Release Change Reference, StarOS Release 21.12/Ultra Services Platform Release 6.6

First Published: 2019-02-14

Last Modified: 2020-07-14

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

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

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

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

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

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

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

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

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

CHAPTER 1

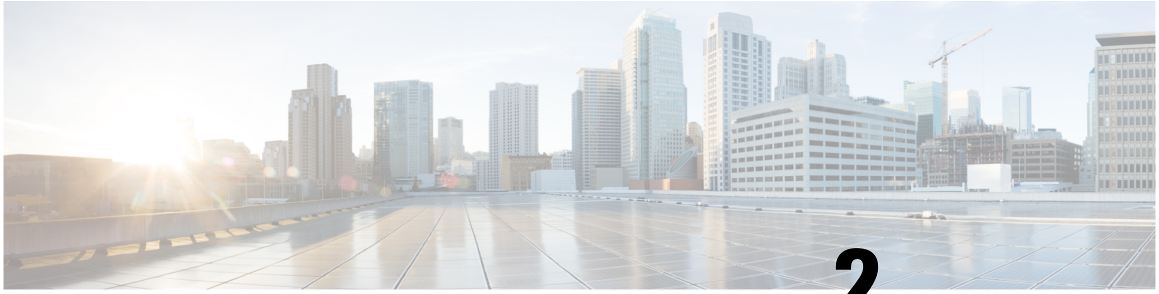
Release 21.12/6.6 Features and Changes Quick Reference

Release 21.12/6.6 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
5G Capable SPGW Selection by MME, on page 17	MME	21.12.2
Access Restriction Support on S6d Interface, on page 23	SGSN	21.12
Cell Broadcast Center - SBc Interface, on page 25	MME	21.12
Collision Handling for Path Update during Bearer Creation, on page 33	MME	21.12.15
Configuring UE Radio Capability IE Size, on page 35	MME	21.12.15
Counters for Reason 50/51 on MME and TAI Level, on page 37	MME	21.12
Delay Value IE Support in MME, on page 43	MME	21.12.2
Deprecated IPSec/IKEv2 Algorithms Support, on page 45	All	21.12
Deprecation of Manual Scaling, on page 49	UAS	6.0
Discontinuation of ORBEM Configuration Support, on page 51	All	21.16
ERAB Setup Retry Handling, on page 59	MME	21.12.15

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
ESC, UEM and VNF Upgrade Support on VMware VCD, on page 53	UEM	6.6
Excluding SGWs During Relocation Procedures, on page 55	MME	21.12.2
Handling of APN Configuration in ISDR from HSS, on page 63	MME	21.12.15
Handling Temporary Failure During UBR-MBC Collision, on page 65	S-GW	21.12.15
Handling the TAU and Location update Request/Response , on page 69	MME	12.12.2
IPv6 MTU Option Support in RA Message Enhancement, on page 71	P-GW	21.12.18
GB Manager Queue Handling, on page 57	SGSN	21.12.13
Mapped-UE-Usage-Type IE Support in MME, on page 73	MME	21.12.2
MEC Location Management, on page 75	MME	21.12.2
MME Handling of Purge Procedure, on page 83	MME	21.12.15
MME-MSC/VLR SGs Disconnect, on page 85	MME	21.12.12
MME Manager Status Traps, on page 87	MME	21.12.12
MME Support for Service Impacting KPI Bulk Statistics, on page 91	MME	21.12.12
Monitor Protocol Support for DCNR, on page 95	MME	21.12.11
NB-IOT EDRX Supported values in ATTACH/TAU Accept, on page 97	MME	21.12.11
NETCONF Event Notification Support for Auto-scaleout, on page 99	UEM	6.6
Network Access Identifier Field Removal from MSISDN, on page 101	P-GW	21.12.12
NFVO-based Deployment of UGP VNF, on page 103	UEM	6.6
OWM Integra Deployment Automation on VMware VCD, on page 105	OWM (3rd party)	6.6

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Paging eDRX H-SFN Changed to 10 Bits Counter, on page 107	MME	21.12.5
RAB Release for Attach on the Same IU Connection, on page 109	SGSN	21.12
Service Impacting SGSN KPI Bulk Statistics, on page 113	SGSN	21.12.12
SRVCC Delete Bearer Request Handling, on page 115	MME	21.12.9
SRVCC HO Timer Configuration for ESM Notification, on page 117	MME	21.12.12
Support for Password Expiry Warning, on page 119	All	21.12
Target MME Load Balancing During Handover, on page 121	MME	21.12.2
Upgrade and Migration of Open SSH to Cisco SSH, on page 123	All	21.16



CHAPTER 2

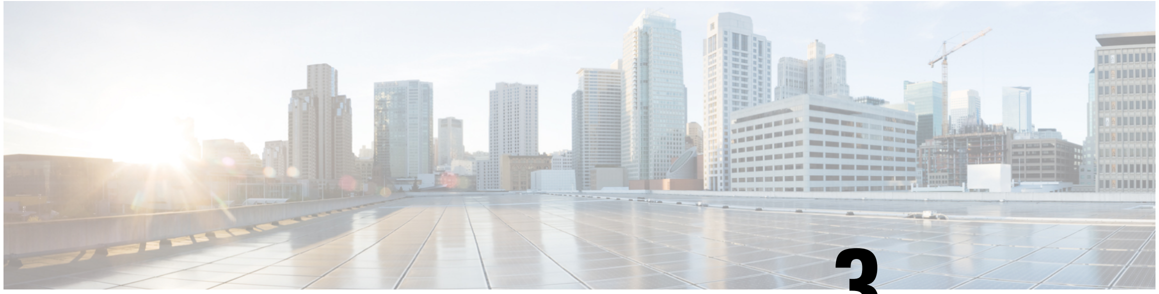
Feature Defaults Quick Reference

Feature Defaults Quick Reference

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

Feature	Default
5G capable SPGW Selection by MME	Enabled - Always-on
Access Restriction Support on S6d Interface	Disabled - Configuration Required
Cell Broadcast Center - SBc Interface	Enabled - Configuration Required
Collision Handling for Path-Update during Bearer Creation	Enabled - Always-on
Configuration of UE Radio Capability IE Size	Enabled - Configuration Required
Counters for Reason 50/51 on MME and TAI	Enabled - Always-on
Deprecated IPSec/IKEv2 Algorithms Support	Enabled - Always-on
Deprecation of Manual Scaling	Disabled - Configuration Required
Delay Value IE Support in MME	Enabled - Configuration Required
Discontinuation of ORBEM Configuration Support	Enabled - Always-on
ERAB Setup Retry Handling	Disabled - Configuration Required
ESC, UEM and VNF Upgrade Support on VMware VCD	Disabled - Configuration required
Excluding SGWs During Relocation Procedures	Enabled - Always-on
GM Manager Queue Handling	Disabled – Configuration Required
Handling of APN Configuration in ISDR from HSS	Enabled – Always-on
Handling Temporary Failure During UBR-MBC Collision	Disabled-Configuration Required

Feature	Default
Handling the TAU and Location Update Request/Response	Enabled - Always-on
IPv6 MTU Option Support in RA Message Enhancement	Enabled - Always-on
Mapped-UE-Usage-Type IE Support in MME	Disabled - Configuration Required
MEC Location Management Support	Enabled - Always-on
MME Handling of Purge Procedure	Enabled - Configuration Required
MME-MSC/VLR SGs Disconnect	Enabled – Configuration Required
MME Manager Status Traps	Enabled - Always-on
MME Support for Service Impacting KPI Bulk Statistics	Enabled - Always-on
Monitor Protocol Support for DCNR	Enabled - Always-on
NB-IOT EDRX Supported values in ATTACH/TAU Accept	Enabled - Configuration Required
NETCONF Event Notification Support for Auto-scaleout	Disabled – Configuration Required **Note** This feature is dependent on the existing Automatic Scale-out feature.
Network Access Identifier Field Removal from MSISDN	Enabled - Always-on
NFVO-based Deployment of UGP VNF	Disabled - Configuration required
OWM Integra Deployment Automation on VMware VCD	Disabled - Configuration required
Paging eDRX H-SFN Changed to 10 Bits Counter	This feature is enabled/disabled, when the eDRX feature is enabled/disabled.
RAB Release for Attach on the Same IU Connection	Disabled - Configuration Required
Service Impacting SGSN KPI Bulk Statistics	Enabled - Always-on
SRVCC Delete Bearer Request Handling	Disabled – Configuration Required
SRVCC HO Timer Configuration for ESM Notification	Enabled – Configuration Required
Support for Password ExpiryWarning	Enabled - Always-on
Target MME Load Balancing During Handover in MME	Enabled - Always-on



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.12 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 21.12 include:

- New Bulk Statistics, on page 7
- Modified Bulk Statistics, on page 8
- Deprecated Bulk Statistics, on page 9

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.12.

MME Schema

The following bulk statistics are added in the MME schema in support Counters for the reason 50/51 on MME and TAU feature.

Bulk Statistics	Description
esm-msgtx-pdncon-rej-pdn-type_ipv4_only	The name of the paging profile.
esm-msgtx-pdncon-rej-pdn-type_ipv6_only	The total number of PDN connections rejected with cause 50 under MME level.
signalling-pdn-reconn-paging-init-events-attempted	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were attempted.
signalling-pdn-reconn-paging-init-events-success	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were successful.
signalling-pdn-reconn-paging-init-events-failures	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that failed.

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

TAI Schema

The following bulk statistics are added in the TAI schema in support Counters for the reason 50/51 on MME and TAU feature.

Bulk Statistics	Description
tai-esm-msgtx-pdncon-rej-pdn-type_ipv4_only	The total number of PDN connections rejected with cause 50 under TAI level.
tai-esm-msgtx-pdncon-rej-pdn-type_ipv6_only	The total number of PDN connections rejected with cause 51 under TAI level.
tai-signalling-pdn-reconn-paging-init-events-attempted	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were attempted.
tai-signalling-pdn-reconn-paging-init-events-success	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that were successful.
tai-signalling-pdn-reconn-paging-init-events-failures	The total number of ECM Statistics-related Paging requests to UE, to reconnect PDN, that failed.
tai-signalling-pdn-reconn-paging-last-enb-success	The total number ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known eNodeB.
tai-signalling-pdn-reconn-paging-last-tai-success	The total number ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at the last known Tracking Area Identifier
tai-signalling-pdn-reconn-paging-tai-list-success	The total number of ECM Statistics-related Paging requests to UE to reconnect PDN that succeeded at an eNodeB in all TAIs present in the TAI list assigned to the UE.

Modified Bulk Statistics

This section identifies bulk statistics that have been modified in release 21.12.

None in this release.

Deprecated Bulk Statistics

This section identifies bulk statistics that are no longer supported in release 21.12.

None in this release.

CHAPTER 4

SNMP MIB Changes in StarOS 21.12 and USP 6.6

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.12 and Ultra Services Platform (USP) 6.6 software releases.

SNMP MIB Object Changes for 21.12

This section provides information on SNMP MIB alarm changes in release 21.12.

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 21.12.

The following alarms are new in this release:

- starSxCPUPGroupName

Modified SNMP MIB Object

This section identifies SNMP MIB alarms modified in release 21.12.

The following alarms have been modified in this release:

- starSxFailureCause
- starSxPeerAssociated
- starSxPeerAssociationRelease

Deprecated SNMP MIB Object

This section identifies SNMP MIB alarms that are no longer supported in release 21.12.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Alarm Changes for 21.12

This section provides information on SNMP MIB alarm changes in release 21.12.

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 21.12.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 21.12.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 21.12.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Conformance Changes for 21.12

This section provides information on SNMP MIB alarm changes in release 21.12.

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

New SNMP MIB Conformance

This section identifies new SNMP MIB alarms available in release 21.12.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Conformance

This section identifies SNMP MIB alarms modified in release 21.12.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Conformance

This section identifies SNMP MIB alarms that are no longer supported in release 21.12.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Object Changes for 6.6

This section provides information on SNMP MIB object changes in the Ultra M MIB corresponding to release 6.6.

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

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 6.6.

The following objects are new in this release:

- None in this release.

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 6.6.

The following objects have been modified in this release:

- None in this release.

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 6.6.

The following objects have been deprecated in this release:

- None in this release.

SNMP MIB Alarm Changes for 6.6

This section provides information on SNMP MIB alarm changes in the Ultra M MIB corresponding to release 6.6.

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 6.6.

The following alarms are new in this release:

- None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 6.6.

The following alarms have been modified in this release:

- None in this release.

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 6.6.

The following alarms have been deprecated in this release:

- None in this release.

SNMP MIB Conformance Changes for 6.6

This section provides information on SNMP MIB conformance statement changes in the Ultra M MIB corresponding to release 6.6.

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

New SNMP MIB Conformance Statements

This section identifies new SNMP MIB conformance statements available in release 6.6.

The following conformance statements are new in this release:

- None in this release.

Modified SNMP MIB Conformance Statements

This section identifies SNMP MIB conformance statements that are modified in release 6.6.

The following conformance statements have been modified in this release:

- None in this release.

Deprecated SNMP MIB Conformance Statements

This section identifies SNMP MIB conformance statements that are no longer supported in release 6.6.

The following conformance statements have been deprecated in this release:

- None in this release.

CHAPTER 5

5G Capable SPGW Selection by MME

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.12.2

Feature Description

With this release, MME is enabled to select 5G capable and co-located SPGW during initial attach, and additional PDN and SGW relocation scenarios. When multiple entries are configured, selection of a candidate is based on weight.

Configuring 5G Capable SPGW Selection by MME

This section provides information on the CLI commands to configure 5G capable SPGW selection by MME.

collocated-node, ue-usage-type in apn-profile mode

Use the following configuration to configure co-located-node/ue-usage-type for SPGW selection at MME.

```
configure
       apn-profile apn_profile_name
         pgw-address ip_address  [ co-located-node  collocated_node_name  [
primary | secondary | weight  value  ] | [ ue-usage-type  ue_usage_type_value
  [ collocated-node | primary | secondary | weight value  ] ]
         no pgw-address [ collocated-node  collocated_node_name  ] [
ue-usage-type  ue_usage_type_value  collocated-node collocated_node_name  ]
         end
```

NOTES:

- **no**: Disables the following options.
- **collocated-node** *collocated_node_name*: Configures the collocation name to select the co-located SPGW node IP addresses for MME. *collocated_node_name* must be string of size 1 to 255.
- **ue-usage-type** *ue_usage_type_value*: Configures the ue-usage for the gateway. *ue_usage_type_value* must be an integer between 1 and 255.
- **weight** *value*: Enter a weight for this address.*value* must be an integer from 1 and 100.

collocated-node, ue-usage-type in mme-service mode

Use the following configuration to configure collocated-node/ue-usage-type for SPGW selection at MME.

```
configure
   context context_name
          mme-service mme_service_name
            pgw-address ip_address  [ collocated-node  collocated_node_name [
weight  value  ] ] | [ ue-usage-type  ue_usage_type_value  [ collocated-node |
 weight value  ] ]
            no pgw-address [ collocated-node  collocated_node_name  ] [
ue-usage-type  ue_usage_type_value  collocated-node collocated_node_name  ]
            end
```

NOTES:

- **no**: Disables the following options.
- **collocated-node** *collocated_node_name*: Configures the collocation name to select the collocated S/PGW node IP addresses for MME. *collocated_node_name* must be a string of size 1 to 255.
- **ue-usage-type** *ue_usage_type_value*: Configures the ue-usage for the gateway. *ue_usage_type_value* must be an integer between 1 through 255.
- **weight** *value*: Enter a weight for this address.*value* must be an integer from 1 through 100.

collocated-node, ue-usage-type in lte-emergency-profile mode

Use the following configuration to configure collocated-node/ue-usage-type for SPGW selection at MME.

```
configure
       lte-policy
         lte-emergency-profile lte_emergency_profile_name
           pgw-address ip-address ip_address  protocol { both | gtp | pmip
 }   weight value  [ collocated-node collocated_node_name ] | [ ue-usage-type
  ue_usage_type_value  [ collocated-node collocated_node_name  ] ]
            no pgw-address ip-address ip_address [ collocated-node
collocated_node_name  ] [ ue-usage-type  ue_usage_type_value  collocated-node
collocated_node_name  ]
            end
```

NOTES:

- **no**: Disables the following options.
- **collocated-node** *collocated_node_name*: Configures the collocation name to select the collocated SPGW node IP addresses for MME. *collocated_node_name* must be an alphanumeric string of 1 through 255.
- **ue-usage-type** *ue_usage_type_value*: Configures the ue-usage for the gateway. *ue_usage_type_value* must be an integer between 1 and 255.
- **weight** *value*: Specifies the weight used for pgw selection.*value* must be an integer from 1 and 100.

collocated-node, ue-usage-type in tai-mgmt-obj mode

Use the following configuration to configure collocated-node/ue-usage-type for SPGW selection at MME.

```
configure
       lte-policy
         tai-mgmt-db tai_mgmt_db_name
            tai-mgmt-obj tai_mgmt_obj_name
              sgw-address ip_address  s5-s8-protocol { both | gtp | pmip }
 weight  value  [ attach-only | collocated-node  collocated_node_name  [
attach-only ]   ] | [ ue-usage-type  ue_usage_type_value  [ collocated-node
  collocated_node_name [ attach-only ] ] ]
             no sgw-address ip_address  s5-s8-protocol { both | gtp | pmip
 } [ collocated-node  collocated_node_name  ] [ ue-usage-type  ue_usage_type_value
  collocated-node collocated_node_name  ]
              end
```

NOTES:

- **no**: Disables the following options.
- **attach-only** : Specifies the SGW preference for SGW-relocation.
- **collocated-node** *collocated_node_name*: Configures the collocated node name to select the collocated S/PGW node IP addresses. *collocated_node_name*must be an alphanumeric string of 1 through 255.
- **ue-usage-type** *ue_usage_type_value*: Specifies the S-GW supported ue-usage-type. *ue_usage_type_value* must be an integer between 1 and 255.
- **weight** *value*: Specifies the protocol supported by the SGW (GTP, PMIP or both). *value* must be an integer from 1 and 100.

Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the 5G Capable SPGW Selection by MME feature.

Show Commands and Outputs

show mme-service name

The output of this command includes the following fields:

- ue_usage_type
- collocated_node

Important "ue_usage_type" and "collocated_node" appears more than once based on number no of P-GW addresses configured.

show lte-policy tai-mgmt-db name

The output of this command includes the following fields:

- ue-usage-type
- collocated-node

Important "ue_usage_type" and "collocated_node" appears more than once based on number no of S-GW addresses configured.

show apn-profile full name

The output of this command includes the following fields:

- ue-usage-type
- collocated-node

Important "ue_usage_type" and "collocated_node" appears more than once based on number no of P-GW addresses configured.

show lte-policy lte-emergency-profile name

The output of this command includes the following fields:

- ue-usage-type
- collocated-node

Important "ue_usage_type" and "collocated_node" appears more than once based on number no of P-GW addresses configured.

CHAPTER 6

Access Restriction Support on S6d Interface

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	SGSN Administration Guide

Revision History

Revision Details	Release
First introduced.	21.12

Feature Changes

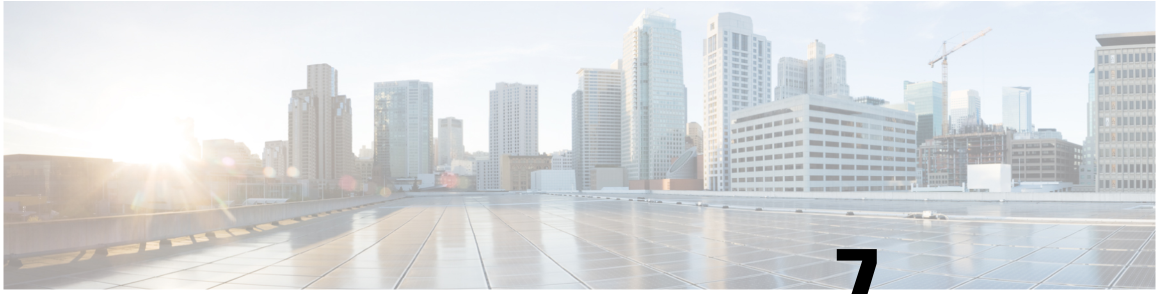
The SGSN supports the below parameters added in the Update Location Request/Answer and Insert Subscriber Data Request/Answer messages on S6d interface:

- SGSN advertises the DCNR feature support by setting the 'NR as Secondary RAT feature bit' in Supported Features list 2 towards HSS if the DCNR feature is configured at SGSN and UE advertises DCNR capability in NAS
- SGSN also handles the new bit 'NR as Secondary RAT Not Allowed' in the Access-Restriction-Data bitmask sent by HSS to control if the subscriber is allowed to access NR via dual connectivity
- SGSN handles the Extended Bandwidth UL/DL parameters under AMBR sent by HSS

Gateway selection is improved to avoid SGSN from falling back and triggering an "A" query to get the normal GGSN information.

Previous Behavior: The SGSN sends a SNAPTR query for gateway resolution and selection when DCNR feature is enabled. If the SGSN does not find a collocated PGW/GGSN with “+nc-nr” capability in DNS response(x-3gpp-pgw:x-gn+nc-nr/ x-3gpp-pgw:x-gp+nc-nr), the SGSN will fall back and triggers a "A" query to get the normal GGSN information.

New Behavior: When no collocated PGW/GGSN with "+nc-nr" capability is found in DNS response, the SGSN will select the next collocated PGW/GGSN node. If “3gpp-pgw:x-gn+nc-nr/ x-3gpp-pgw:x-gp+nc-nr” is not present in DNS response, the SGSN will select “3gpp-pgw:x-gn / x-3gpp-pgw:x-gp” instead of triggering another to "A" query to get the GGSN information. "UP Function Selection Indication Flags" IE in Create PDP Context Request message will be set to "1" only when “+nc-nr” capable gateway is selected.



CHAPTER 7

Cell Broadcast Center - SBc Interface

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

Revision History

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

Revision Details	Release
Enhancement to SBc and S1-AP interfaces	21.12
First introduced	Pre 19.0

Feature Description

The MME uses the SBc interface, between the MME and the Cell Broadcast Center (CBC), for warning message delivery and control functions.

The MME provides support for Commercial Mobile Alert System (CMAS) — SBc interface and underlying protocols. Warning Messages can be received from a CBC over the SBc-AP interface and relayed to all relevant eNodeBs over the S1-AP interface.

The CMAS functionality is enabled in the networks to provide warning notifications to subscribers.

Important From release 18.4 onwards, a valid license key is required to enable the SBc interface. Contact your Cisco account representative for information on how to obtain a license.

How It Works

The MME accepts incoming SBc associations coming from multiple CBCs.

The MME is responsible for the delivery of the Warning Messages received from CBC to all relevant eNodeBs serving the given TAI list. In the absence of TAI list in the received Warning Message, MME sends the Warning Message to all connected eNodeBs.

The MME acknowledges to CBC when it has started distributing the Warning Message to all relevant eNodeBs. If a response is not received from any eNodeB, it shall not result in any exclusive error messaging to CBC.

Even if the MME node is experiencing congestion, Warning Messages are forwarded and not dropped.

When connected to multiple CBCs, the uniqueness of Warning Messages as identified by Message Type, Message Identifier and Serial Number, must be ensured across these CBCs.

DSCP Marking for SBc Interface

SBc services support the Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SBc interface.

Either the predefined DSCP values can be used for marking or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

```
config
   context context_name
      sbc-service service_name
```

```
[ no ] ip qos-dscp dscp_value
end
```

NOTES:

- **ip**: Defines the Internet Protocol parameters for the packets leaving through the SBc interface.
- **qos-dscp**: Designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SBc interface.
- *dscp_value*: Value assigned to the packet for DSCP marking. The value can be a predefined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

Warning Message Call Flows

In compliance with 3GPP TS 29.168 v15.1.0, the MME supports the following procedures:

- Write-Replace Warning Procedure
- Stop Warning Procedure
- Error Indication Procedure
- Write-Replace Warning Indication Procedure
- Stop Warning Indication Procedure

Limitations

This section describes the known limitations for the Cell Broadcast Center feature:

- The size of the SBc message supported by MME is a maximum of 50K bytes. If MME receives the WRITE-REPLACE WARNING REQUEST over 50K bytes, the message cannot be processed and a warning syslog is generated.

Standards Compliance

The Cell Broadcast Center feature complies with the following standards:

- 3GPP TS 22.268 v10.4.0: Public Warning System
- 3GPP TS 23.041 v10.6.0: Technical realization of Cell Broadcast Service (CBS)
- 3GPP TS 29.168 v15.1.0: Cell Broadcast Centre Interfaces with the Evolved Packet Core
- 3GPP TS 36.413 v15.3.0: S1-AP Interface

Configuring SBc Interface

This section describes how to configure the SBc interface on MME.

Creating and Configuring SBc Service

An SBc service must be created within a context to configure the SBc-AP interface to accept connections from one or more CBCs.

Important From release 18.4 onwards, a valid license key is required to access the commands used to configure and manage the SBc interface. Contact your Cisco account representative for license information.

Use the following configuration to create and configure the SBc service.

```
configure
   context ctxt_name
      sbc-service sbc_svc_name
         associate sctp-param-template sctp_param_template_name
        bind ipv4/v6-address ipv4/v6_address_value1 ipv4-address ipv4_address_value2

         cbc-associations maximum number
         sbc-mme sctp port port_num
         end
```

NOTES:

- Up to 8 SGs + MME + SBc + SLs services can be configured on the system. The SBc service name must be unique across all contexts.
- Associating the SBc service to the SCTP parameter template is not required for the SBc service to be operational. However, if a template is associated, the template must exist before the SBc service is associated to it.
- The SBc service must be bound to at least 1 IP address. Up to 2 IPv4 or 2 IPv6 addresses can be specified for multihoming purposes.
- The **cbc-associations** command is used to define the maximum number of CBC connections allowed for this SBc service. The default setting is 1. Up to 2 connections are allowed per SBc service.
- The default SCTP port used is 29168. The MME listens for incoming SBc-AP connections from an CBC on this port.

Associating the SBc Service with the MME Service

Use the following configuration to associate the SBc service to an MME service.

```
configure
   context ctxt_name
      mme-service mme_svc_name
         associate sbc-service sbc_svc_name [ context ctxt_name ]
         end
```

NOTES:

- Each MME service can be associated with one unique SBc service.

- The SBc service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.
- The MME will always check for a valid SBc service that is up and connected to a CBC before performing any meaningful operations on the Warning Messages received on the S1-AP interface (like attempting to forward the messages).
- Use the optional **context** keyword if the SBc service and MME service are configured in separate contexts.
- The SBc service is not operationally STARTED unless the MME service to which it is associated is in a STARTED state.

Configuring ENB Response Aggregate Timer

Use the following configuration timeout values for aggregating responses received from eNB at MME.

```
config
   context context_name
         sbc-service service_name
           enb-response-aggr-timer timeout_value
          [ default ] enb-response-aggr-timer
          end
```

- **enb-response-aggr-timer** *timeout_value*: Configures the timeout value in seconds for aggregating responses received from eNB at MME.
- *timeout_value* : must be an integer between 4 and 120.
- **default** : Sets the default timeout value for aggregating responses received from eNB at MME. Default value is 10 seconds.

Configuring Send Warning Indication

Use the following configuration to enable or disable the warning indication messages towards CBC from MME.

```
config
   context context_name
         sbc-service service_name
           [ no | default ] send stop-warning-ind
           [ no | default ] send write-replace-warning-ind
          end
```

- **send stop-warning-ind** : Enables the stop warning indication messages towards CBC from MME.
- **send write-replace-warning-ind** : Enables the write-replace-warning indication messages towards CBC from MME.
- **no**: Removes the configuration of sending the warning indication [stop warning / write replace warning] messages towards CBC from MME.
- **default** : Sets the default configuration of sending the warning indication [stop warning / write replace warning] messages towards CBC from MME. By default sending of warning indication messages are disabled.

Verifying the SBc Service Configuration

The following command displays configuration information for all SBc services, for the specified for the specified SBc service, or for the specified Cell Broadcast Center.

```
show sbc-service { all | cbc-associations { all | sbc-service-name
sbc_svc_name [ path-info | summary ] } | sbc-service-name sbc_svc_name }
```

The following command displays the SBc Service name and SBc Service Context which has been associated with each MME service.

```
show mme-service all
```

The following command displays configuration errors and warnings related to all SBc services on the MME:

```
show configuration errors section sbc-service verbose
```

Monitoring SBc Services

This section lists the SNMP traps, bulk statistics, and show commands that display operational statistics relating to SBc services.

SNMP Traps

The following traps are available to track status and conditions relating to the SBc service.

- **starSBCServiceStart**: An SBc Service has started.
- **starSBCServiceStop**: An SBc Service has stopped.

The following traps are generated to track status and conditions of individual CBC associations.

- **starCBCAssocDown**: A CBC Association is down.
- **starCBCAssocUp**: A CBC Association is up.

SBc Bulk Statistics

SBc service related bulk statistics are provided within the **SBc** schema.

Use the following command to display a list of all variables available within this schema:

```
show bulkstats variables sbc
```

For more information about these statistics, refer to the **SBc Schema** chapter of the *Statistics and Counters Reference*.

SBc Service Show Commands and Outputs

show sbc statistics

The following command displays all statistics related to the SBc service. These statistics can be filtered based on CBC association (peer-id) or SBc service name.

```
show sbc statistics { all | peer-id peer_id | sbc-service-name sbc_svc_name
}
```

show mme-service statistics s1ap

The following command displays S1-AP statistics related to the SBc interface. See the lines for Kill Request and Kill Response in the example below:

```
S1AP Statistics:
   Transmitted S1AP Data:

       Kill Request: 0    Write-Replace Warning Request: 0
   Received S1AP Data:

       Kill Response: 0   Write-Replace Warning Response: 0
```

Event Logging

Event logging for the SBc interface can be enabled using the following command:

```
logging filter active facility sbc level severity_level
```

See the *System Logs* chapter of the *System Administration Guide* for more information about event logging.

CHAPTER 8

Collision Handling for Path Update during Bearer Creation

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

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

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

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

CHAPTER 9

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
Increase to UE Radio Capability IE Size from 3072 to 9000.	21.20.3
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.

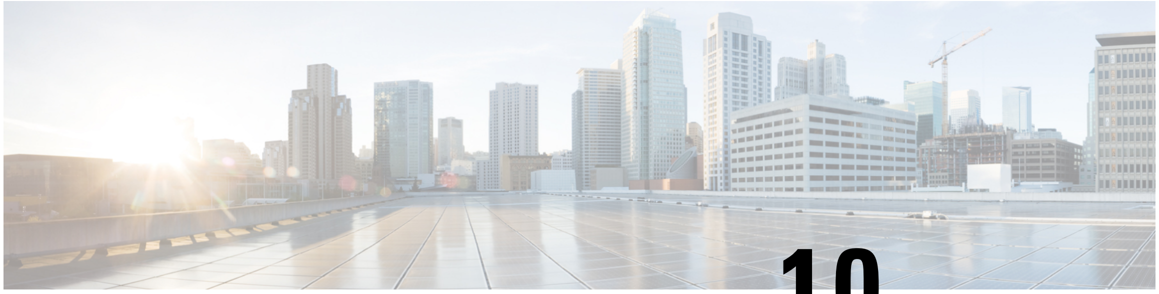
Configuring the UE Radio Capability IE

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 10

Counters for Reason 50/51 on MME and TAI Level

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.12

Feature Description

With this release new counters are introduced for the NAS-ESM message "PDN_CONNECTIVITY_REJECT" with cause code "PDN TYPE IPV4 ONLY ALLOWED (50)" and "PDN TYPE IPV6 ONLY ALLOWED (51)".

Important Previously these causes were populated in other reasons counter, same behavior holds good ever.

Show Commands and Outputs

show mme-service statistics esm-only

The output of this command includes the following fields:

- PDN type IPv4 only
- PDN type IPv6 only

show mme-service statistics tai taidb <> mcc <> mnc <> tac <>

The output of this command includes the following fields:

- PDN type IPv4 only
- PDN type IPv6 only

Bulk Statistics

This section provides information on the bulk statistics for the reason 50/51 on MME and TAU.

MME Schema

The following counters for reason 50/51 related bulk statistics are available in the MME schema.

Bulk Statistics	Description
esm-msgtx-pdncon-rej-pdn-type_ipv4_**only**	The total number of PDN connections rejected with cause 50 under MME level.
esm-msgtx-pdncon-rej-pdn-type_ipv6_**only**	The total number of PDN connections rejected with cause 51 under MME level.

TAI Schema

The following counters for reason 50/51 related bulk statistics are available in the TAI schema.

Bulk Statistics	Description
tai-esm-msgtx-pdncon-rej-pdn-type_ipv4_only	The total number of PDN connections rejected with cause 50 under TAI level.
tai-esm-msgtx-pdncon-rej-pdn-type_ipv6_only	The total number of PDN connections rejected with cause 51 under TAI level.

CHAPTER 11

Debug Console Swap

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

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

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

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

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

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

Customer Impact:

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

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

Command Changes

logging

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

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

NOTES:

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

CHAPTER 12

Delay Value IE Support in MME

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
MME sends configured delay value as “Data Notification Delay" in DDN-ACK and "Delay Downlink Packet Notification Request" IE in Modify-Bearer-Request to SGW.	21.12.2
First introduced.	Pre 21.9

Feature Changes

Previous Behavior: MME does not support sending of delay value IE in Modify Bearer Request and DDN Ack messages towards SGW.

New Behavior: MME sends configured delay value as “Data Notification Delay" in DDN-ACK and "Delay Downlink Packet Notification Request" IE in Modify-Bearer-Request to SGW. When delay value is not configured, this IE will not be included in DDN-ACK and Modify bearer request messages.

Command Changes

This section provides information on the CLI commands to configure Delay Value IE Support in MME.

ddn-delay

Use the following configuration to configure ddn-delay value.

```
configure
   context  context_name
      mme-service mme-service_name
         ddn-delay ddn-delay_value
         no ddn-delay
         end
```

NOTES:

- **no**: Removes the configured downlink-data-notification delay value.
- **ddn-delay** Configures the downlink-data-notification delay value in multiples of 50 milliseconds. *ddn-delay_value* is an integer and it must be between 0 and 255.

Performance Indicator Changes

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

Show Commands and Outputs

show mme-service all

The output of this command includes "DDN Delay Value".

CHAPTER 13

Deprecated IPSec/IKEv2 Algorithms Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All products using IKEv2 for IPsec
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	• Command Line Interface Reference • ePDG Administration Guide

Revision History

Revision Details	Release
First introduced.	21.12

Feature Changes

Deprecated algorithms supported removed under IPSec/IKEv2 transform set.

Previous Behavior: Following algorithms are supported under IPSec/IKEv2 transform set:

- AES-GCM-128 and 64 bit ICV
- AES-GCM-128 and 96 bit ICV
- DH Group 5

New Behavior: Following algorithms supported is removed under IPSec/IKEv2 transform set as they are deprecated:

- AES-GCM-128 and 64 bit ICV
- AES-GCM-128 and 96 bit ICV
- DH Group 5

Important Algorithms support changes are applicable only to the trusted builds.

The following security supplement certificates signing schema are deprecated for the trusted builds:

- MD2WithRSAEncryption
- MD4WithRSAEncryption
- MD5WithRSAEncryption
- RIPEMD128WithRSAEncryption
- RIPEMD160WithRSAEncryption
- RIPEMD256WithRSAEncryption

Command Changes

This section describes the CLI configuration required to configure Certificate Key Size.

crypto template min-key-size

Use the following configuration to set minimum key size.

```
configure
   context context_name
      crypto template crypto_template_name ikev2-dynamic
      authentication min-key-size min_key_size
      [ default | no ] authentication min-key-size
      end
```

NOTES:

- **authentication min-key-size** *min_key_size*: Sets minimum certificate key size, *min_key_size* must be an integer between 255 to 8192.
- **default**: Sets default key size. Default is 255

- **no**: Disables minimum key size validation feature.

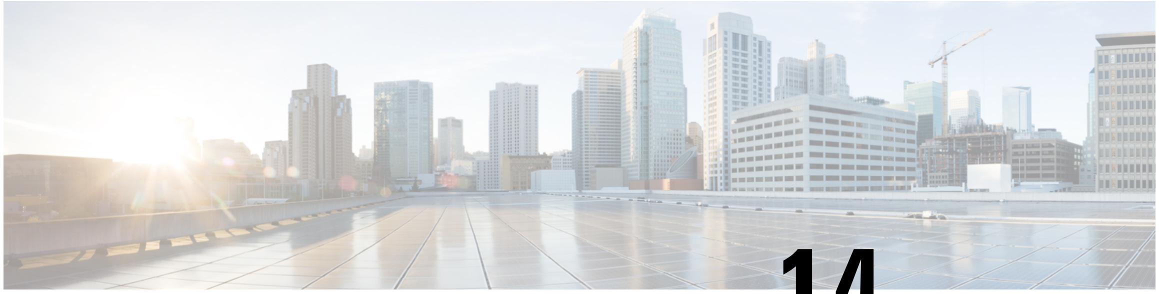
crypto map min-key-size

Use the following configuration to set minimum key size.

```
configure
   context context_name
      crypto map crypto_map_name [ikev2-ipv4 | ikev2-ipv6 ]
      authentication min-key-size min_key_size
      [ default | no ] authentication min-key-size
      end
```

NOTES:

- **authentication min-key-size** *min_key_size*: Sets minimum certificate key size, *min_key_size* must be an integer between 255 to 8192.
- **default**: Sets default key size. Default is 255
- **no**: Disables minimum key size validation feature.



CHAPTER 14

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 15

Discontinuation of ORBEM Configuration Support

Feature Summary and Revision History

Summary Data

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

Revision History

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

Revision Details	Release
With this release onwards, the **orbem** CLI command is discontinued and no longer recommended for use.	21.16
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: In releases earlier to 21.16, the **orbem** CLI command was supported.

New Behavior: With Release 21.16 onwards, the **force** keyword has to be appended to the **orbem** CLI command to enter the ORBEM mode and enable the feature. The **orbem** keyword is now hidden.

Note Support for the end-of-life ORBEM/WEM feature will be fully discontinued in future releases.

CHAPTER 16

ESC, UEM and VNF Upgrade Support on VMware VCD

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	6.6

Feature Changes

ESC, UEM and VPC VNF upgrade support on VMware VCD server is available in this release. For detailed instructions on upgrading these components, see the *VMware VCD VNF Deployment Guide*.

CHAPTER 17

Excluding SGWs During Relocation Procedures

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.12.2

Feature Description

With this release, MME is enabled to exclude SGW during SGW relocation procedures. When an entry is configured with exclude option it will not be considered as a target candidate for SGW relocation procedures.

Configuration to Exclude SGWs During Relocation Procedures

This section provides information on the CLI commands to exclude SGWs during relocation procedures in the MME.

attach-only

Use the following configuration to exclude the SGWs during relocation procedures.

```
configure
   lte-policy
      tai-mgmt-db tai_mgmt_db_name
         tai-mgmt-obj tai_mgmt_obj_name
             sgw-address  ipv4_or_ipv6_address  s5-s8-protocol { both | gtp |
pmip } weight weight attach-only
            end
```

NOTES:

attach-only: Specifies the SGW preference for SGW-relocation.

Monitoring and Troubleshooting

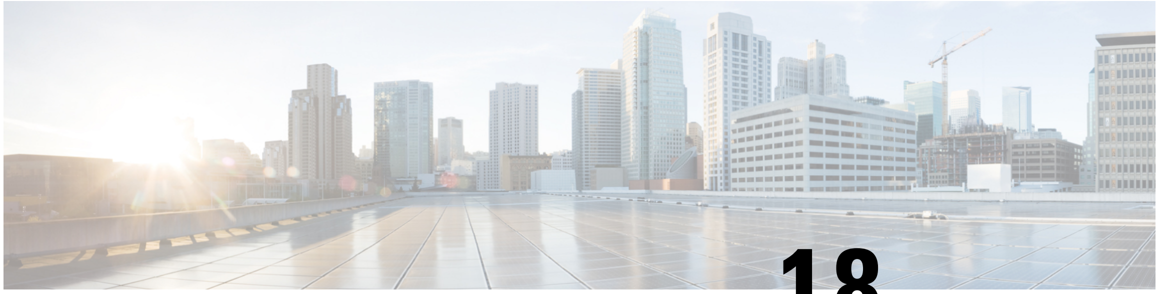
This section provides information regarding show commands available to monitor and troubleshoot this feature.

Show Commands and Outputs

show lte-policy tai-mgmt-db name

The output of this command includes "attach-only".

Note Show output "attach-only" appears more than once based on the number of times it is configured.



CHAPTER 18

GB Manager Queue Handling

Feature Summary and Revision History

Summary Data

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

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

Feature Description

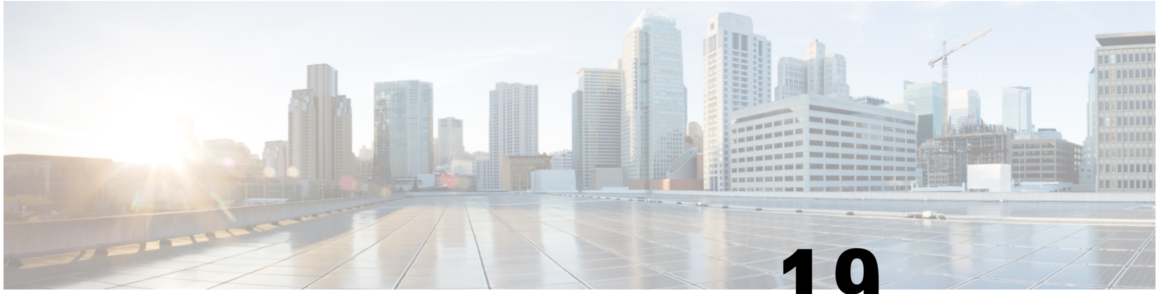
Important This feature is customer-specific.

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

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

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

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



CHAPTER 19

ERAB Setup Retry Handling

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

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

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

Feature Changes

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

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

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

Command Changes

erab-setup-rsp-fail retry-timer

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

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

NOTES:

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

Performance Indicator Changes

show mme-service name <mme_svc_name>

The output of this command includes the following fields:

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

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

show mme-service name <mme_svc_name>

CHAPTER 20

Handling of APN Configuration in ISDR from HSS

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

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

CHAPTER 21

Handling Temporary Failure During UBR-MBC Collision

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
S-GW sends the Update Bearer Response message to P-GW with the cause code as 110 (Temp_Rejected_Due_To_Handover_In_Progress) when it identifies an ongoing Update Bearer Request message.	21.12.15
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: During a 3G to 4G handover, when PCRF initiates a QoS Class Index (QCI) change, MME neither rejects nor processes the Update Bearer Request message and it fails to send the Update Bearer Response message back to P-GW through S-GW. At the same time, MME tries to send the Modify Bearer Command (MBC) message to P-GW through S-GW. Then, S-GW sends the Update Bearer Response message to P-GW with the cause code as 89 (Service_Denied) when it identifies an ongoing Update Bearer Request message. MME is unable to update the QoS change because P-GW does not retry to send the Update Bearer Request message after it receives the Update Bearer Response message with the cause code as Service_Denied.

New Behavior: In 21.12.15 and later releases, S-GW sends the Update Bearer Response message to P-GW with the cause code as 110 (Temp_Rejected_Due_To_Handover_In_Progress) when it identifies an ongoing Update Bearer Request message. In this case, P-GW with the existing cause-code temp-fail configuration retries to send the Update Bearer Request message and MME is updated with the QCI change.

Note The temp-fail CLI for P-GW must be configured for the solution to work properly.

Customer Impact: Not applicable

Command Changes

egtp cause-code temp-failure ubr-mbc-collision

To enable the temporary failure of Update Bearer Request (UBR)-MBC collision handling functionality, use the following configuration:

```
configure
   contextcontext_name
      sgw-serviceservice_name
         [default | no] egtp cause-code temp-failure ubr-mbc-collision
         end
```

NOTES:

- **no** Disables the specified parameter.
- **cause-code** Configures the collision-handling failure response.
- **temp-failure** Configures the temporary failure response during collision-handling.
- **ubr-mbc-collision** Configures the service to send cause code 110 (temporary failure) for UBR-MBC collision. The default behavior is disabled.
- **default** Sets or resets the corresponding parameter to its default value.

Performance Indicator Changes

show sgw-service name sgw-service

The output of this command includes the following field:

- temp-failure ubr-mbc-collision: Indicates whether the temporary failure configuration for Update Bearer Request (UBR)-MBC collision is enabled or disabled.

CHAPTER 22

Handling the TAU and Location update Request/Response

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
MME sends Location Update Request/Response.	21.12.2
First introduced.	Pre 21.3

Handling the TAU and Location Update Request/Response

This behaviour is only applicable when all the following conditions are met:

- CIOT UE combined attached
- With UE in PSM or EDRX mode, data being sent to the UE, MME rejects the DDN with EGTP_CAUSE_UNABLE_TO_PAGE_UE
- Buffering starts in S-GW and with UE sending TAU with type as IMSI attach.

Previous Behavior: MME does not send modify bearer request, affecting buffering at S-GW.

New Behavior: UE triggers TAU, results in MME sending Location Update Request/Response. MME sends TAU Accept to UE (with S1 downlink-nas to eNB). With UE sending TAU Complete, MME sends TMSI Relocation Complete to MSC and Modify Bearer Request towards S-GW.

CHAPTER 23

IPv6 MTU Option Support in RA Message Enhancement

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	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
Enhancement to the CLI **ipv6 initial-router-advt**	21.12.18

Feature Changes

Previous Behavior: The CLI 'ipv6 initial-router-advt option mtu' was used to enable or disable by sending MTU in RA packet.

New Behavior: For the P-GW and SAEGW, an additional option **value** is added to the existing CLI command **ipv6 initial-router-advt option mtu**. The configured value must be in *octets -integer 1280-2000*. The syntax is as follws:

```
ipv6 initial-router-advt { interval int_value | num-advts num_value | option
mtu | value }
[ default ] ipv6 initial-router-advt { interval | num-advts| option mtu |
value }
no ipv6 initial-router-advt option mtu
```

The configured value is sent in the RA packet rather than the data tunnel MTU.

Important This value is used only for advertisement in RA packet and the gateway need not enforce this value. The behaviour of 'default' and 'no' options of this CLI remains the same.

CHAPTER 24

Mapped-UE-Usage-Type IE Support in MME

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.12.2

Feature Description

The "ue-usage-type" parameter is negotiated and already stored in subscriber database. This "ue-usage-type" is encoded in "Mapped UE Usage Type" IE in Create-Session-Request gtpv2 message and sent to SPGW to assist in network slicing. This is feature is CLI controlled.

Configuring Mapped-UE-Usage-Type IE Support in MME

This section provides information on the CLI commands to configure Mapped-UE-Usage-Type IE Support in MME.

decor send-ue-usage-type-in-csr

Use the following configuration to enable the sending of mapped UE-Usage to Dedicated Core Network Configuration.

```
configure
   call-control-profile call_control_profile_name
      [ remove ] decor send-ue-usage-type-in-csr
      end
```

NOTES:

- **remove**: Removes the configuration to enable the sending of mapped UE-Usage to Dedicated Core Network Configuration.
- **decor send-ue-usage-type-in-csr**: Enables the sending of mapped UE-Usage to Dedicated Core Network Configuration.

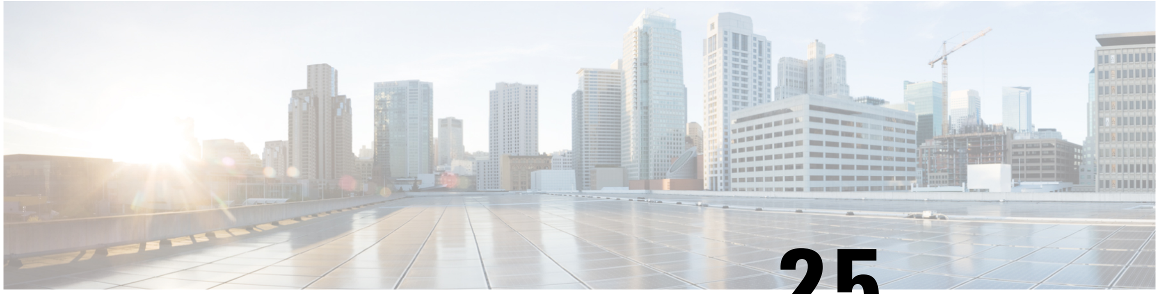
Monitoring and Troubleshooting

This section provides information regarding show commands available to monitor and troubleshoot the Mapped-UE-Usage-Type IE Support feature.

Show Commands and Outputs

show call-control-profile

The output of this command includes "Sending Ue-Usage-Type in CSR".



CHAPTER 25

MEC Location Management

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.14

Feature Description

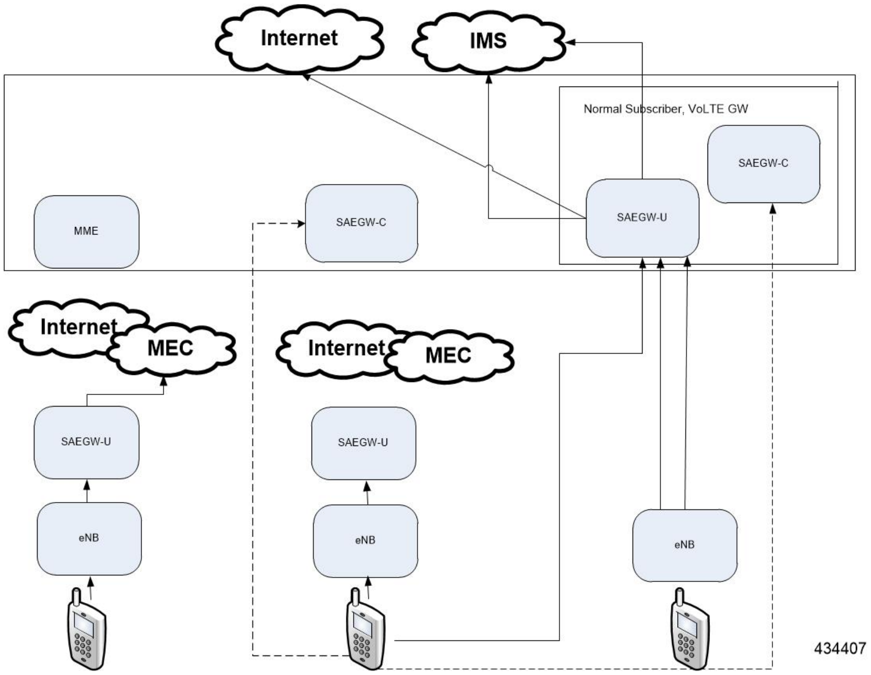
Mobile Edge Computing (MEC) Support is used to bring application with low latency requirements and capabilities to the carrier's network in order to explore a wide range of new use cases and applications. This feature enables selection of proper Edge User Plane nodes for MEC user sessions.

How It Works

Architecture

This section describes the MEC architecture.

Figure 1: MEC Architecture



Flows

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

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

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

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

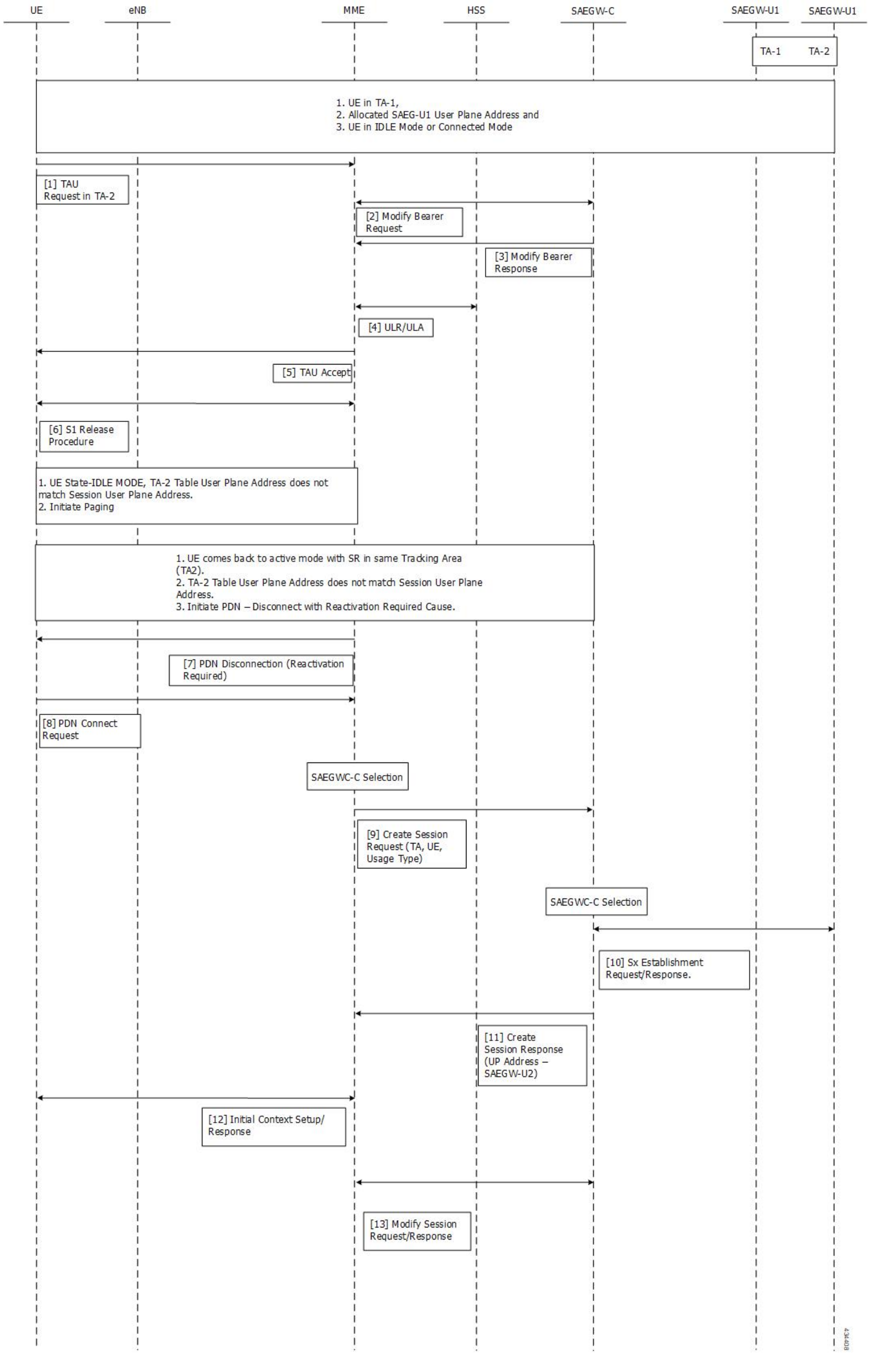
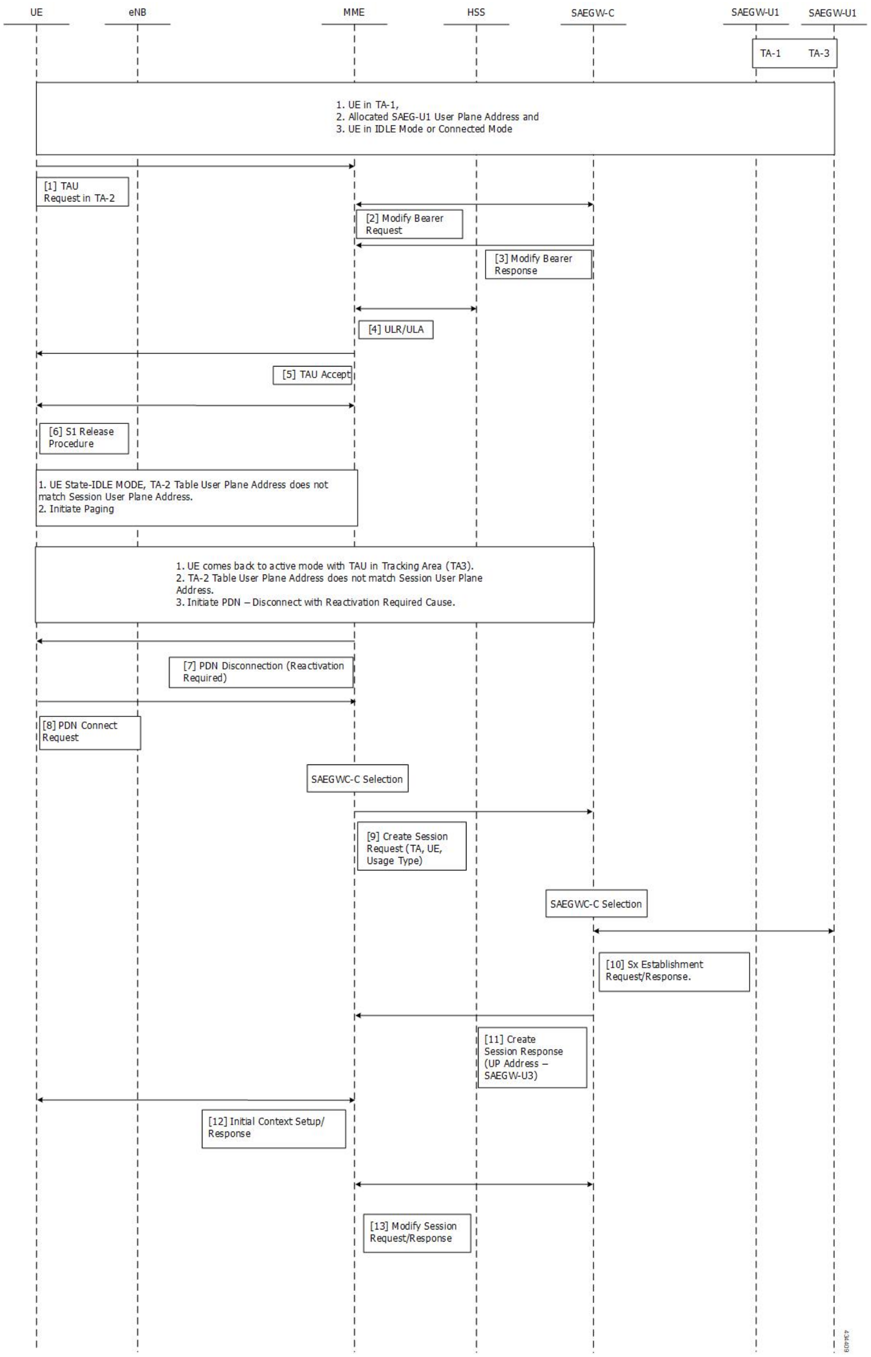

UE
eNB
MME
HSS
SAEGW-C
SAEGW-U1
SAEGW-U1
TA-1
TA-2
1. UE in TA-1,
2. Allocated SAEG-U1 User Plane Address and
3. UE in IDLE Mode or Connected Mode
[1] TAU Request in TA-2
[2] Modify Bearer Request
[3] Modify Bearer Response
[4] ULR/ULA
[5] TAU Accept
[6] S1 Release Procedure
1. UE State-IDLE MODE, TA-2 Table User Plane Address does not match Session User Plane Address.
2. Initiate Paging
1. UE comes back to active mode with SR in same Tracking Area (TA2).
2. TA-2 Table User Plane Address does not match Session User Plane Address.
3. Initiate PDN – Disconnect with Reactivation Required Cause.
[7] PDN Disconnection (Reactivation Required)
[8] PDN Connect Request
SAEGWC-C Selection
[9] Create Session Request (TA, UE, Usage Type)
SAEGWC-C Selection
[10] Sx Establishment Request/Response.
[11] Create Session Response (UP Address – SAEGW-U2)
[12] Initial Context Setup/ Response
[13] Modify Session Request/Response
434039

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


UE
eNB
MME
HSS
SAEGW-C
SAEGW-U1
SAEGW-U1
TA-1
TA-3
1. UE in TA-1,
2. Allocated SAEG-U1 User Plane Address and
3. UE in IDLE Mode or Connected Mode
[1] TAU Request in TA-2
[2] Modify Bearer Request
[3] Modify Bearer Response
[4] ULR/ULA
[5] TAU Accept
[6] S1 Release Procedure
1. UE State-IDLE MODE, TA-2 Table User Plane Address does not match Session User Plane Address.
2. Initiate Paging
1. UE comes back to active mode with TAU in Tracking Area (TA3).
2. TA-2 Table User Plane Address does not match Session User Plane Address.
3. Initiate PDN – Disconnect with Reactivation Required Cause.
[7] PDN Disconnection (Reactivation Required)
[8] PDN Connect Request
SAEGWC-C Selection
[9] Create Session Request (TA, UE, Usage Type)
SAEGWC-C Selection
[10] Sx Establishment Request/Response.
[11] Create Session Response (UP Address – SAEGW-U3)
[12] Initial Context Setup/ Response
[13] Modify Session Request/Response
434409

Configuring MEC Support

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

Configureing up-address in TAI Management DB

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

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

NOTES:

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

Configuring up-address in MEC TAI Group

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

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

NOTES:

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

Configuring tai in MEC TAI Group

Use the following configuration to configure the Tracking Area Identity.

```
configure
  lte-policy
    mec-tai-grp mec_tai_grp_name
     [ no ] tai mcc mcc_value mnc mnc_value { tac value1... value20  | tac-range
from  tac_value_from   to  tac_value_to   }
         [ no ] up-address ( IP-ADDRESS | IP-ADDRESS/MASK }
         end
```

NOTES:

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

Configuring up-service-area-change

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

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

NOTES:

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

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

Monitoring and Troubleshooting

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

Show Commands and Outputs

show mme-service statistics

The output of this command includes the following fields:

Paging Initiation for SIGNALING PDN RECONN Events:

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

Bulk Statistics

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

Table 1: MME Schema

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

Table 2: TAI Schema

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

CHAPTER 26

MME Handling of Purge Procedure

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

Command Changes

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

Configuring hss-purge-ue-request

Use the following configuration to configure HSS purge UE request.

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

NOTES:

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

Performance Indicator Changes

show mme-service all

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

CHAPTER 27

MME-MSC/VLR SGs Disconnect

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
Introduced to 21.12 release.	21.12.12
First introduced.	21.5.18

Feature Description

Without the **perform-imsi-detach** option the SGs SCTP association with respect to the peer-id will be aborted and corresponding SCTP data, timers are cleared and stopped, then the SCTP re-association will be triggered.

When the **perform-imsi-detach** and **without detach-rate** options are executed, the SGs SCTP association with respect to the peer-id will be aborted. UEs that are associated with the VLR will be detached at default-rate of 50 detaches/cycle and SGs-Reset-Indication will be send once the VLR re-association is up.

When the **perform-imsi-detach** and **detach-rate** options are executed, the SGs SCTP association with respect to the peer-id will be aborted. UEs that are associated with the VLR will be detached at the specified-rate and SGs-Reset-Indication will be send once the VLR re-association is up.

Important Increasing the detach rate might increase MME Manager load.

Configuring MME MSC/VLR SGs Disconnect

This section provides information on the CLI commands to configure MME disconnect SGs peer.

sgs-peer

Use the following configuration to disconnect the SGs peer and perform IMSI detach.

```
mme disconnect sgs-peer peer_id perform-imsi-detach [ detach-rate detach_rate
 ]
end
```

NOTES:

- **sgs-peer** *peer_id* : Disconnects the SGs peer. *peer_id* Must be an integer from 1 to 4294967295.
- **perform-imsi-detach**: Perform IMSI detach.
- **detach-rate** *detach_rate*: Detaches per cycle. *detach_rate* Must be an integer from 1 to 100.

CHAPTER 28

MME Manager Status Traps

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

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

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

Configuring MME Manager Status Traps

Use the following configuration to enable MME Manager Status Traps.

Enable MME manager busy trap

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

Enable MME manager normal trap

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

Disable MME manager busy trap

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

Disable MME manager normal trap

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

NOTES:

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

Monitoring and Troubleshooting

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

SNMP Traps

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

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

CHAPTER 29

MME Support for Service Impacting KPI Bulk Statistics

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

Monitoring and Troubleshooting

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

Show Commands and Outputs

show mme-service statistics recovered-values

The output of this command includes the following fields:

EMM Control Messages:

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

Procedure Failure Reasons:

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

Bulk Statistics

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

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

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

CHAPTER 30

Monitor Protocol Support for DCNR

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

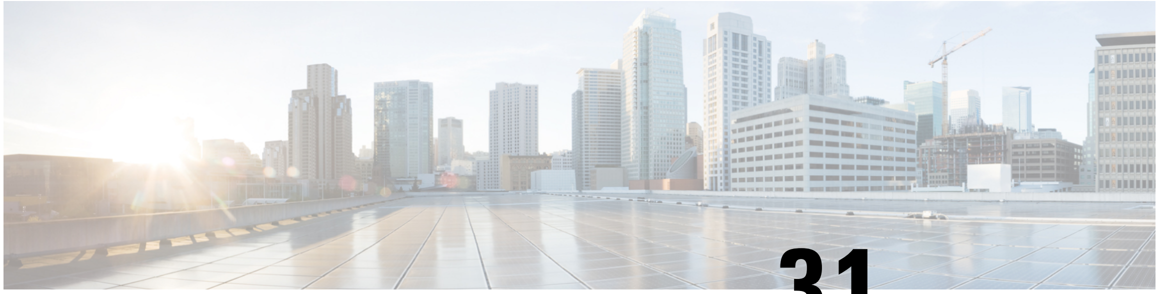
Revision History

Revision Details	**Release**
Monitor Protocol Support for DCNR is Introduced to 21.12 release.	21.12.11
First introduced.	21.14

Feature Changes

Previous Behavior: Monitor Protocol did not display dcnr flag and rDCNR flag.

New Behavior: Monitor Protocol is enhanced to displays newly introduced dcnr flag and rDCNR flag.



CHAPTER 31

NB-IOT EDRX Supported values in ATTACH/TAU Accept

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
NB-IOT EDRX Supported values in ATTACH/TAU Accept is Introduced to 21.12 release.	21.12.11
NB-IOT EDRX Supported values in ATTACH/TAU Accept is Introduced to 21.13 release.	21.13.11
First introduced.	21.14

Feature Changes

Previous Behavior: UE requests the EDRX value in the Extended DRX parameters IE in the Attach-Request or in the TAU-Request. In the Attach-Accept or in the TAU-Accepts, the requested value is sent.

New Behavior: For the NBIOT device, If the Extended DRX parameter values are 4, 6, 7 or 8, it is interpreted as 2 and sent in the Attach-Accept or in the TAU Accept.

CHAPTER 32

NETCONF Event Notification Support for Auto-scaleout

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UEM
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required **NOTE**: This feature is dependent on the existing Automatic Scale-out feature.
Related Features in this Release	Not Applicable
Related Documentation	• *UEM-based VNF Deployment Guide* • *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide*

Revision History

Revision Details	**Release**
First introduced.	6.6

Feature Changes

Event notifications are generated on em-notify stream via NETCONF protocol based on the status of Automatic Scale-out process.

Following are the different states at which the scale-out notifications are sent:

- required-initiated – Triggered when Auto scale-out is required and initiated
- required-not-initiated – Triggered when Auto scale-out is required but not initiated (for example: Auto scale-out resource constraints, etc.)
- successful – Triggered when Auto scale-out procedure is completed successfully
- failed – Triggered when Auto scale-out procedure could not be completed successfully

For more information on this feature, see the *UEM-based VNF Deployment Guide* for this release.

CHAPTER 33

Network Access Identifier Field Removal from MSISDN

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

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

Revision Details	**Release**
The change in behavior is also applicable to this release.	21.12.12
With this release, the P-GW does not add an extra character "19", that is Network Access Identifier (NAI) field in MSISDN, which is sent in Protocol Configuration Option (PCO) IE in CSRsp message.	21.13

Revision Details	Release
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: When MSISDN was sent in PCO in Create Session Response (CSRsp), the P-GW added an extra character "19" in MSISDN that was present in PCO.

New Behavior: While sending MSISDN in PCO in CSRsp, the P-GW does not send NAI, that is to say, the extra character "19".

Customer Impact: None

CHAPTER 34

NFVO-based Deployment of UGP VNF

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	6.6

Feature Changes

ESC supports NFVO-driven deployment of UEM and VPC VNFs as per the ETSI-NFV-SOL003 specification for the Or-Vnfm interface. It is assumed that the NFVO is from a third-party vendor.

To support the deployment of UEM and VPC VNFs, CSAR package is created and uploaded to the NFVO. The CSAR package comprises the VNFD for the VPC. Note that the package is compliant with the ETSI SOL004 v2.5.1 specification.

As part of this feature, the ESC version has been updated from 4.3.0.121 to 4.4.0.88.

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

CHAPTER 35

OWM Integra Deployment Automation on VMware VCD

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	OWM (3rd party)
Applicable Platform(s)	UGP
Feature Default	Disabled - Configuration required
Related Features in this Release	Not Applicable
Related Documentation	• *VMware VCD VNF Deployment Guide*

Revision History

Revision Details	**Release**
First introduced.	6.6

Feature Changes

Integra is a VNF-based traffic management solution from a 3rd party vendor, Openwave. It is a part of traffic steering solution, which comprises VPC VNF and Integra VNF deployed as a Service Function Chaining a.k.a Network Service Chaining.

This release supports the deployment of OWM Integra VNF in a VMware VCD environment. For detailed information on this feature, see the *VMware VCD VNF Deployment Guide*.

CHAPTER 36

Paging eDRX H-SFN Changed to 10 Bits Counter

Feature Summary and Revision History

Summary Data

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

Revision History

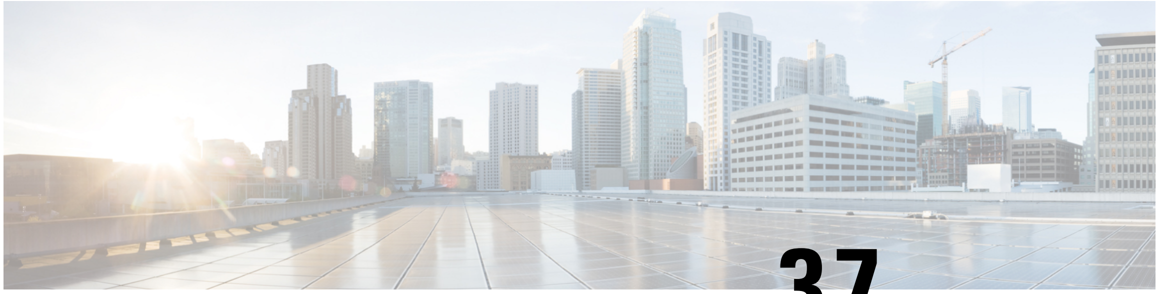
Revision Details	**Release**
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.13.	21.13.11
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.11.	21.11.3
Paging eDRX H-SFN changed to 10 bits counter introduced in release 21.12.	21.12.5
First introduced.	21.0

Feature Changes

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

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

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



CHAPTER 37

RAB Release for Attach on the Same IU Connection

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
First introduced.	21.12

Feature Description

With this release SGSN will send “RAB Assignment Request” with RABs to be released list to RNC and the session will be cleaned-up internally when “Attach Request” is received on Direct Transfer message on the existing IU connection.

Configuring RAB Release for Attach on the Same IU Connection

This section describes how to configure RAB Release for Attach on the Same IU connection.

Configuring RAB Assignment Request

Use the following configuration to send “RAB Assignment Request” with RABs to be released list to RNC by SGSN.

```
config
   context context_name
      iups-service  iups_service_name
              rnc id rnc_id
                 [ no ]ranap rab-release-att-ext-iu
                 end
```

Notes:

- **ranap rab-release-att-ext-iu** : When this CLI is configured, the SGSN will send “RAB Assignment Request” with RABs to be released list to RNC and the session will be cleaned-up internally when “Attach Request” is received on Direct Transfer message .
- **no**: Disables the configuration. By default this configuration is disabled.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the RAB Release for Attach on same IU connection.

Show Commands and Outputs

show iups-service name *service_name*

The output of this command includes the following fields:

IUPS configuration Output

- Rab release for Attach Request on existing IU:

Verifying the RAB Release Extension configuration

The following command displays configuration information about Enable/Disable sending of RAB Release list to RNC when new Attach Request is received on same the IU connection.

show configuration

CHAPTER 38

Service Impacting SGSN KPI Bulk Statistics

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

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

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

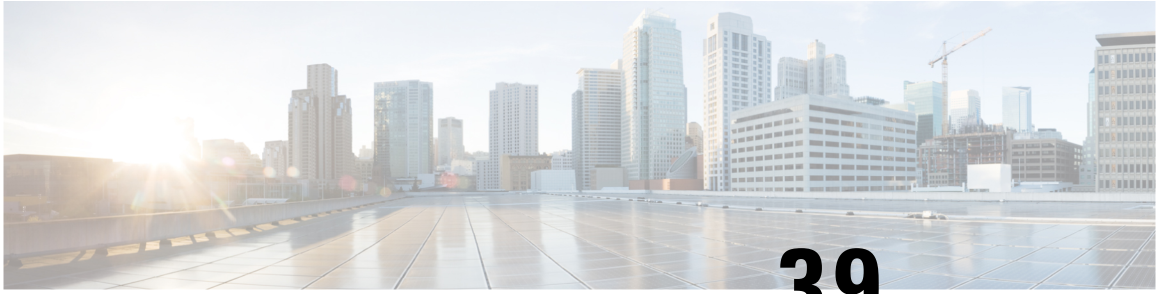
Once the session manager crashes or restarts all the backup counters will be restored to session manager.

Monitoring and Troubleshooting

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

Bulk Statistics

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



CHAPTER 39

SRVCC Delete Bearer Request Handling

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

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

Revision History

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

Revision Details	Release
First introduced.	Pre 21.5

Feature Changes

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

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

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

Command Changes

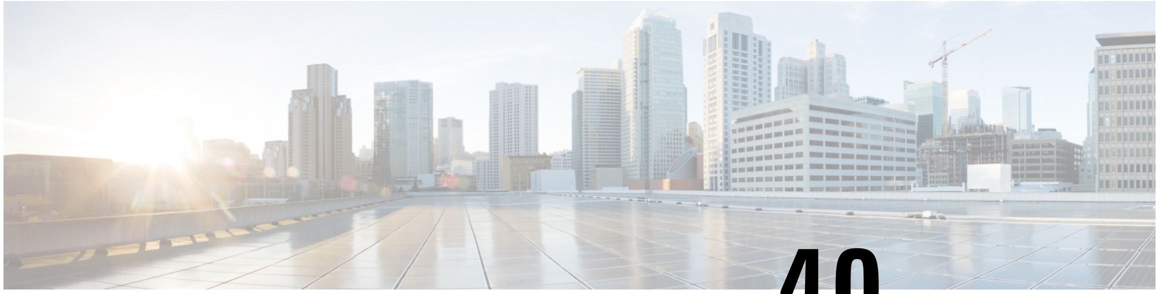
Configuring DBR Handling while SRVCC is Ongoing

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

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

Notes:

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



CHAPTER 40

SRVCC HO Timer Configuration for ESM Notification

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

Command Changes

Configuring UE Come Back Time

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

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

Notes:

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

CHAPTER 41

Support for Password Expiry Warning

Feature Summary and Revision History

Summary Data

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

Revision History

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

Revision Details	Release
First introduced.	21.12

Feature Description

The Support for Password Expiry Warning enables the password expiry warning interval to be configured for local users. A warning message is displayed that informs the user about the password expiry interval. The user is recommended to change the password after login. It is only after the user acknowledges the warning message that the user can proceed to log in.

A new keyword **exp-warn-interval** *days* is added to the **local-user password** CLI command in support of this feature.

Configuring Support for Password Expiry Warning

The following section provides information about the CLI command in support of this feature.

Configuring Password Expiry Warning Interval

Use the following CLI commands to configure the password expiry warning interval. This command is configured in in Global Configuration Mode.

```
configure
   local-user password exp-warn-interval days
   end
```

```
no local-user password exp-warn-interval
```

```
default local-user password exp-warn-interval
```

NOTES:

- **no** : Disables the specified password expiry warning interval configuration.
- **exp-warn-interval** *days*: Specifies the password expiry warning interval in days.
- **default** : Sets the password expiry warning interval to the default value of 30 days.

CHAPTER 42

Target MME Load Balancing During Handover

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	**Release**
With this release, this feature is fully qualified.	21.13
First introduced. **Important** Target MME Load Balancing During Handover feature is not fully qualified in this release. It is available only for testing purposes.	21.12.2

Feature Description

MME can now configure multiple MME addresses for the same Tracking Area Identity (TAI) with the same priority. During the S1 handover procedure, MME selects the target MME based on the static configuration. If more than one MME is configured for the same TAI and priority then the round robin logic of selecting MMEs is used.

With this release, the limitation in configuring multiple MME addresses for the same TAI and priority is removed.

Consider an example where target MMEs with ip-address1, ip-address2 and ip-address3 are configured for the same TAI and priority. For the first handover to target TAI, the MME with address1 is used, for the second handover the MME address2 is used, and for the third handover the MME address3 is used. This sequence is repeated upon successive handovers to the same TAI.

```
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address1>
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address2>
peer-mme tai-match  priority <val> mcc <val> mnc <val> tac <val> address <ip-address3>
```

Note Each Session Manager independently load balances between the target MMEs.

CHAPTER 43

Upgrade and Migration of Open SSH to Cisco SSH

Feature Summary and Revision History

Summary Data

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

Revision History

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

Revision Details	Release
With this release, the algorithm values of Ciphers and MACs are modified based on the upgrade and migration of OpenSSH to CiscoSSH.	21.16
First introduced.	Pre 21.2

Feature Changes

As a security measure for Cisco ASR 5500 and VPC products, the Ciphers and MACs algorithm values are modified to support the upgrade and migration of the Open SSH to Cisco SSH versions.

Previous Behavior: In releases earlier to 21.16, the **default** algorithm values of the **cipher** and **macs** commands were as follows:

- **Cipher**

  Release 20.x to 21.15 (Normal build only)

  Resets the value of *algorithm* in a Normal build to:

  ```
  blowfish-cbc,3des-cbc,aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
  ```

- **MACs**

  Release 20.x to 21.15 (Trusted build only)

  Resets the value of *algorithm* in a Trusted build to:

  ```
  hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
  hmac-sha2-256,hmac-sha1
  ```

- **KEX Algorithms**

  Release 20.x to 21.15

  Available Algorithms in Normal and Trusted Builds:

  ```
  diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
  ```

New Behavior: In this release, the **default** algorithm values of the **cipher** and **macs** commands are as follows:

- **Cipher**

  Release 21.16 onwards: Post OpenSSH to CiscoSSH Upgrade and Migration

  Default Algorithms in a Normal Build:

  ```
  aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com
  ```

  Available Algorithms in a Normal Build:

  ```
  aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc
  ```

  Default and Available Algorithms in Trusted Builds:

  ```
  aes256-ctr,aes192-ctr,aes128-ctr
  ```

Note There is no change in the default and configurable Ciphers for Trusted builds.

- **MACs**

  Release 21.16 onwards: Post OpenSSH to CiscoSSH Upgrade and Migration

  Default and Available Algorithms in Normal Builds:

  ```
  hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
  hmac-sha2-256,hmac-sha1
  ```

  Default Algorithms in Trusted Builds:

  ```
   hmac-sha2-512,hmac-sha2-256,hmac-sha1
  ```

  Available Algorithms in Trusted Builds:

  ```
  hmac-sha2-512,hmac-sha2-256,hmac-sha1
  ```

  Note hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com are removed from the Trusted builds.

- **KEX Algorithms**

  Release 21.16 onwards: Post OpenSSH to CiscoSSH Upgrade and Migration

  Available Algorithms in Normal and Trusted Builds:

  ```
  diffie-hellman-group14-sha1
  ```

  Note KEX algorithms are not configurable in StarOS. Therefore, there are no CLI changes.