-GW if reporting to P-GW is enabled. And report will be sent over Delete Session Request to S-GW if MME had received the Serving GW change indication.

How It Works

Architecture

This section describes the external interfaces required to support the 5G NSA architecture.

S6a (HSS) Interface

The S6a interface supports new AVPs "Extended-Max-Requested-BW-UL" and "Extended-Max-Requested-BW-DL" in grouped AVP "AMBR" to handle the 5G throughput ranges. When the maximum bandwidth value for UL (or DL) traffic is higher than 4294967295 bits per second, the "Max-Requested-Bandwidth-UL" AVP (or DL) must be set to the upper limit 4294967295 and the

"Extended-Max-Requested-BW-UL" AVP (or DL) must be set to the requested bandwidth value in kilobits per second.

S1AP (eNodeB) Interface

Extended UE-AMBR

The S1AP interface supports new IEs "Extended UE Aggregate Maximum Bit Rate Downlink" and "Extended UE Aggregate Maximum Bit Rate Uplink" in the grouped IE "UE Aggregate Maximum Bit Rate", where the units are bits/second. If the Extended UE Aggregate Maximum Bit Rate Downlink/Uplink IE is included, then the UE Aggregate Maximum Bit Rate Downlink/Uplink IE must be ignored.

Extended E-RAB MBR/GBR

The S1AP interface supports new AVPs "Extended E-RAB Maximum Bit Rate Downlink/Uplink" and "Extended E-RAB Guaranteed Bit Rate Downlink/Uplink" in the "GBR QoS Information" grouped IE, where the units are bits/second.

NAS (UE) Interface

Extended APN Aggregate Maximum Bit Rate

The new IE "Extended APN aggregate maximum bit rate" is added in all applicable NAS messages to convey the 5G throughput (beyond 65.2Gbps) over NAS. The existing IE in NAS "APN-AMBR" supports APN-AMBR values up to 65.2Gbps.

Extended EPS Quality of Service

The new IE "Extended EPS Quality of Service" is added in all applicable NAS messages to convey the 5G throughput (beyond 10Gbps) over NAS. The existing IE in NAS "EPS Quality of Service" supports MBR and GBR values up to 10Gbps.

Limitations

This section describes the known limitations for the 5G NSA feature:

- DCNR for S3 interface is supported only for inbound handover of UE from 2G/3G to 4G.
- MME does not support the NR capable gateway selection during connected mode inbound handover from Gn-SGSN.
- Maximum of 11 reports can be sent in single GTPV2 message towards S-GW.
- Reports sent without handover flag during handover procedure will be dropped by MME.
- Reports are not stored as part of session recovery.
- At any point of time only two reports per bearer will be handled by MME.
- Filling of “Secondary RAT Data Usage Request” IE in E-RAB MODIFY REQUEST message and handling of report in ERAB Modify RESPONSE is not supported.
- During 4g to 3g/2g IRAT handover without S-GW change, if PGW reporting is enabled, reports will be sent over the Change Notification message. Reports will not be sent to S-GW, even if the S-GW reporting is configured.

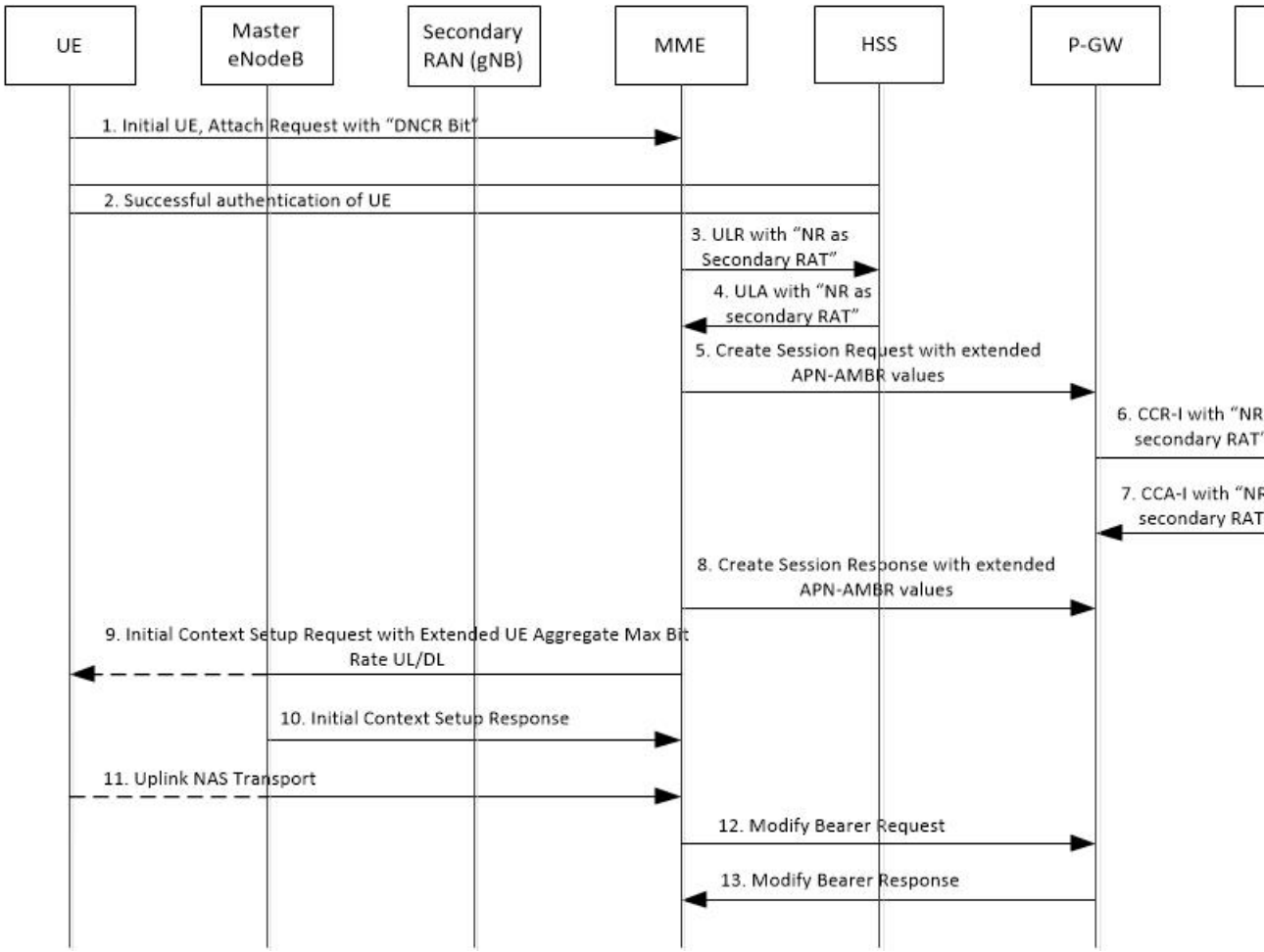
Flows

This section describes the call flow procedures related to MME for 5G NSA.

Initial Registration Procedure

The following call flow illustrates the Initial Registration procedure for DCNR capable UE.

Initial Registration of DCNR Capable UE



Step	Description
1	The DCNR capable UE sets the "DCNR bit" in NAS message "Attach Request" in "UE Network Capability" IE. DCNR must be enabled at MME service or call control profile depending upon the operator requirement.
2	MME successfully authenticates the UE.

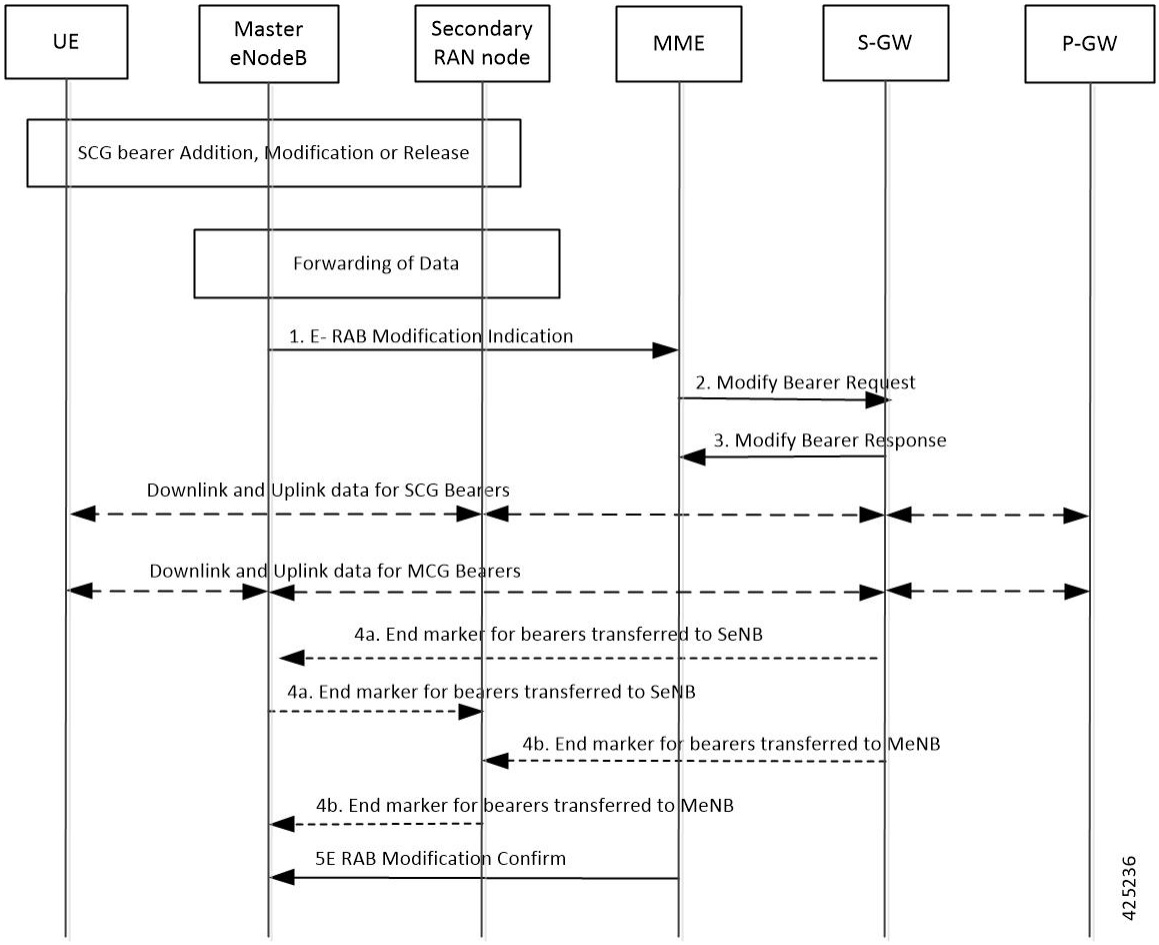
Step	Description
3	As part of the authorization process, while sending ULR to HSS, MME advertises the DCNR support by sending the "NR as Secondary RAT" feature bit in "Feature-List-ID-2".
4	HSS sends ULA by advertising the DCNR by sending "NR as Secondary RAT" feature bit in "Feature-List-ID-2", "Max-Requested-Bandwidth-UL" as 4294967295 bps, "Max-Requested-Bandwidth-DL" as 4294967295 bps, and the extended bandwidth values in AVPs "Extended-Max-Requested-BW-UL" and "Extended-Max-Requested-BW-DL". If HSS determines that the UE is not authorized for DCNR services, then HSS sends Subscription-Data with "Access-Restriction" carrying "NR as Secondary RAT Not Allowed".
5	MME sends the Create Session Request message with the extended APN-AMBR values in existing AMBR IE. As the APN-AMBR values in GTPv2 interface are encoded in kbps, the existing AMBR IE handles the 5G NSA bit rates.
6	P-GW sends CCR-I to PCRF advertising the DCNR by sending "Extended-BW-NR" feature bit in "Feature-List-ID-2", "APN-Aggregate-Max-Bitrate-UL" as 4294967295 bps, "APN-Aggregate-Max-Bitrate-DL" as 4294967295 bps, and the extended bandwidth values in AVPs "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL".
7	PCRF sends CCA-I advertising the DCNR by sending "Extended-BW-NR" feature bit in "Feature-List-ID-2", "APN-Aggregate-Max-Bitrate-UL" as 4294967295 bps, "APN-Aggregate-Max-Bitrate-DL" as 4294967295 bps, and the extended bandwidth values in AVPs "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL". PCRF can offer the same extended APN-AMBR values that are requested by PCRF or modify the extended APN-AMBR values. P-GW enforces the APN-AMBR values accordingly.
8	P-GW honors the APN-AMBR values as offered by PCRF and sends the extended APN-AMBR values in existing APN-AMBR IE in the Create Session Response message.

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

E-RAB Modification Procedure

When Secondary Cell Group (SCG) bearer option is applied to support DCNR, the E-RAB Modification procedure is used to transfer bearer contexts to and from secondary eNodeB or secondary gNodeB.

Figure 2: E-RAB Modification Procedure by Master eNodeB



Step	Description
1	The master eNodeB (MeNB) sends an E-RAB Modification Indication message (eNodeB address(es) and TEIDs for downlink user plane for all the EPS bearers) to the MME. The MeNB indicates if each bearer is modified or not. The "E-RAB to be Modified List" IE contains both "E-RAB to Be Modified Item" and "E-RAB not to Be Modified Item" IEs. For the bearer that need to be switched to secondary eNodeB/gNodeB (SeNB), the "E-RAB to Be Modified Item" IE contains the transport layer address of gNodeB and TEID of gNodeB.
2	The MME sends a Modify Bearer Request message (eNodeB address(es) and TEIDs for downlink user plane for all the EPS bearers) per PDN connection to the S-GW, only for the affected PDN connections.
3	The S-GW returns a Modify Bearer Response message (S-GW address and TEID for uplink traffic) to the MME as a response to the Modify Bearer Request message.
4	For the bearers transferred to SeNB, S-GW sends one or more end marker packets on the old path (to MeNB) immediately after switching the path.

Step	Description
5	The MME confirms E-RAB modification with the E-RAB Modification Confirm message. The MME indicates if each bearer was successfully modified, retained, unmodified or already released by the EPC.

Standards Compliance

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

- 3GPP 23.003 Release 15.2.0 - Numbering, addressing and identification.
- 3GPP 23.401 Release 15.2.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 29.272 Release 15.2.0 - Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP 29.274 Release 15.2.0 - 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP 29.303 Release 15.2.0 - Domain Name System Procedures

Cisco's implementation of the Secondary RAT Usage Reporting complies with the following standards:

- 3GPP 29.274: 15.5.0 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) Stage 3
- 3GPP 36.413: 15.3.0 Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)
- 3GPP 23.401: 15.5.0 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

Configuring 5G NSA for MME

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

Configuring 5G NSA on MME involves:

- Enabling DCNR in MME Service, on page 20
- Enabling DCNR in Call Control Profile, on page 21
- Configuring APN AMBR Values, on page 21
- Configuring Dedicated Bearer MBR Values, on page 24
- Configuring UE AMBR Values , on page 25

Enabling DCNR in MME Service

Use the following configuration to enable DCNR to support 5G NSA.

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

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service, name must be an string from 1 to 63 characters.
- **no**: Disables the DCNR configuration.
- The **dcnr** CLI command is disabled by default.

Enabling DCNR in Call Control Profile

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

```
configure
  call-control-profile profile_name
    [ no | remove ] dcnr
    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, it must be an string from 1 to 64 characters.
- **no**: Disables the DCNR configuration in the call control profile.
- **remove**: Removes the DCNR configuration from the call control profile.
- The **dcnr** CLI command is disabled by default.

Configuring APN AMBR Values

Use the following configuration to configure the APN aggregate maximum bit rate (AMBR) that will be stored in the Home Subscriber Server (HSS).

```
configure
  apn-profile profile_name
    qos apn-ambr max-ul mbr_up max-dl mbr_down
    remove qos apn-ambr
    end
```

NOTES:

- **apn-profile** *profile_name*: Creates an instance of an access point name (APN) profile. *profile_name* specifies the name of the APN profile as an alphanumeric string of 1 to 64 characters.
- **qos**: Configures the quality of service (QoS) parameters to be applied.
- **apn-ambr**: Configures the aggregate maximum bit rate (AMBR) for the APN.

- **max-ul** *mbr_up*: Defines the maximum bit rates for uplink traffic. *mbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).
- **max-dl** *mbr_down*: Defines the maximum bit rates for downlink traffic. *mbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).
- **remove**: Removes the APN AMBR changes from the configuration for this APN profile.

Enabling Secondary RAT Data Usage Report in Call Control Profile

Use the following configuration to enable Secondary RAT Data Usage Report to support 5G NSA.

```
configure
     call-control-profile profile_name
        secondary-rat data-usage-report { pgw [ sgw ] | sgw [ pgw ] }
        [ no | remove ] secondary-rat data-usage-report
        end
```

Important Both CLI configuration and the current running procedure are taken into account while filling the flags IRSGW/IRPGW in GTPv2 messages towards S-GW/P-GW.

NOTES:

- **no**: Disables the Secondary RAT Usage Report at call-control-profile.
- **remove**: Removes the Secondary-RAT Usage Report configuration from call-control-profile. It fallbacks to MME service-level configuration.
- **secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }** MME sets IR-SGW and IR-PGW flags based on the available options configured for Secondary-RAT data usage report. By default, MME disables the Secondary-RAT data usage reporting towards both SGW and PGW. If the configuration is removed from call-control-profile, then it fall-back to MME-SERVICE level configuration for Secondary-RAT-Data-Usage-Report functionality.
  - **secondary-rat data-usage-report sgw** Disables the Secondary-RAT Usage Report option for P-GW and enables only for S-GW.
  - **secondary-rat data-usage-report pgw** Disables the Secondary-RAT Usage Report option for SGW and enables only for PGW.
  - **secondary-rat data-usage-report sgw pgw** Enables Secondary-RAT Usage Report option for both SGW and PGW.
  - **secondary-rat data-usage-report pgw sgw** Enables Secondary-RAT Usage Report option for both SGW and PGW.

Enabling Secondary RAT Data Usage Report in MME Service

Use the following configuration to enable Secondary RAT Data Usage Report to support 5G NSA.

```
configure
  context context_name
    mme-service service_name
      secondary-rat data-usage-report { pgw [ sgw ] | sgw [ pgw ] }
      no secondary-rat data-usage-report
      end
```

Important Both CLI configuration and the current running procedure are taken into account while filling the flags IRSGW/IRPGW in GTPv2 messages towards S-GW/P-GW.

NOTES:

- **no**: Disables the Secondary RAT Usage Report at mme-service.
- **secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }** MME sets IR-SGW and IR-PGW flags based on the available options configured for Secondary-RAT data usage report. By default, MME disables the Secondary-RAT data usage reporting towards both SGW and PGW. If the configuration is removed from call-control-profile, then it fall-back to MME-SERVICE level configuration for Secondary-RAT-Data-Usage-Report functionality.
  - **secondary-rat data-usage-report sgw**: Disables the Secondary-RAT Usage Report option for P-GW and enables only for S-GW.
  - **secondary-rat data-usage-report pgw** : Disables the Secondary-RAT Usage Report option for S-GW and enables only for P-GW.
  - **secondary-rat data-usage-report sgw pgw**: Enables Secondary-RAT Usage Report option for both S-GW and P-GW.
  - **secondary-rat data-usage-report pgw sgw**: Enables Secondary-RAT Usage Report option for both S-GW and P-GW.

Configuring Pre-Release 8 QoS Mapping QCI

Use the following configuration to configure mapping of EPC QOS (non-standard QCIs) to 3GPP Pre-Release 8 QOS.

```
configure
  bearer-control-profile profile_name
    pre-rel8-qos-mapping qci qci_val
    remove pre-rel8-qos-mapping qci
    end
```

NOTES:

- **bearer-control-profile** *profile_name*: Creates an instance of a bearer control profile. *profile_name* specifies the name of the bearer control profile as an alphanumeric string of 1 to 64 characters.
- **remove**: Removes the DCNR configuration from the call control profile.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 65, 66, 69, 70, 80, 82, and 83.

Configuring Dedicated Bearer MBR Values

Use the following configuration to configure the quality of service maximum bit rate (MBR) values for the dedicated bearer.

```
configure
  apn-profile apn_profile_name
    qos dedicated-bearer mbr max-ul mbr_up max-dl mbr_down
    remove qos dedicated-bearer
    end
```

NOTES:

- **apn-profile** *apn_profile*: Creates an instance of an Access Point Name (APN) profile. *apn_profile_name* specifies the name of the APN profile as an alphanumeric string of 1 to 64 characters.
- **qos**: Configures the quality of service (QoS) parameters to be applied.
- **dedicated-bearer mbr**: Configures the maximum bit rate (MBR) for the dedicated bearer.
- **max-ul** *mbr_up*: Defines the maximum bit rate for uplink traffic. *mbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).
- **max-dl** *mbr_down*: Defines the maximum bit rate for downlink traffic. *mbr_down* must be an integer from 1 to 4000000000000 (4 Tbps).
- **remove**: Deletes the dedicated bearer MBR changes from the configuration for this APN profile.

Configuring Dedicated Bearer MBR Values

Use the following configuration to configure the quality of service maximum bit rate (MBR) values for the dedicated bearer.

```
configure
  bearer-control-profile profile_name
    dedicated-bearer { mbr mbr-up mbr_up mbr-down mbr_down | gbr gbr-up gbr_up
 gbr-down gbr_down
    remove dedicated-bearer { gbr | mbr }
    end
```

NOTES:

- **bearer-control-profile** *profile_name*: Creates an instance of a bearer control profile. *profile_name* specifies the name of the bearer control profile as an string from 1 to 64 characters.
- **dedicated-bearer mbr**: Configures the maximum bit rate (MBR) for the dedicated bearer.
- **gbr-up** *gbr_up*: Defines the guaranteed bit rate for uplink traffic. *gbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).
- **gbr-down** *gbr_down*: Defines the guaranteed bit rate for downlink traffic. *gbr_down* must be an integer from 1 to 4000000000000 (4 Tbps).
- **mbr-up** *mbr_up*: Defines the maximum bit rate for uplink traffic. *mbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).

- **mbr-down** *mbr_down*: Defines the maximum bit rate for downlink traffic. *mbr_down* must be an integer from 1 to 4000000000000 (4 Tbps).
- **remove**: Deletes the dedicated bearer MBR changes from the configuration for this bearer control profile.

Configuring UE AMBR Values

Use the following configuration to configure the values for aggregate maximum bit rate stored on the UE (UE AMBR).

```
configure
  call-control-profile profile_name
    qos ue-ambr { max-ul mbr_up max-dl mbr_down }
    remove qos ue-ambr
    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.
- **qos**: Configures the quality of service (QoS) parameters to be applied.
- **ue-ambr**: Configures the aggregate maximum bit rate stored on the UE (UE AMBR).
- **max-ul** *mbr_up*: Defines the maximum bit rate for uplink traffic. *mbr_up* must be an integer from 1 to 4000000000000 (4 Tbps).
- **max-dl** *mbr_down*: Defines the maximum bit rate for uplink traffic. *mbr_down* must be an integer from 1 to 4000000000000 (4 Tbps).
- **remove**: Deletes the configuration from the call control profile.

Monitoring and Troubleshooting

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

Show Commands and Outputs

show mme-service db record imsi

The output of this command includes the following fields:

ARD:

- Dual-Connectivity-NR-not-allowed — Displays True or False to identify if the ARD received from HSS indicates the DCNR feature is allowed for the given IMSI or not.

show mme-service name <mme_svc_name>

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

show mme-service session full all

The output of this command includes the following fields:

UE DC-NR Information:

- DC-NR capable UE — Indicates whether the UE is DCNR capable.
- DC-NR operation allowed — Indicates whether the DCNR operation is allowed by MME for the DCNR capable UE.

show mme-service statistics

- Dual Connectivity with NR Statistics:

  Attach Procedure

  - Attach Request Rcvd — The number of Attach Request messages received with UE advertising DCNR support.
  - Attach Acc DCNR allowed — The number of Attach Accept messages sent by the MME acknowledging the DCNR support for UE (Restrict DCNR bit not set in Attach Accept).
  - Attach Acc DCNR denied — The number of Attach Accepts sent by MME rejecting the DCNR support for the UE (Restrict DCNR bit set in Attach Accept).
  - Attach Reject Sent — The number of Attach Reject messages sent by MME whose corresponding Attach Request messages have DCNR support capability.
  - Attach Complete Rcvd — The number of Attach Complete messages received by MME whose corresponding Attach Request messages have DCNR support capability.

  Intra-MME TAU Procedure

  - TAU Request Rcvd — The number of TAU Request messages received for Intra-MME TAU procedure with UE advertising DCNR support.
  - TAU Accept DCNR allowed — The number of TAU Accept messages sent by the MME acknowledging the DCNR support for UE (Restrict DCNR bit not set in TAU Accept) for Intra-MME TAU procedure.
  - TAU Accept DCNR denied — The number of TAU Accept messages sent by the MME rejecting the DCNR support for UE (Restrict DCNR bit set in TAU Accept) for Intra-MME TAU procedure.
  - TAU Complete Rcvd — The number of TAU Complete messages received by the MME whose corresponding Intra-MME TAU Requests have DCNR support capability.

  Inter-MME TAU Procedure

  - TAU Request Rcvd — The number of TAU Request messages received for Inter-MME TAU procedure with UE advertising DCNR support.

- TAU Accept DCNR allowed — The number of TAU Accept messages sent by the MME acknowledging the DCNR support for UE (Restrict DCNR bit not set in TAU Accept) for Inter-MME TAU procedure.
- TAU Accept DCNR denied — The number of TAU Accept messages sent by the MME rejecting the DCNR support for UE (Restrict DCNR bit set in TAU Accept) for Inter-MME TAU procedure.
- TAU Reject Sent — The number of TAU Reject messages sent by the MME whose corresponding Inter-MME TAU Requests have DCNR support capability.
- TAU Complete Rcvd — The number of TAU Complete messages received by the MME whose corresponding Inter-MME TAU Requests have DCNR support capability.

Dual Connectivity with NR Subscribers

- Attached Calls — The number of DCNR supported UEs attached with the MME.
- Connected Calls — The number of DCNR supported UEs in connected mode at the MME.
- Idle Calls — The number of DCNR supported UEs in idle mode at the MME.

Node Selection:

SGW DNS:

- Common — The number of times S-GW DNS selection procedures are performed with DNS RR excluding the NR network capability.
- NR Capable — The number of times S-GW DNS selection procedures are performed with DNS RR including the NR network capability.

SGW Local Config

- Common — The number of times S-GW selection procedures are performed with locally configured S-GW address, without considering the NR network capability.

PGW DNS:

- Common — The number of times P-GW DNS selection procedures are performed with DNS RR excluding the NR network capability.
- NR Capable — The number of times P-GW DNS selection procedures are performed with DNS RR including the NR network capability.

PGW Local Config:

- Common — The number of times P-GW selection procedures are performed with locally configured P-GW address, without considering the NR network capability.

Important When UE is defined with "UE usage type" and "NR Capable", S-GW/P-GW via DNS is selected in the following order:

1. MME chooses S-GW/P-GW that support both +ue and +nr services.
2. If step 1 fails, MME selects S-GW/P-GW that supports +nr service only.
3. If step 2 fails, MME selects S-GW/P-GW that supports +ue service only.
4. If step 3 fails, MME selects S-GW/P-GW without +nr or +ue service.

- Handover Statistics:
  - Bearer Statistics
    - ERAB Modification Indication
      - Attempted — The number of bearers for which the E-RAB Modification Indication procedure is attempted (bearer level stats).
      - Success — The number of bearers for which the E-RAB Modification Indication procedure has succeeded (bearer level stats).
      - Failures — The number of bearers for which the E-RAB Modification Indication procedure has failed (bearer level stats).

- ESM Statistics:

  DCNR User PDN Connections:
  - Attempted — The total number of attempts made for DCNR user PDN connections associated with all MME services on the system.
  - Success — The total number of successful attempts for DCNR user PDN connections associated with all MME services on the system.
  - Failures — The total number of attempts failed for DCNR user PDN connections associated with all MME services on the system.

- DCNR User PDN Statistics:
  - All PDNs — Displays statistics for all DCNR user PDNs, connected and idle, through the MME service(s) on the system.
  - Connected PDNs — Displays statistics for connected DCNR user PDNs through the MME service(s) on the system.
  - Idle PDNs — Displays statistics for idle DCNR user PDNs through the MME service(s) on the system.

- Paging Initiation for PS QCI-80, QCI 82, and QCI 83 Events:
  - Attempted — The total number of ECM statistics related to PS paging initiation events attempted for QCI 80, QCI 82, and QCI 83.

- Success — The total number of ECM statistics related to PS paging initiation events successful for QCI 80, QCI 82, and QCI 83.
- Failures — The total number of ECM statistics related to PS paging initiation events failed for QCI 80, QCI 82, and QCI 83.
  - Success at Last n eNB — The total number of ECM statistics related to PS paging initiation events succeeded at the last known eNodeB for QCI 80, QCI 82, and QCI 83.
  - Success at Last TAI — The total number of ECM statistics related to PS paging initiation events succeeded at the eNodeB in the TAI from which the UE was last heard for QCI 80, QCI 82, and QCI 83.
  - Success at TAI List — The total number of ECM statistics related PS paging initiation events succeeded at the eNodeB in all TAIs present in the TAI list assigned to the UE for QCI 80, QCI 82, and QCI 83.

show mme-service statistics dcnr

The output of this command includes the following fields:

Secondary RAT Usage Reports Rx Count

- UE Ctxt Release Req — Indicates the number of secondary RAT data usage reports received in UE context release request message.
- UE Ctxt Release Cmpl — Indicates the number of secondary RAT data usage reports received in UE context release complete message .
- E-RAB Mod Ind — Indicates the number of secondary RAT data usage reports received in eRAB Modification Indication message.
- E-RAB Release Ind — Indicates the number of secondary RAT data usage reports received in eRAB Release Indication message.
- E-RAB Release Resp — Indicates the number of secondary RAT data usage reports received in eRAB Release Response message.
- Secondary RAT Data Usage Report[Periodic] — Indicates the number of secondary RAT data usage reports received in Secondary RAT Data Usage Report message without Handover flag.
- Seccondary RAT Data Usage Report[Handover] — Indicates the number of secondary RAT data usage reports received in Secondary RAT Data Usage Report message with Handover flag.
- S10 Fwd Reloc Cmpl Ack — Indicates the number of secondary RAT data usage reports received in Forward Reloc Complete Ack message from MME to MME.
- Dropped Periodic Report[HO in progress] — Indicates the number of secondary RAT data usage reports dropped when Secondary RAT Data Usage Report message was received without Handover flag during Handover.

Secondary RAT Usage Reports Tx Count:

- Create Session Req — Indicates the number of secondary RAT data usage reports sent in Create Session Request .

- Delete Session Req — Indicates the number of secondary RAT data usage reports sent in Delete Session Request.
- Delete Bearer Rsp — Indicates the number of secondary RAT data usage reports sent in Delete Bearer Response .
- Release Access Brr Req — Indicates the number of secondary RAT data usage reports sent in Release Access Bearer Request.
- Delete Bearer Cmd —Indicates the number of secondary RAT data usage reports sent in Delete Bearer Command.
- Modify Bearer Req — Indicates the number of secondary RAT data usage reports sent in Modify Bearer Request.
- Change Notification — Indicates the number of secondary RAT data usage reports sent in Change Notification.
- S10 Fwd Reloc Cmpl Ack — Indicates the number of secondary RAT data usage reports sent in Forward Reloc Complete Ack.

show mme-service statistics s1ap

The output of this command includes the following fields:

S1AP Statistics:

Transmitted S1AP Data:

- E-RAB Modification Cfm — Indicates the number of E-RAB Modification Confirm messages sent by MME upon successful E-RAB modification procedure.

Received S1AP Data

- E-RAB Mod Ind — Indicates the number of E-RAB Modification Indication messages received from the master eNodeB.

Received S1AP Data:

- Secondary RAT Data Usage Report — Indicates the number of Secondary RAT Data Usage Report messages received from eNodeB.

show subscribers mme-service

The output of this command includes the "DCNR Devices" field to indicate the number of DCNR devices that are attached to the MME.

show call-control-profile full all

The output of this command includes the following fields:

- DCNR
- Secondary RAT Usage Report

show mme-service all

The output of this command includes the following fields:

- DCNR
- Secondary RAT Usage Report

Bulk Statistics

This section provides information on the bulk statistics for the 5G NSA feature on MME.

MME Schema

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

Bulk Statistics	Description
attached-dcnr-subscriber	The current total number of attached subscribers capable of operating in DCNR.
connected-dcnr-subscriber	The current total number of subscribers capable of operating in DCNR and in connected state.
idle-dcnr-subscriber	The current total number of subscribers capable of operating in DCNR and in idle state.
dcnr-attach-req	The total number of Attach Request messages that are received with DCNR supported.
dcnr-attach-acc-allowed	The total number of Attach Accept messages that are sent with DCNR allowed.
dcnr-attach-acc-denied	The total number of Attach Accept messages that are sent with DCNR denied.
dcnr-attach-rej	The total number of DCNR requested Attach Rejected messages.
dcnr-attach-comp	The total number of Attach Complete messages that are received for DCNR supported attaches.
dcnr-intra-tau-req	The total number of Intra-TAU Request messages that are received with DCNR supported.
dcnr-intra-tau-acc-allowed	The total number of Intra-TAU Accept messages that are sent with DCNR allowed.
dcnr-intra-tau-acc-denied	The total number of Intra-TAU Accept messages that are sent with DCNR denied.
dcnr-intra-tau-comp	The total number of Intra-TAU Complete messages that are received for DCNR supported requests.

Bulk Statistics	Description
dcnr-inter-tau-req	The total number of Inter-TAU Request messages that are received with DCNR supported.
dcnr-inter-tau-acc-allowed	The total number of Inter-TAU Accept messages that are sent with DCNR allowed.
dcnr-inter-tau-acc-denied	The total number of Inter-TAU Accept messages that are sent with DCNR denied.
dcnr-inter-tau-rej	The total number of DCNR requested Inter-TAU Request messages that are rejected.
dcnr-inter-tau-comp	The total number of Inter-TAU Complete messages that are received for DCNR supported requests.
s1ap-recdata-eRabModInd	The total number of S1 Application Protocol - E-RAB Modification Indication messages received from all eNodeBs.
s1ap-transdata-eRabModCfm	The total number of E-RAB Modification Confirmation messages sent by the MME to the eNodeB.
erab-modification-indication-attempted	The total number of bearers for which E-RAB Modification Indication messages were sent.
erab-modification-indication-success	The total number of bearers for which E-RAB Modification Indication messages were sent.
erab-modification-indication-failures	The total number of bearers for which E-RAB Modification Indication failed as shown in E-RAB Modification Indication Confirm message.
emmevent-path-update-attempt	The total number of EPS Mobility Management events - Path Update attempted.
emmevent-path-update-success	The total number of EPS Mobility Management events - Path Update successes.
emmevent-path-update-failure	The total number of EPS Mobility Management events - Path Update failures.
dcnr-dns-sgw-selection-common	The total number of times S-GW DNS selection procedures are performed with DNS RR excluding NR network capability.
dcnr-dns-sgw-selection-nr	The total number of times S-GW DNS selection procedures were performed with DNS RR including NR network capability.

Bulk Statistics	Description
dcnr-dns-sgw-selection-local	The total number of times S-GW selection procedures were performed with locally configured S-GW address, without considering the NR network capability.
dcnr-dns-pgw-selection-common	The total number of times P-GW DNS selection procedures were performed with DNS RR excluding NR network capability.
dcnr-dns-pgw-selection-nr	The total number of times P-GW DNS selection procedures were performed with DNS RR including NR network capability.
dcnr-dns-pgw-selection-local	The total number of times P-GW selection procedures were performed with locally configured P-GW address, without considering the NR network capability.
esmevent-dcnr-user-pdncon-attempt	The total number of EPS Session Management events - DCNR User PDN connections - attempted.
esmevent-dcnr-user-pdncon-success	The total number of EPS Session Management events - DCNR User PDN connections - successes.
esmevent-dcnr-user-pdncon-failure	The total number of EPS Session Management events - DCNR User PDN connections - failures.
pdn-dcnr-user-all	The current total number of DCNR user PDN connections in any state.
pdn-dcnr-user-connected	The current total number of DCNR user connected PDNs.
pdn-dcnr-user-idle	The current total number of DCNR user idle PDNs.
ps-qci-80-paging-init-events-attempted	The total number of ECM statistics related to PS paging initiation events attempted for QCI 80.
ps-qci-80-paging-init-events-success	The total number of ECM statistics related to PS paging initiation events successful for QCI 80.
ps-qci-80-paging-init-events-failures	The total number of ECM statistics related to PS paging initiation events failed for QCI 80.
ps-qci-80-paging-last-enb-success	The total number of ECM statistics related to PS paging initiation events succeeded at the last known eNodeB for QCI 80.
ps-qci-80-paging-last-tai-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in the TAI from which the UE was last heard for QCI 80.

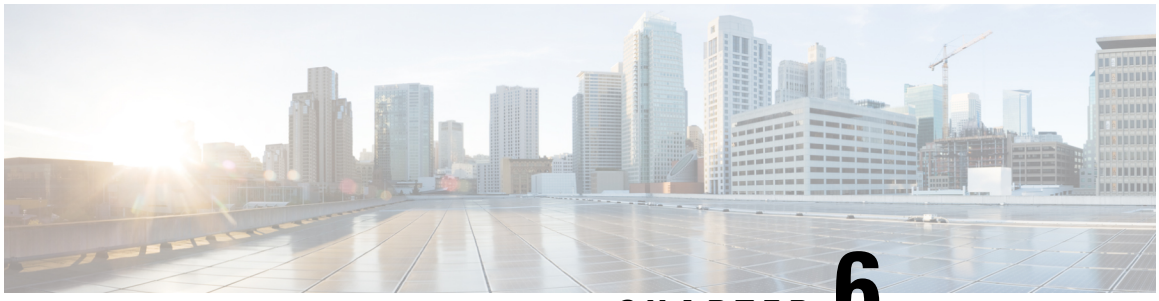
Bulk Statistics	Description
ps-qci-80-paging-tai-list-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE for QCI 80.
ps-qci-82-paging-init-events-attempted	The total number of ECM statistics related to PS paging initiation events attempted for QCI 82.
ps-qci-82-paging-init-events-success	The total number of ECM statistics related to PS paging initiation events successful for QCI 82.
ps-qci-82-paging-init-events-failures	The total number of ECM statistics related to PS paging initiation events failed for QCI 82.
ps-qci-82-paging-last-enb-success	The total number of ECM statistics related to PS paging initiation events succeeded at the last known eNodeB for QCI 82.
ps-qci-82-paging-last-tai-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in the TAI from which the UE was last heard for QCI 82.
ps-qci-82-paging-tai-list-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE for QCI 82.
ps-qci-83-paging-init-events-attempted	The total number of ECM statistics related to PS paging initiation events attempted for QCI 83.
ps-qci-83-paging-init-events-success	The total number of ECM statistics related to PS paging initiation events successful for QCI 83.
ps-qci-83-paging-init-events-failures	The total number of ECM statistics related to PS paging initiation events failed for QCI 83.
ps-qci-83-paging-last-enb-success	The total number of ECM statistics related to PS paging initiation events succeeded at the last known eNodeB for QCI 83.
ps-qci-83-paging-last-tai-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in the TAI from which the UE was last heard for QCI 83.
ps-qci-83-paging-tai-list-success	The total number of ECM statistics related to PS paging initiation events succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE for QCI 83.

Bulk Statistics	Description
s1ap-recdata-secratdatausagerep	Total number of Secondary RAT Data Usage Report messages received by MME.
dcnr-s1ap-rx-srur-uectxtrelreq	Total number of reports received in UE Context Release Request.
dcnr-s1ap-rx-srur-uectxtrelcmpl	Total number of reports received in UE Context Release Complete.
dcnr-s1ap-rx-srur-erabmodind	Total number of reports received in eRAB Modification Indication.
dcnr-s1ap-rx-srur-erabrelind	Total number of reports received in eRAB Release Indication.
dcnr-s1ap-rx-srur-erabrelres	Total number of reports received in eRAB Release Response.
dcnr-s10-rx-srur-fwdrelcmpack	Total number of reports received in Forward Relocation Complete Ack.
dcnr-s11-tx-srur-csreq	Total number of reports sent in Create Session Request.
dcnr-s11-tx-srur-dsreq	Total number of reports sent in Delete Session Request.
dcnr-s11-tx-srur-dbrsp	Total number of reports sent in Delete Bearer Response.
dcnr-s11-tx-srur-rabreq	Total number of reports sent in Release Access bearer Request.
dcnr-s11-tx-srur-dbcmd	Total number of reports sent in Delete Bearer Command.
dcnr-s11-tx-srur-mbreq	Total number of reports sent in Modify Bearer Request.
dcnr-s11-tx-srur-chngnot	Total number of reports sent in Change Notification.
dcnr-s10-tx-srur-fwdrelcmpack	Total number of reports sent in Forward Relocation Complete Ack.
dcnr-s1ap-rx-srur-periodicdropped	Total number of reports dropped when Secondary RAT Data Usage Report message was received without Handover flag during Handover.
dcnr-s1ap-rx-srdur-periodic	Total number of reports received in Secondary RAT Data Usage Report message without Handover flag.
dcnr-s1ap-rx-srdur-ho	Total number of reports received in Secondary RAT Data Usage Report message with Handover flag.

TAI Schema

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

Bulk Statistics	Description
tai-esmevent-dcnr-user-pdncon-attempt	The total number of DCNR User PDN connection EPS Session Management events attempted per TAI.
tai-esmevent-dcnr-user-pdncon-success	The total number of successful DCNR User PDN connection EPS Session Management events per TAI.
tai-esmevent-dcnr-user-pdncon-failure	The total number of failed DCNR User PDN connection EPS Session Management events per TAI.



CHAPTER 6

Co-Located SPGW Selection for Emergency Bearer

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*

Revision History

Revision Details	Release
Introduced to 21.17 release.	21.17
First Introduced.	21.14.8

Feature Changes

Previous Behavior: MME selects random P-GW based on LTE Emergency Profile configuration for Emergency Bearer service requested using PDN Connectivity Request.

New Behavior: MME uses the canonical name of the selected S-GW (from DNS response) for the previously established PDNs and compares it with the statically configured P-GW collocation string in the LTE emergency profile to select the P-GW. The static P-GW collocation string must be configured with the canonical node name of the P-GW to ensure to select collocated node for emergency call.

Important This behavior applies only to the PDN connectivity request for Emergency Bearer Service.

Command Changes

pgw co-location

Use the following configuration to configure P-GW co-location:

```
configure
   lte-policy
      lte-emergency-profile profile_name
         [ no ] pgw co-location
         end
```

NOTES:

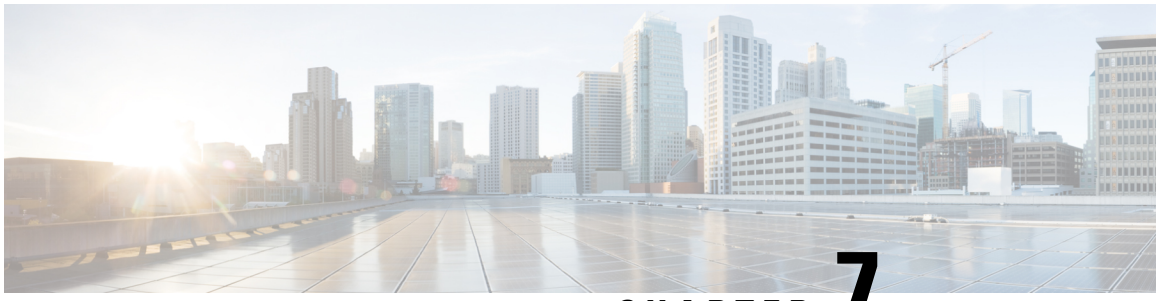
- **no** Disables the P-GW co-location configuration.
- **co-location** Configures to select the co-located S-GW/P-GW node based on static P-GW configuration and S-GW selected through DNS.

Performance Indicator Changes

show lte-policy lte-emergency-profile <profile_name>

The output of this command includes the following fields:

- pgw co-location: Indicates if the P-GW co-location feature is enabled or disabled.



CHAPTER 7

Configuring UE Radio Capability IE Size

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	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.

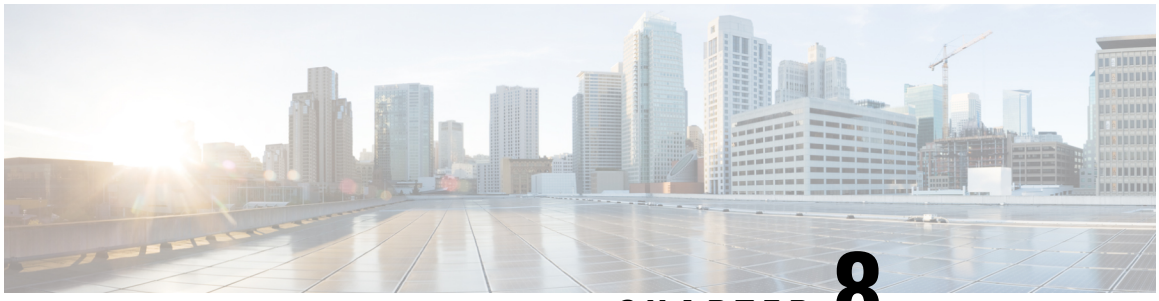
Configuring the UE Radio Capability IE

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 8

Counter Enhancements on TAC and LAC Levels

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
New counters are added iin 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 1: 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.

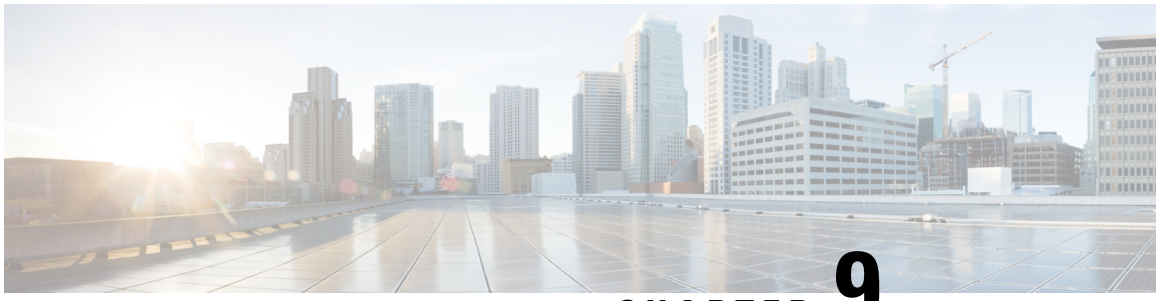
Bulk Statistics

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

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*

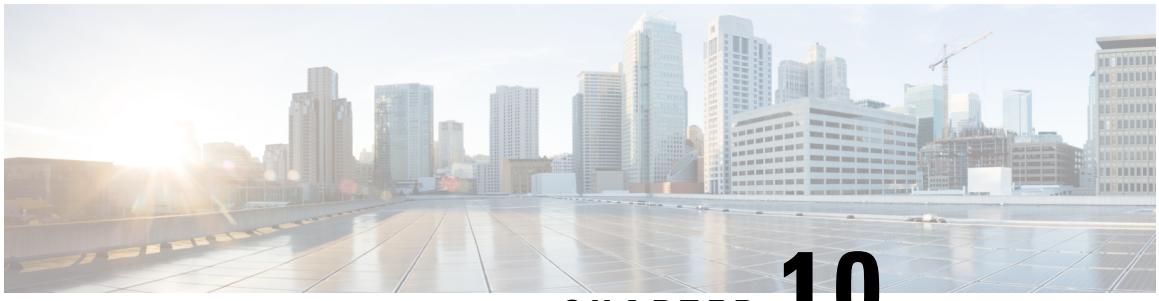
Revision History

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

Diameter Pending Transaction

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SAEGW
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.

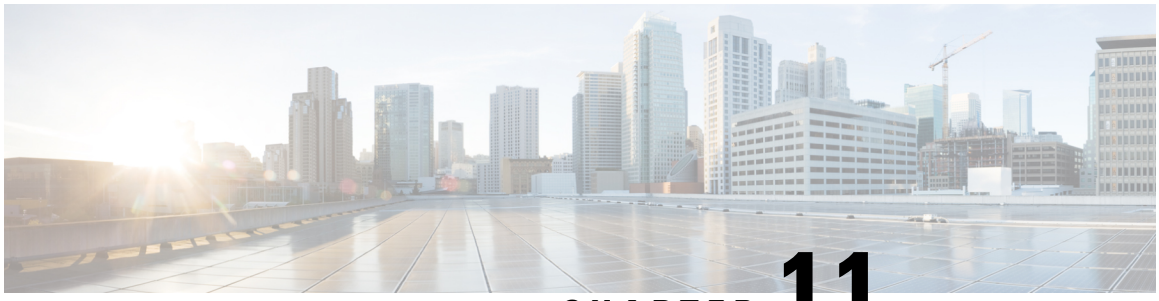
Revision Details	Release
With this release, new behaviour for sending Diameter result code is added in compliance with 3GPP TS 29.212.	21.17
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: The P-GW sends result code as 4144 in RAA when pending transaction feature was enabled/disabled, and CCA-T was pending from PCRF.

New Behavior: The P-GW sends experimental result code as 4144 in RAA when pending transaction feature is enabled. The P-GW sends result code as 3002 in RAA when pending transaction feature is disabled in RAA, and CCA-T is pending from PCRF.

Customer Impact: This behavior change is in compliance with the 3GPP TS 29.212.



CHAPTER 11

Extraction of IPv4 Addresses Embedded in IPv6 Addresses

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
With this release, support is added for extraction of IPv4 addresses embedded in IPv6 addresses using the Command Line Interface (CLI).	21.17.16

Feature Description

Learning the IPv4 address, which is embedded in IPv6 address through DNS snooping, requires matching of IPv4 format against the address learnt from the DNS response.

In the release 21.17.16, IPv4 extraction is done by enhancing the existing Command Line Interface (CLI) for Well-known prefix and Network-specific prefix. For more information on prefixes, refer RFC6052 document.

After the required changes are done in the CLI, IPv4 address extraction happens and the lookup of IPv4 address is done using the learnt address pool.

Relationships to other Features

This feature is related to DNS Snooping feature. For more information about DNS Snooping feature, refer the *DNS Snooping* chapter in the *ECS Administration Guide.*

License Requirements

The Extraction of IPv4 Addresses Embedded in IPv6 Addresses requires the same DNS Snooping license. 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*.

How it Works

The following procedure describes the steps to be followed for IPv4 address extraction:

1. P-GW monitors all responses sent to the UE.
2. P-GW snoops only the DNS response and identifies all the IP addresses resulting from the DNS response.
3. The first data packet from IPv4 device reaches P-GW.
4. The Session Manager receives data indication and routes the packet to the ACS manager.
5. The ACS manager analyzes the packet and assigns data session for the flow.
6. Prefix matching is done based on the configured prefix.

Based on the matching, IPv4 address is extracted and it is stored in the ACS data session. Then, IPv4 address starts the lookup in the IPv4 address pool and if it matches, then the traffic is matched with the DNS snooping rule. If match does not happen, then it starts to check for other rules.

Restrictions

This section identifies the restrictions to be applied in CLI for IPv4 address extraction.

Prefix-Set Restrictions:

- Allows network-specific prefixes, well-known prefixes but restricts other prefixes.
- Restricts configuring multiple mask values under the same prefix-set.

- Restricts prefix removal from prefix-set, if the same prefix-set is associated with rule base-strip CLI.
- Restricts prefix-set removal, if the same prefix-set is associated with rule base-strip CLI.

Rule base Restrictions:

- Allows network-specific prefixes, well-known prefixes but restrict other prefixes.
- Restricts strip CLI configuration, if rulebase prefix length is not matched to the associated prefix-set mask value.
- Restricts strip CLI configuration, if the rule base associated prefix-set is invalid.
- Restricts strip CLI configuration, if the available prefix-set is empty.

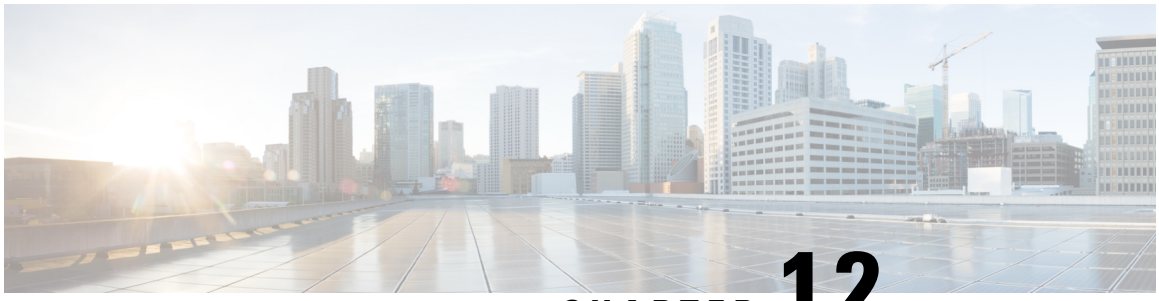
Associating Rulebase to Prefix-Set

Use the following configuration to associate rulebase to the prefix-set.

```
configure
  active-charging service ecs_service_name
    prefix-set prefix_set_name
      exit
    rulebase <rulebase_name>
      strip server-ipv6 prefix_length prefix-set prefix_set_name
      exit
```

NOTES:

- **strip server-ipv6** : Matches the prefix of server IPv6 address with the configured prefixset and prefix length. If match is found then extracts the IPv4 address from the server IPv6 address.
- *prefix_length*: Enter values 32,40,48,56,64 or 96.
- **prefix-set**: Configures the active configuration for Well-known prefix or Netowrk-specific prefix. You can configure a maximum of 10 IPv6 prefixes in a prefix-set.



CHAPTER 12

GTPV1/V2 Echo Support for Peer MME and SGSN

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
This feature is fully qualified in this release.	21.18

Revision Details	Release
First introduced. **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.	21.17

Feature Description

MME supports path management status of MME (S10) and SGSN (Gn/Gp). MME sends and receives GTP V2 Echo Message for Peer Node status in S10 Interface and GTP V1 Echo Message for Peer node status in Gn/Gp Interface. MME sends and receives the Echo message for Configured peer Node in MME regardless of GTP session.

Path failure is detected when there is no response to Echo Request even after max retransmissions. Path failure detection is not done based on "Restart counter value change in echo response".

GTP V1 Echo Message is supported in compliance with the 3GPP 29.060 7.2 Path Management Messages operation and GTP V2 Echo Message is supported in compliance with the 3GPP 29.274, 7.1 Path Management Messages operation.

Existing traps SGSNGtpcPathFailure, SGSNGtpcPathFailureClear, EGTPCPathFail, and EGTPCPathFailClear are used by this feature.

Configuring GTPV1/V2 Echo Support for Peer MME and SGSN

This section provides information on the CLI commands to configure GTPV1/V2 Echo Support for Peer MME and SGSN feature.

Configuring Path Management for Peer MME

Use the following configuration to configure the path management for Peer MME.

```
configure
   context context_name
      mme-service mme_service_name
         peer-mme echo-params interval interval retransmission-timeout
retransmission_timeout max-retransmissions max_retransmissions reconnect-interval
 reconnect_interval
               [ no ] peer-mme echo-params
               end
```

NOTES:

- **no**: Removes the path management configuration for peer MME with Gn/Gp capability.
- **peer-mme**: Configures a Peer MME for inter-MME relocations.
- **echo-params** : Configures echo parameters for peer MME with GN/GP capability.

- **interval** *interval*: Configures echo interval in seconds. *interval* must be an integer from 60 to 300.
- **retransmission-timeout** *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an integer from 1 to 20.
- **max-retransmissions** *max_retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an integer from 0 to 15.
- **reconnect-interval** *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an integer from 60 to 86400.

Configuring Path Management for Peer SGSN

Use the following configuration to configure the path management for Peer SGSN.

```
configure
   context context_name
      mme-service mme_service_name
         peer-sgsn echo-params interval interval retransmission_timeout
retransmission_timeout max-retransmissions max-retransmissions reconnect-interval
 reconnect_interval
            no peer-sgsn echo-params
            end
```

NOTES:

- **no**: Removes the path management configuration for peer SGSN with Gn/Gp capability.
- **echo-params** : Configures echo parameters for peer SGSN with GN/GP capability.
- **interval** *interval*: Configures echo interval in seconds. *interval* must be an integer from 60 to 300.
- **retransmission-timeout** *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an integer from 1 to 20.
- **max-retransmissions** *max-retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an integer from 0 to 15.
- **reconnect-interval** *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an integer from 60 to 86400.

Monitoring and Troubleshooting

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

Show Commands and Outputs

show mme-service all name

The output of this command includes the following fields:

- PEER MME Echo Parameters :
  - interval
  - retransmission timeout
  - max retransmissions
  - reconnect interval
- PEER GN/GP SGSN Echo Parameters:
  - interval
  - retransmission timeout
  - max retransmissions
  - reconnect interval

show egtpc statistics

The output of this command includes the following fields:

Path Management Messages:

PEER MME Echo Request

- Total TX
- Initial TX
- Retrans TX

PEER MME Echo Response:

- Total RX

show egtpc peers mme

```
+----Status:   (D) - Dead    (A) - Alive
 |
 |+---IP Type:     (S) - Static  (D) - Dynamic
 ||  Service              Echo Req           Echo Req   Echo Rsp
 vv  ID      Peer Address  Time of Creation   Sent       Retransmitted  Received
 -- --- ---------------    ------------------ --------  ---------------
```

Total Peers:

Show sgtpc statistic

Path Management Messages:

Echo Request:

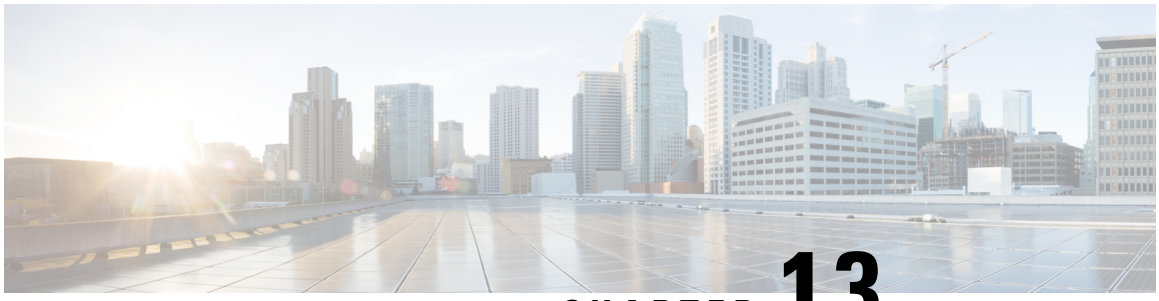
```
  Total   Echo-Req TX:     Total   Echo-Req RX:
  Initial Echo-Req TX:     Initial Echo-Req RX:
  Retrans Echo-Req TX:
```

Echo Response:

```
Total Echo-Rsp TX:    Total Echo-Rsp RX:
```

show sgtpc peers

```
Path     Service               Echo Req       Echo Req        Echo Rsp
Status   ID      Peer Address           Sent         Retransmitted     Received
----     --- ----------------------  -----------   ---------------   ---------
```



CHAPTER 13

MME MDT Management Support

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
First introduced.	21.17

Feature Description

If "MDT User Consent AVP" with value CONSENT_GIVEN(1) is received from HSS/S6a, MME encodes MDT Management Allowed IE in S1AP ICSR and Handover Request messages. Also, during handover this MDT status information is sent as part of Indication flags IE in Forward Relocation Request and Context Response messages.

Configuring MDT Management

This section describes how to configure MME MDT Management.

Configuring MME Minimization Drive Test

Use the following configuration to configure minimization drive test.

```
configure
  context context_name
    mme-service service_name
      [ no ] minimization-drive-test
      end
```

NOTES:

- **no minimization-drive-test**: Disables the Minimization Drive Test (MDT) handling on MME.
- **minimization-drive-test**: Enable Minimization Drive Test (MDT) handling on MME.

Monitoring and Troubleshooting

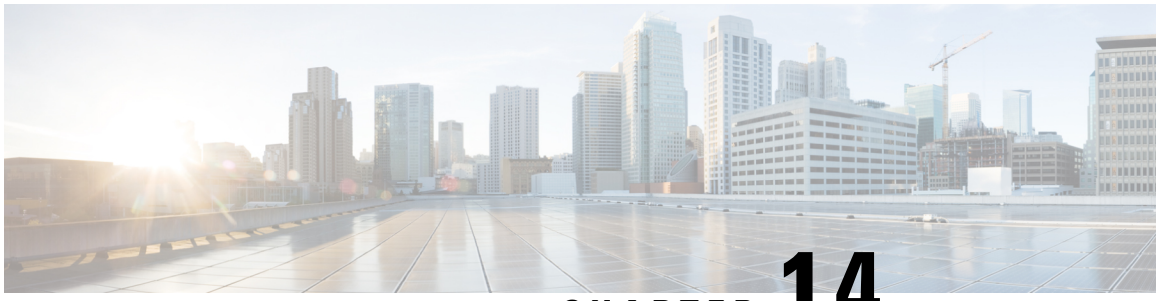
This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the MME MDT Management.

Show Commands and Outputs

show mme-service all

The output of this command includes the following fields:

- Minimization Drive Test



CHAPTER 14

MME Support for EN-DC SON Configuration Transfer IE on S1-AP

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	Configuration Not Required
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	Release
This feature is fully qualified in this release.	21.18
First introduced. **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.	21.17

Feature Description

Configuration Transfer enables the transfer of information between two eNodeBs at any time via S1 interface and the Core Network.

MME supports EN-DC SON Configuration Transfer IE in eNB Configuration Transfer Message and MME Configuration Transfer Message in compliance with specification 36.413 V15.6.0.

eNB Configuration Transfer procedure is initiated with eNB configuration transfer message sent from the eNB to the MME. If the MME receives the EN-DC SON Configuration Transfer IE, it transparently transfers the EN-DC SON Configuration Transfer IE either towards the eNB indicated in the Target eNB-ID IE or towards an eNB connected to the en-gNB indicated in the Target en-gNB-ID IE which is included in the EN-DC SON Configuration Transfer IE. MME sends EN-DC SON Configuration information through Configuration Transfer Tunnel Message to the peer MME.

MME identifies the dynamic eNB to en-gNB mapping entries through the Connected en-gNB List IE in S1 Setup Request message. The connected en-gNB List IE includes Connected en-gNB To Be Added List IE and Connected en-gNB To Be Removed List IE in eNB Configuration Update message. MME maintains eNB and en-gNB mapping entries to handle enb config transfer messages that are received with target engnb-id but without target enb-id.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the MME feature.

Show Commands and Outputs

show mme-service enodeb-association connected-en-gnb all

The output of this command includes the following field:

- connected-en-gnb all — Shows all the en-gNBs connected to all eNodeBs.

  The sample configuration output is an example for the **show mme-service enodeb-association connected-en-gnb all** command :

```
asr5500# show mme-service enodeb-association connected-engnb all
  MMEMgr                        : Instance 1
  Peerid                        : 17301506
  Global ENodeB ID        : 123:123:456
    Connected engNB ID : 4194306
    Broadcast PLMNs       :123:456
                          123:455
    TAC                   : 2400
```

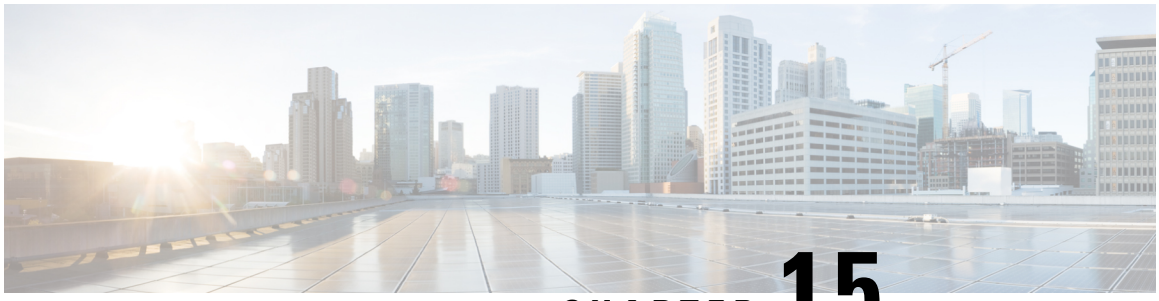
show mme-service enodeb-association connected-en-gnb enodeb-name <enb name>

The output of this command includes the following field::

- connected-en-gnb enodeb-name <enb name> — Shows en-gNBs connected to specific eNodeB.

The sample configuration output is an example for the **show mme-service enodeb-association connected-en-gnb enodeb-name <enb name>** command

```
]asr5500# show mme-service enodeb-association connected-engnb enodeb-name enb1
MMEMgr                          : Instance 1
  Peerid                        : 17301506
  Global ENodeB ID    : 123:123:456
     Connected engNB ID     : 4194306
    Broadcast PLMNs          :123:456
                              123:455
    TAC                       : 2400
```



CHAPTER 15

Maximum MTU Size Changes for Diameter Data Packets Fragmentation

Feature Summary and Revision-History

Summary Data

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

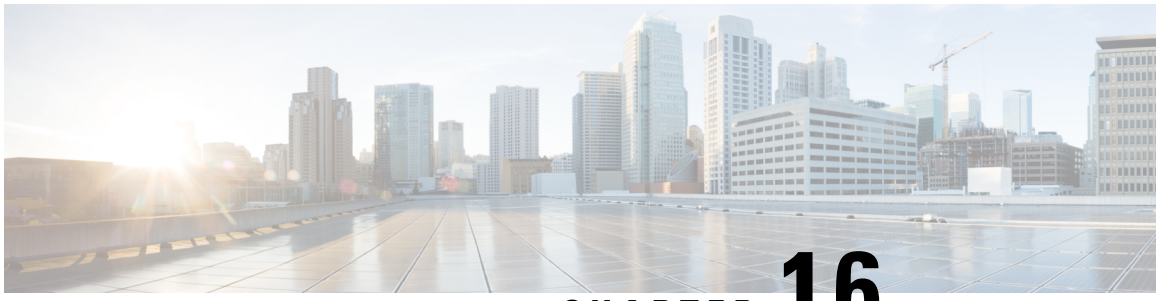
Revision History

Revision Details	Release
With this release, fragmentation of data packets works properly when the sctp CLI is set with the maximu MTU value starting from 512 bytes.	21.17.17

Feature Changes

Previous Behavior: Diameter data packets are not fragmented as per the **sctp-max-mtu-size** configured. This is because the Max MTU size values had the range starting from 508 bytes.

New Behavior: Diameter data packets are fragmented properly when the Maximum MTU size value is configured starting from the range 512 bytes in the **sctp-max-mtu-size** CLI.



CHAPTER 16

NAS Notification for SRVCC Cancellation due to TAU Request

Feature Summary and Revision History

Summary Data

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

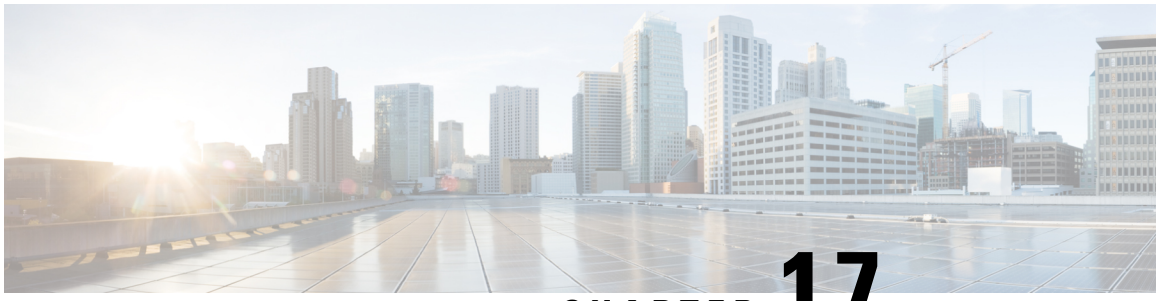
Revision History

Revision Details	Release
In this release, MME supports NAS notification to reestablish IMS for SRVCC Cancellation.	21.11.16
In this release, MME supports NAS notification to reestablish IMS for SRVCC Cancellation.	21.5.26
First Introduced	21.17.6

Feature Changes

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

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



CHAPTER 17

Origin-State-Id AVP Support on P-GW

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Introduced support for indirectly connected Policy and Charging Rules Functions (PCRFs) through Diameter Routing Agent (DRA).	21.17

Revision Details	Release
First introduced.	21.6

Feature Description

The interfaces connected to the P-GW use Diameter protocol for communcation. This protocol provides a mechanism through the Origin-State-Id AVP to detect sessions that are terminated due to unanticipated shutdown of a peer node.

Storing the Origin-State-Id AVP of a peer node enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This ensures that the diameter-nodes are always synchronized with the P-GW. To enable this functionality of storing the Origin-State-Id AVP on the P-GW, the **osid-change** CLI command is introduced at the diameter endpoint level.

Origin-State-Id change detection is applicable only for PCRF nodes.

How It Works

When the **osid-change** CLI command is configured, the diabase starts storing the Origin-State-Id of each peer configured under a diameter endpoint. On receiving a diameter message from a peer, if the Origin-State-Id AVP is present, it is compared with the stored Origin-State-Id. If the received Origin-State-Id is greater than the stored one, gateway will start clearing calls. The Session Manager marks all the subscribers connected to the diameter-session for deletion and starts clearing sessions in a staggered manner. Clearing calls in a staggered manner helps avoid a storm of messages on other connected interfaces. When a subscriber is marked for deletion, the GW drops all the outbound diameter messages on the interface.

As per RFC 6733 (Diameter Base Protocol) Origin-State-Id could come in any diameter message, so the Gateway provides support to detect the change in CEA, CCA and RAR messages.

This feature is supported only with diamproxy mode (single and multiple).

Configuring Origin State Identifier AVP Support on P-GW

The following section provides the configuration command to enable or disable the functionality.

Configuring Origin-State-Id AVP on P-GW

Use the following CLI commands to store the Origin-State-Id AVP of a Diameter peer node on the P-GW. This command is introduced at the diameter endpoint level.

```
configure
  context context_name
    diameter endpoint endpoint_name
      [no] osid-change action clear-subscribers
      end
```

NOTES:

- **no:** Disables the command.
- **action:** Specifies the action to be taken.
- **clear subscribers:** Clears subscribers connected to the peer.
- This functionality is disabled by default.

Monitoring and Troubleshooting

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

Show Commands and/or Outputs

The output of the following CLI command has been enhanced in support of the feature.

show diameter

As part of this functionality, the **show diameter** CLI now includes the values for the following new fields:

- osid-info sessmgr all
- osid-info sessmgr instance_number

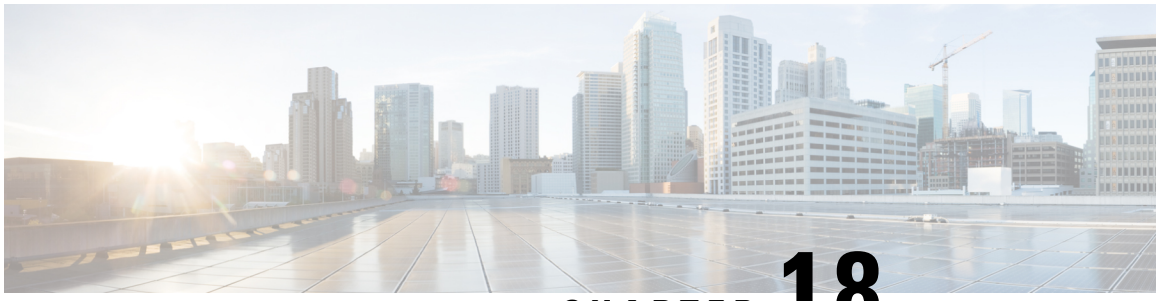
show session disconnect-reasons

The **show session disconnect-reasons** CLI now includes the **osid-change** field.

Bulk Statistics

The following bulk statistics are added in the System schema to support this feature:

Bulk Statistics	Description
disc-reason-656	Indicates the total number of sessions cleared due to change in Origin-State-Id of the Diameter peer.



CHAPTER 18

RTLLI Management for 2G M2M Devices

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
Counter enhancements on TAC and LAC levels are introduced	21.17.9

Feature Description

Fixed Random TLLI (RTLLI) Management for 2G M2M devices is intended to expand the operator's control of TLLI (temporary logical link identifier) in the following scenario:

When multiple M2M devices attempt PS Attaches, with the same fixed RTLLI coming from different NSEIs (network service entity identifier), the SGSN cannot distinguish between the devices. The SGSN functions ***as if*** the first device bearing an RTLLI is no longer attached and begins to communicate with the next device using that same RTLLI. With multiple M2M devices attempting attaches - all with the same RTLLI - the result is TLLI collision and dropped calls.

Counter Enhancements on TAC and LAC Levels

In StarOS 21.17 and later releases, the existing bulk statistics counters, 2G-simple-attach-rej-randomtlli-collision and 2G-combined-attach-rej-randomtlli-collision are updated at LAC level.

How It Works

This feature deals with Attach problems due to simultaneous IMSI attaches, all with the same fixed RTLLI.

Beginning with Release 16.3, it became possible to configure the SGSN to discard/drop Attach Request messages received from an MS with an RTLLI already in use on the SGSN by adding validation of the NSEI. Attach gets processed if the attach is coming from a different NSEI. This functionality is disabled by default.

Beginning with Release 19.3, to further reduce jumbling of authentication vectors across subscribers, the Fixed Random TLLI Handling mechanism extends the functionality noted above. A new verification table has been added to the GbMgr. The table maintains a list of TLLI + NSEI and if an incoming Attach Request includes a TLLI + NSEI already on the table then the call is dropped. This functionality is disabled by default.

Configuring RTLLI Management

No new commands or keywords have been added to the CLI in support of Fixed Random TLLI Management. Enabling / Disabling this mechanism is integrated into existing CLI.

For information about the commands, parameters and parameter values, please check your *Command Line Interface Reference* manual for each of the commands listed below.

Important The following configurations should be performed during system boot up. It is not advisable to enable/disable this TLLI management functionality during runtime.

Verifying Both the RTLLI and the NSEI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying both the RTLLI and the NSEI, use the following configuration:

```
config
  sgsn-global
    gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei
```

```
    old-tlli invalidate tlli hex_value
    old-tlli hold-time time
    end
```

Notes:

- **only-on-same-nsei** - This keyword is required to enable this new verification mechanism.

Verifying Only the RTLLI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying only the RTLLI, use the following configuration:

```
config
  sgsn-global
    gmm-message attach-with-tlli-in-use discard-message
    old-tlli invalidate tlli hex_value
    old-tlli hold-time time
    end
```

Notes:

- **only-on-same-nsei** - Do not include this keyword to disable this new verification mechanism. The system defaults to the verification mechanism provided with Release 16.3 (see *How It Works*).

Verifying Configuration

To verify if the functionality is enabled or disabled, use the following commands from the Exec mode:

```
show configuration | grep gmm-mess
show configuration | grep old-
show configuration verbose | grep old-
```

Monitoring and Troubleshooting

This section provides information for monitoring and/or troubleshooting the RTLLI Management functionality.

To see the statistics of attach drops that are due to same-RTLLI collisions, execute the show commands listed below. When you are looking at the generated statistics, consider the following:

- If the generated counter values are not increasing then collisions are not occurring.
- If the generated counter values are increasing then it means collisions are occurring and attaches were dropped.

Configured to Verify Both RTLLI and NSEI

If **gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei** is configured then the following show command can give the drop count of attaches caused by same RTLLI and NSEI:

```
show gbmgr all parser statistics all | grep use

IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI+NSEI
```

```
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Configured to Verify Only RTLLI

If "gmm-message attach-with-tlli-in-use discard-message" is configured then the following show command can give the drop count of attaches caused by same RTLLI:

```
show gbmgr all parser statistics all | grep use

 IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Verify Attach Rejects due to Same RTLLI

The following show command generates SessMgr counters that track the Attach Rejects due to same RTLLI collision:

```
show gmm sm stats | grep Same random tlli collision

Same random tlli collision: 10
```

Beginning with Release 19.3.5, the 'sgsn-implicit-detach(237)' session disconnect reason pegs when the 2G-SGSN rejects the Attach Request due to same RTLLI collision.

Beginning in Release 19.4, the following show command identifies the two bulk statistics the SGSN uses to track the number of times the SGSN rejects Attach Requests or Combined Attach Requests due to same RTLLI collision.

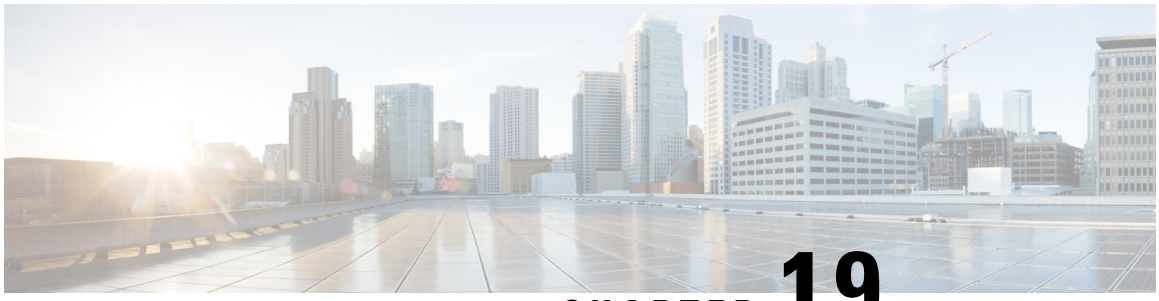
```
show bulkstats variables sgsn | grep colli
%2G-simple-attach-rej-randomtlli-collision%                  Int32     0   Counter
%2G-combined-attach-rej-randomtlli-collision%                Int32     0   Counter
```

In StarOS 21.17 and later releases, the existing bulkstats counters (%2G-simple-attach-rej-randomtlli-collision% , %2G-combined-attach-rej-randomtlli-collision%) are updated at LAC level. Existing counters are added as part of recovery, **gprs-bk schema**:

```
show bulkstats variables gprs-bk | grep tlli
%2G-simple-attach-rej-randomtlli-collision-bk%               Int32     0   Counter
%2G-combined-attach-rej-randomtlli-collision-bk%             Int32     0   Counter
```

To print the recovered statistics, run the following show command:

```
show gmm-sm statistics recovered-values verbose
    2G Attach Rejects due to same rtlli collisions:
      Simple :           0
      Combined :           0
```



CHAPTER 19

SGSN Controlling Peer Status Based on Heartbeat Message

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	ASR 5000
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

Revision Hisotry	Details
First Introduced.	21.17

Feature Description

SGSN considers the peer active only after receiving "ACK" for its heartbeat message. This feature is CLI Controlled for SGSN not to make the SCTP peer active after receiving heartbeat from the peer.

Configuring SGSN Controlling Peer Status Based on Heartbeat Message

This section provides information on the CLI commands to configure SGSN Controlling Peer Status Based on Heartbeat Message feature.

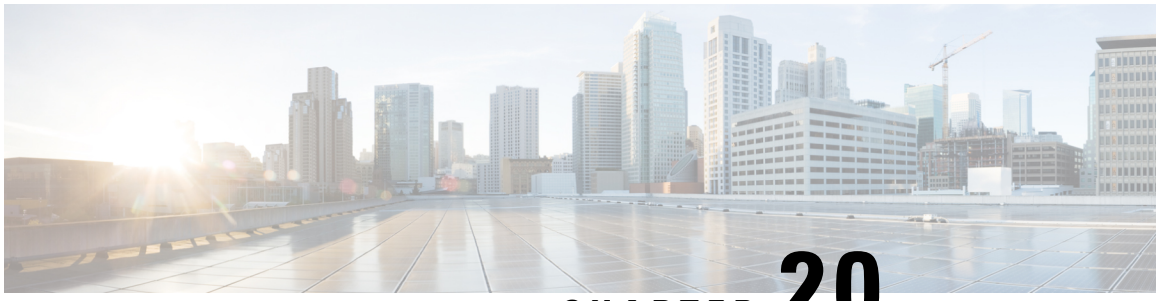
Configuring SCTP Peer Active Heartbeat Acknowledgment

Use the following configuration to configure SCTP peer active heartbeat acknowledgment.

```
configure
  ss7-routing-domain SS7_routing_domain_index variant itu
    peer-server id server_id
       psp instance psp_instance
          no associate asp
             [ no ] sctp-peer active hbeat-ack
             end
```

NOTES:

- **no** : Removes peer active heart beat acknowledgment.
- **sctp-peer active hbeat-ack**: Configures SCTP peer active heartbeat acknowledgment.



CHAPTER 20

Support for DH group 5 Encryption under IKE and IPSEC Transform Set

Feature Summary and Revision History

Summary Data

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

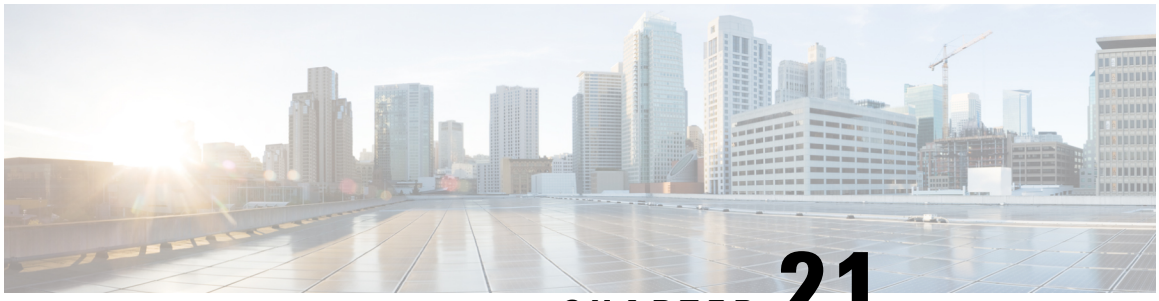
Revision History

Revision Details	**Release**
First introduced.	21.17.12

Feature Changes

In earlier StarOS releases to be in compliant with network security, DH group 5 algorithm was identified as deprecated one and removed for trusted builds from 21.12.x onwards. In the StarOS 21.17.12 release, to

support VoWiFi services for IPhone subscribers, ePDG supports DH group 5 algorithm for trusted builds and this DH group 5 algorithm can be configured under both IKE and IPSEC transform set.



CHAPTER 21

UEM Interworking with Generic VNFM

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UEM
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required
Related Changes in This Release	Not applicable
Related Documentation	• *UEM-based VNF Deployment Guide*

Revision History

Revision Details	Release
With this release, the support is extended to certain VNF Performance Management functions.	6.11
First introduced (Supported only VNF Lifecycle Management functions)	6.8

Feature Changes

The UEM supports the Ve-Vnfm interface as per the ETSI-NFV-SOL002 specification, version 2.3.1.

Important In this case, it is assumed that the VNFM is from a third-party vendor.

Earlier, the Ve-VNFM interface for SOL002 was supported for VNF Lifecycle Management and Performance Management functions. As part of the lifecycle management functions, VNF Instantiation, VNF Termination, Notification Subscription, Notification Handling, and Authentication procedures were supported.

This release supports certains VNF Performance Management functions, that is, Create, Get, and Delete Performance Management (PM) operations for PM jobs and reports.