Release Change Reference, StarOS Release 21.14/Ultra Services Platform Release 6.8

First Published: 2019-07-19

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

CONTENTS

CHAPTER 1 **Release 21.14/6.8 Features and Changes Quick Reference** 1

Release 21.14/6.8 Features and Changes 1

CHAPTER 2 **Feature Defaults Quick Reference** 3

Feature Defaults 3

CHAPTER 3 **Bulk Statistics Changes Quick Reference** 5

New Bulk Statistics 5

Modified Bulk Statistics 11

Deprecated Bulk Statistics 11

CHAPTER 4 **SNMP MIB Changes in StarOS 21.14 and USP 6.8** 13

SNMP MIB Object Changes for 21.14 13

SNMP MIB Alarm Changes for 21.14 14

SNMP MIB Conformance Changes for 21.14 14

SNMP MIB Object Changes for 6.8 15

SNMP MIB Alarm Changes for 6.8 15

SNMP MIB Conformance Changes for 6.8 15

CHAPTER 5 **Adding Discrete eNB IDs to eNB Group in MME** 17

Feature Summary and Revision History 17

Feature Description 18

Adding Discrete eNB IDs to eNB Group in MME 18

Adding the eNB Group 18

Adding the eNB ID List in the eNB Group 19

Monitoring and Troubleshooting 19

Show Commands and Outputs 19

CHAPTER 6 **Auto-Recovery of AutoDeploy and AutoIT Instances** 21

Revision History 21

Feature Summary and Revision History 21

Feature Description 22

CHAPTER 7 **Availability Zone and Host Placement Support for VPC on UEM** 25

Revision History 25

Feature Summary and Revision History 25

Feature Description 26

CHAPTER 8 **Buffer Usage Reduction on TCP Slow Start** 27

Feature Summary and Revision History 27

Feature Changes 27

CHAPTER 9 **Cisco Ultra Traffic Optimization** 29

Feature Summary and Revision History 29

Overview 30

How Cisco Ultra Traffic Optimization Works 31

Architecture 31

Handling of Traffic Optimization Data Record 32

List of Attributes and File Format 32

Licensing 34

Limitations and Restrictions 34

Configuring Cisco Ultra Traffic Optimization 34

Loading Traffic Optimization 34

Enabling Cisco Ultra Traffic Optimization Configuration Profile 35

Configuring the Operating Mode 35

Enabling Cisco Ultra Traffic Optimization Configuration Profile Using Service-scheme Framework 35

Session Setup Trigger 36

Bearer Creation Trigger 36

Flow Creation Trigger 37

Generating TODR 38
Multi-Policy Support for Traffic Optimization 39
How Multi-Policy Support Works 39
Configuring Multi-Policy Support 40
Configuring a Traffic Optimization Profile 40
Configuring a Traffic Optimization Policy 41
Associating a Trigger Action to a Traffic Optimization Policy 44
Enabling TCP and UDP 44
Service-Scheme Configuration for Multi-Policy Support 44
Monitoring and Troubleshooting 52
Cisco Ultra Traffic Optimization Show Commands and/or Outputs 52
show active-charging traffic-optimization counters 52
show active-charging traffic-optimization info 54
show active-charging traffic-optimization policy 54
Bulk Statistics 55

CHAPTER 10 **Cisco Ultra Traffic Optimization Library Version Upgrade 61**
Feature Summary and Revision History 61
Feature Changes 62

CHAPTER 11 **Co-Located SPGW Selection for Emergency Bearer 63**
Feature Summary and Revision History 63
Feature Changes 64
Command Changes 64
pgw co-location 64
Performance Indicator Changes 64
show lte-policy lte-emergency-profile <profile_name> 64

CHAPTER 12 **Collision Handling of Last PDN Disconnect Connection Establishment 65**
Feature Summary and Revision History 65
Feature Changes 66
Command Changes 66
Enabling PDN Disconnect by UE 66
Performance Indicator Changes 66

show mme-service all 66

CHAPTER 13 **Collision Handling for Path Update during Bearer Creation 67**

Feature Summary and Revision History 67

Feature Description 68

CHAPTER 14 **ConfD Upgrade Support 69**

Feature Summary and Revision History 69

Feature Description 70

CHAPTER 15 **Dedicated Core Networks on MME 71**

Feature Summary and Revision History 71

Feature Description 73

Overview 73

External Interfaces 73

DNS 73

S6a (HSS) Interface 74

GTPv2 (MME or S4-SGSN) 75

How It Works 75

Flows 76

P-GW Selection based on ULAs UE Usage Type 76

UE Assisted Dedicated Core Network Selection 76

UE Usage Type Deletion by DSR Flag 76

NAS Message Redirection Procedure 76

ATTACH/TAU Procedure 77

HSS Initiated Dedicated Core Network Reselection 80

Impact to Handover Procedures 81

Roaming 82

Network Sharing 82

Limitations 82

Standards Compliance 82

Configuring DECOR on MME 83

Configuring custom-actions ula gw-selection 83

Configuring DECOR Profile 84

Associating a DECOR Profile under MME Service 85
Associating a DECOR Profile under Call Control Profile 86
Configuring UE Usage Type over S6a Interface under MME Service 86
Configuring UE Usage Type over S6a Interface under Call Control Profile 87
Configuring UE Usage Type under Call Control Profile 87
Configuring Non-Broadcast TAI 87
Monitoring and Troubleshooting 88
Show Commands and/or Outputs 88
show decor-profile full all 88
show mme-service all 89
show mme-service name <mme_svc_name> 89
show mme-service session full all 89
show mme-service statistics decor decor-profile <decor_profile_name> 89
show mme-service statistics decor 91
show mme-service statistics 93
show mme-service statistics recovered-values 96
Bulk Statistics 96
MME Schema 96
MME Decor Schema 100

CHAPTER 16 **Deprecation of Manual Scaling** 105
Feature Summary and Revision History 105
Feature Changes 105

CHAPTER 17 **Dynamic and Static Proxy Changes for IPv6 Flow Label** 107
Feature Summary and Revision History 107
Feature Changes 107

CHAPTER 18 **Enhanced Password Security** 109
Feature Summary and Revision History 109
Feature Changes 110
Command Changes 110
local-user password 110
local-user username 111

CHAPTER 19 ERAB Setup Retry Handling 113
Feature Summary and Revision History 113
Feature Changes 114
Command Changes 114
erab-setup-rsp-fail retry-timer 114
Performance Indicator Changes 115
show mme-service name <mme_svc_name> 115

CHAPTER 20 IPv6 Address Support for TACACS+ Server 117
Feature Summary and Revision History 117
Feature Changes 118
Command Changes 118
server 118

CHAPTER 21 GMLC Interworking Support 121
Feature Summary and Revision History 121
Feature Description 122
GMLC Interworking Support Configuration 122
Including Experimental Result Code in PLA 122
Monitoring and Troubleshooting 122
Show Commands and Outputs 123

CHAPTER 22 Implicit Update Location to HSS 125
Feature Summary and Revision History 125
Feature Description 126
Configuring Implicit Update Location to HSS 126
Enabling Implicit Update Location to HSS 126
Monitoring and Troubleshooting 126
Show Commands and Outputs 126

CHAPTER 23 MME Clear Subscriber Enhancement 127
Feature Summary and Revision History 127

Feature Description 128
MME Clear-Subscriber Enhancement 128
Configuring Clear Subscriber MME-Only 128
Monitoring and Troubleshooting 128
Show Commands and Outputs 128
Bulkstatistics 129

CHAPTER 24 MME Double Counting Statistics of DECOR Rerouted Attach Accept 131
Feature Summary and Revision History 131
Feature Changes 132
Command Changes 132
Configuring custom-actions air explicit-air-flags 132

CHAPTER 25 MME-MEF Interface 133
Feature Summary and Revision History 133
Feature Description 134
How It Works 134
Architecture 134
Limitations 137
Configuring MME MEF Interface 138
Configuring egtp-mef-service 138
Configuring Peer MEF Address 138
Monitoring and Troubleshooting 139
Show Commands and Outputs 139

CHAPTER 26 Monitoring and Reporting of Stonith Service Failures 141
Feature Summary and Revision History 141
Feature Description 141

CHAPTER 27 Monitor Protocol Support for DCNR 143
Feature Summary and Revision History 143
Feature Changes 144

CHAPTER 28 NB-IOT EDRX Supported values in ATTACH/TAU Accept 145
Feature Summary and Revision History 145
Feature Changes 146

CHAPTER 29 NR UE Security Capability IE for 5G Security Support on MME 147
Feature Summary and Revision History 147
Feature Changes 148
Command Changes 149
NR UE Security Capability IE 149

CHAPTER 30 P-GW Buffering Mechanism 151
Feature Summary and Revision History 151
Feature Description 152
How It Works 152
Configuring the P-GW Buffering Mechanism Feature 152

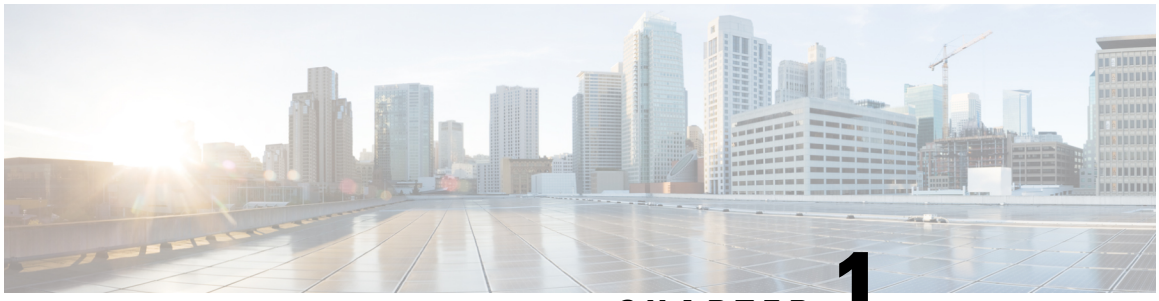
CHAPTER 31 Sender FTEID IE in Modify Bearer Request Message 153
Feature Summary and Revision History 153
Feature Changes 154

CHAPTER 32 SGSN Clear Subscriber Enhancement 155
Feature Summary and Revision History 155
Feature Description 156
Configuring Clear Subscriber 156
Clear Subscribers Enhancement 156

CHAPTER 33 UEM as CF Active/Standby Arbitrator 157
Revision History 157
Feature Summary and Revision History 157
Feature Description 158
How It Works 158
Configuring the UEM as CF Active/Standby Arbitrator 158

CHAPTER 34 UEM Interworking with Generic VNFM 161
Feature Summary and Revision History 161
Feature Description 161

CHAPTER 35 Unique Virtual Router ID for All UEM Deployments 163
Feature Summary and Revision History 163
Feature Changes 163



CHAPTER 1

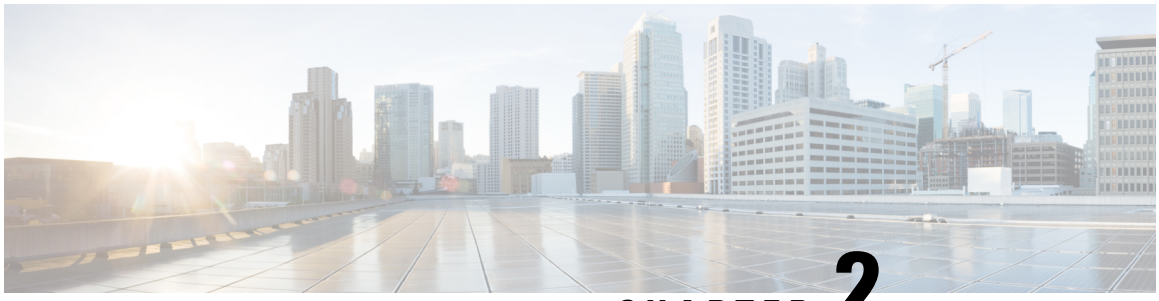
Release 21.14/6.8 Features and Changes Quick Reference

- Release 21.14/6.8 Features and Changes, on page 1

Release 21.14/6.8 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Adding Discrete eNB IDs to eNB Group in MME, on page 17	MME	21.14
Auto-Recovery of AutoDeploy and AutoIT Instances, on page 21	UAS	6.8
Availability Zone and Host Placement Support for VPC on UEM, on page 25	UEM	6.8
Buffer Usage Reduction on TCP Slow Start, on page 27	VPC-DI	21.14.10
Cisco Ultra Traffic Optimization, on page 29	P-GW	21.14
Cisco Ultra Traffic Optimization Library Version Upgrade, on page 61	P-GW	21.14.2
Co-Located SPGW Selection for Emergency Bearer, on page 63	MME	21.14.8
Collision Handling for Path Update during Bearer Creation, on page 67	MME	21.14
Collision Handling of Last PDN Disconnect Connection Establishment, on page 65	MME	21.14.16
ConfD Upgrade Support, on page 69	All	21.14
Dedicated Core Networks on MME, on page 71	MME	21.14

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Deprecation of Manual Scaling, on page 105	UAS	6.0
Dynamic and Static Proxy Changes for IPv6 Flow Label, on page 107	P-GW	21.14.5
Enhanced Password Security	All	21.14
ERAB Setup Retry Handling, on page 113	MME	21.14.3
GMLC Interworking Support , on page 121	MME	21.14
IPv6 Address Support for TACACS+ Server, on page 117	All	21.14
Implicit Update Location to HSS, on page 125	MME	21.14
MME-MEF Interface, on page 133	MME	21.14
MME Clear Subscriber Enhancement, on page 127	MME	21.14
MME Double Counting Statistics of DECOR Rerouted Attach Accept, on page 131	MME	21.14
Monitoring and Reporting of Stonith Service Failures, on page 141	UAS	6.8
Monitor Protocol Support for DCNR, on page 143	MME	21.14
NB-IOT EDRX Supported values in ATTACH/TAU Accept, on page 145	MME	21.14
NR UE Security Capability IE for 5G Security Support on MME, on page 147	MME	21.14.19
P-GW Buffering Mechanism, on page 151	P-GW	21.14
Sender FTEID IE in Modify Bearer Request Message, on page 153	P-GW	21.14
SGSN Clear Subscriber Enhancement, on page 155	SGSN	21.14
UEM as CF Active/Standby Arbitrator, on page 157	UEM	21.14 6.8
UEM Interworking with Generic VNFM, on page 161	UEM	6.8
Unique Virtual Router ID for All UEM Deployments, on page 163	UEM	6.8



CHAPTER 2

Feature Defaults Quick Reference

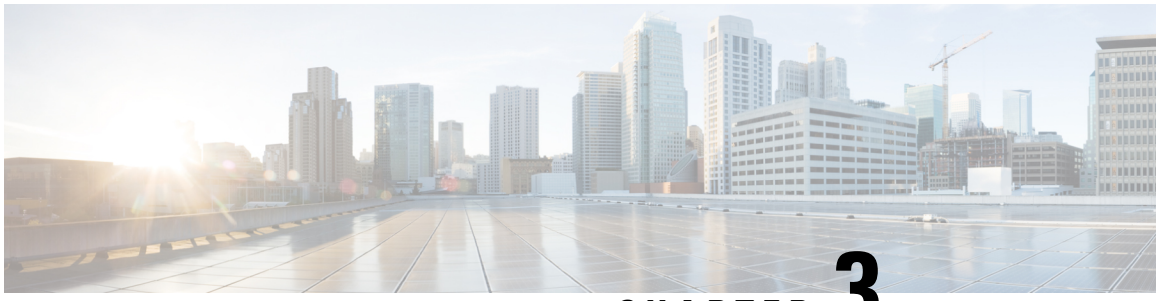
- Feature Defaults, on page 3

Feature Defaults

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

Feature	Default
Adding Discrete eNB IDs to eNB Group in MME	Enabled - Configuration Required
Auto-Recovery of AutoDeploy and AutoIT Instances	Enabled - Configuration Required
Availability Zone and Host Placement Support for VPC on UEM	Enabled - Always-on
Buffer Usage Reduction on TCP Slow Start	Enabled - Always-on
SGSN Clear Subscriber Enhancement	Enabled - Configuration Required
Cisco Ultra Traffic Optimization	Disabled - Configuration required
Cisco Ultra Traffic Optimization Library Version Upgrade	Not Applicable
Co-Located SPGW Selection for Emergency Bearer	Disabled - Configuration Required
Collision Handling for Path-Update during Bearer Creation	Enabled - Always-on
Collision Handling of Last PDN Disconnect Connection Establishment	Enabled - Configuration Required
ConfD Upgrade Support	Enabled - Always-on
Dedicated Core Networks on MME	Enabled - Configuration Required
Deprecation of Manual Scaling	Disabled - Configuration Required
Enhanced Password Security	Enabled - Always-on
ERAB Setup Retry Handling	Disabled - Configuration Required
GMLC Interworking Support	Enabled - Configuration Required

Feature	Default
Implicit Update Location to HSS	Disabled - Configuration required
IPv6 Address Support for TACACS+ Server	Disabled - Configuration Required
MME Clear Subscriber Enhancement	Enabled - Configuration Required
MME Double Counting Statistics of DÉCOR Rerouted Attach Accept	Enabled - Configuration Required
MME MEF-Interface	Enabled - Configuration Required
Monitoring and Reporting of Stonith Service Failures	Enabled - Always on
Monitor Protocol Support for DCNR	Enabled - Always-on
NB-IOT EDRX Supported values in ATTACH/TAU Accept	Enabled - Configuration Required
NR UE Security Capability IE for 5G Security Support on MME	Enabled - Configuration Required
P-GW Buffering Mechanism	Disabled - Configuration Required
Sender F-TEID IE in Modify Bearer Request Message	Enabled - Always-on
SGSN Clear Subscriber Enhancement	Enabled - Configuration Required
UEM as CF Active/Standby Arbitrator	Disabled - Configuration Required
UEM Interworking with Generic VNFM	Disabled - Configuration required
Unique Virtual Router ID for All UEM Deployments	Disabled - Configuration required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.14 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 21.14 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 11
- Deprecated Bulk Statistics, on page 11

New Bulk Statistics

This section identifies new bulk statistics and new bulk statistic schemas introduced in release 21.14.

ECS Schema

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

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

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

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

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

Bulk Statistics	Description
udp-uplink-hold	Indicates the number of UDP uplink-hold for Cisco Ultra Traffic Optimization.
udp-uplink-forward	Indicates the number of UDP uplink-forward for Cisco Ultra Traffic Optimization.
udp-uplink-forward-and-hold	Indicates the number of UDP uplink-forward and hold for Cisco Ultra Traffic Optimization.
udp-uplink-hold-failed	Indicates the number of UDP uplink-hold failed for Cisco Ultra Traffic Optimization.
udp-uplink-bw-limit-flow-sent	Indicates the number of UDP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-drop	Indicates the number of UDP downlink-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-hold	Indicates the number of UDP downlink-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-forward	Indicates the number of UDP downlink-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-forward-and-hold	Indicates the number of UDP downlink-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-hold-failed	Indicates the number of UDP downlink-hold failed for Cisco Ultra Traffic Optimization.
udp-dnlink-bw-limit-flow-sent	Indicates the number of UDP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-async-drop	Indicates the number of UDP downlink-async-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold	Indicates the number of UDP downlink-async-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward	Indicates the number of UDP downlink-async-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward-and-hold	Indicates the number of UDP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold-failed	Indicates the number of UDP downlink-async-hold failed for Cisco Ultra Traffic Optimization.
udp-process-packet-drop	Indicates the number of UDP process-packet-drop for Cisco Ultra Traffic Optimization.
udp-process-packet-hold	Indicates the number of UDP process-packet-hold for Cisco Ultra Traffic Optimization.

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

MME TAI Schema

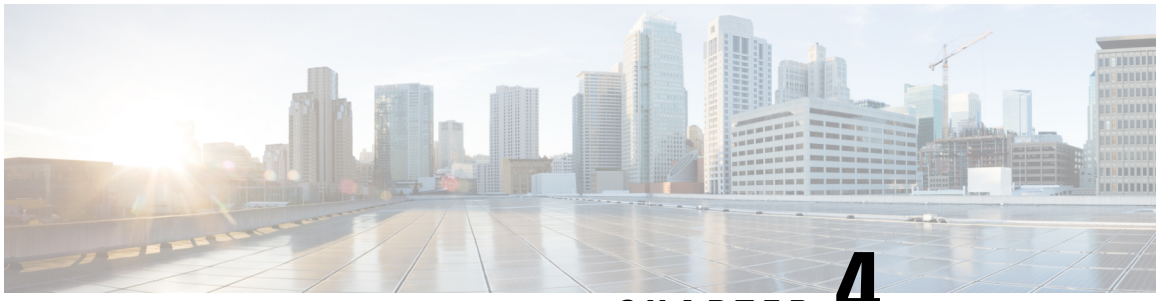
Statistics	Description
tai-sess-call-attached	Indicates the current total number of calls in attached per TAI.
tai-sess-call-connected	Indicates the current total number of calls in connected state per TAI.
tai-sess-call-idle	Indicates the current total number of calls in idle state.

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.14 and USP 6.8

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.14 and Ultra Services Platform (USP) 6.8 software releases.

- SNMP MIB Object Changes for 21.14, on page 13
- SNMP MIB Alarm Changes for 21.14, on page 14
- SNMP MIB Conformance Changes for 21.14, on page 14
- SNMP MIB Object Changes for 6.8, on page 15
- SNMP MIB Alarm Changes for 6.8, on page 15
- SNMP MIB Conformance Changes for 6.8, on page 15

SNMP MIB Object Changes for 21.14

This section provides information on SNMP MIB alarm changes in release 21.14.

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 21.14.

The following alarms are new in this release:

- starMMEManagerInst
- starMMEManagerStatus
- starMMEManagerBusy
- starMMEManagerNormal

Modified SNMP MIB Object

None in this release.

Deprecated SNMP MIB Object

None in this release.

SNMP MIB Alarm Changes for 21.14

This section provides information on SNMP MIB alarm changes in release 21.14.

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

New SNMP MIB Alarms

None in this release.

Modified SNMP MIB Alarms

None in this release.

Deprecated SNMP MIB Alarms

None in this release.

SNMP MIB Conformance Changes for 21.14

This section provides information on SNMP MIB alarm changes in release 21.14.

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

New SNMP MIB Conformance

None in the release.

Modified SNMP MIB Conformance

None in the release.

Deprecated SNMP MIB Conformance

None in the release.

SNMP MIB Object Changes for 6.8

This section provides information on SNMP MIB object changes in the Ultra M MIB corresponding to release 6.8.

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

New SNMP MIB Objects

None in this release.

Modified SNMP MIB Objects

None in this release.

Deprecated SNMP MIB Objects

None in this release.

SNMP MIB Alarm Changes for 6.8

This section provides information on SNMP MIB alarm changes in the Ultra M MIB corresponding to release 6.8.

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

New SNMP MIB Alarms

None in this release.

Modified SNMP MIB Alarms

None in this release.

Deprecated SNMP MIB Alarms

None in this release.

SNMP MIB Conformance Changes for 6.8

This section provides information on SNMP MIB conformance statement changes in the Ultra M MIB corresponding to release 6.8.

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

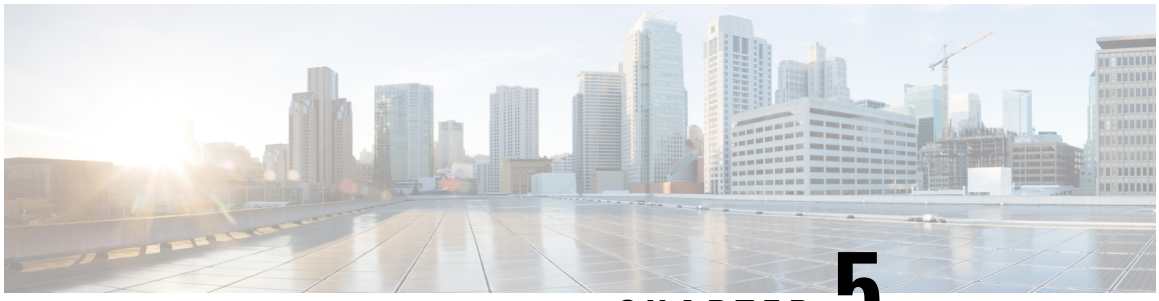
None in this release.

Modified SNMP MIB Conformance Statements

None in this release.

Deprecated SNMP MIB Conformance Statements

None in this release.



CHAPTER 5

Adding Discrete eNB IDs to eNB Group in MME

- Feature Summary and Revision History, on page 17
- Feature Description, on page 18
- Adding Discrete eNB IDs to eNB Group in MME, on page 18
- Monitoring and Troubleshooting, on page 19

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

Important This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account representative.

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

Adding Discrete eNB IDs to eNB Group in MME

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

Adding the eNB Group

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

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

NOTES:

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

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

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

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

Adding the eNB ID List in the eNB Group

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

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

NOTES:

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

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

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

Monitoring and Troubleshooting

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

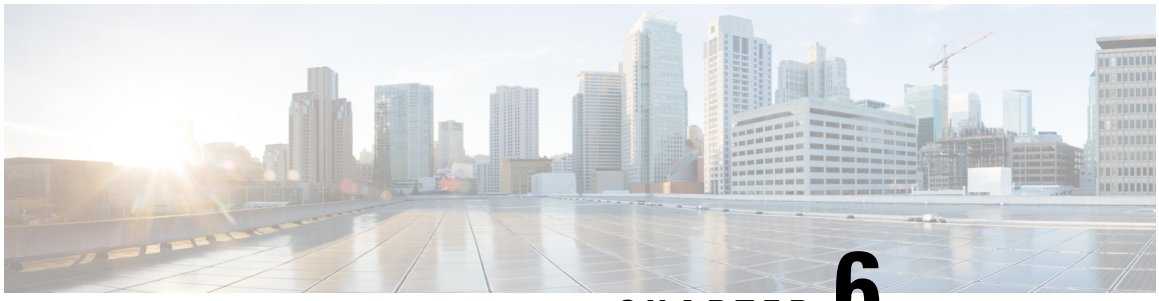
Show Commands and Outputs

show lte-policy enb-group name *enb_group_name*

The output of this command includes the following fields:

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

- List of eNB IDs



CHAPTER 6

Auto-Recovery of AutoDeploy and AutoIT Instances

- Revision History, on page 21
- Feature Description, on page 22

Revision History

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	6.8

Feature Description

This feature automates the recovery of AutoDeploy and AutoIT instances in KVM and OpenStack environment when any of the instances are inactive. This functionality can be achieved using the **boot_uas.py** script.

Important The auto-recovery mechanism works only in the HA mode.

To perform the auto-recovery of AutoDeploy instance, use the following script from a bare metal server:

./boot_uas.py --kvm --autodeploy --hostname *HOSTNAME* **--recover** *RECOVERY ID*

To perform the auto-recovery of AutoIT instance, use the following script from the bare metal server:

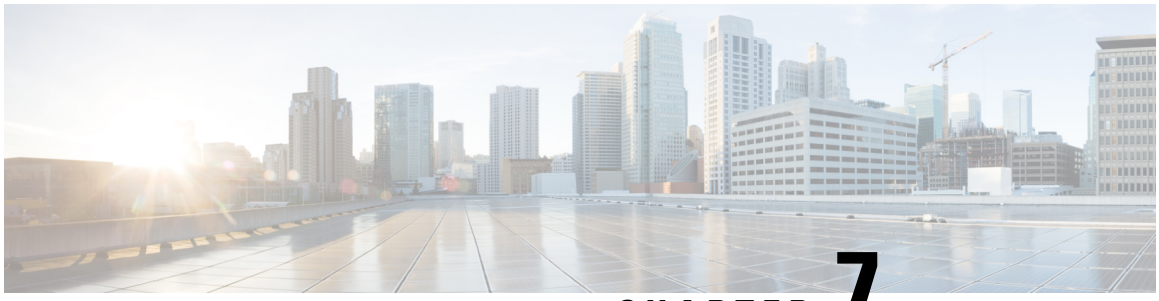
./boot_uas.py --kvm --autoit --hostname *HOSTNAME* **--recover** *RECOVERY ID*

The description of the options in the script is as follows:

Options	Description
--kvm	Specifies the recovery of the AutoDeploy or AutoIT instance from KVM (bare metal server). **Important** Recovery of the AutoDeploy and AutoIT instances in the OpenStack environment uses the same script but replacing the **kvm** option with **openstack** option in the script.
--autodeploy	Specifies the recovery of the AutoDeploy instances.
--autoit	Specifies the recovery of the AutoIT instances.

Options	Description
--hostname	Specifies the hostname of the instance to recover. Each of the AutoDeploy and AutoIT instances has one instance ID that is used to identify the instance to recover in the HA mode. So, setting this option is mandatory. To determine the hostname, follow these steps: **In the OpenStack environment:** **1.** Navigate to the */opt/cisco/uas-deployments* directory path. **2.** Use the **grep** command with the image name, which is used at the time of deployment of the AutoDeploy and AutoIT, to identify the deployment ID. For example : **grep -nr "64regression-image" *** **3.** Open the text file that corresponds to the identified deployment ID and check the value of the "name" key in the file. **Note** The value of the name key is the hostname. **In the KVM environment**: Use the hostname that was already configured during the deployment of AutoIT and AutoDeploy. Otherwise, log on to the AutoIT or AutoDeploy node and obtain the hostname from the active node.

Options	Description
--recover	**In the KVM environment:** Specifies the recovery value as an instance ID. Use this value to identify the unique deployment. **Note** The deployment ID for the AutoDeploy and AutoIT is available at the */var/cisco/AutoDeploy* and */var/cisco/AutoIT* directory paths, respectively. **In the OpenStack environment:** Specifies the recovery value as a deployment ID. Use this value to identify the unique deployment. **Note** The deployment ID for AutoDeploy and AutoIT is available at the */opt/cisco/uas-deployments* directory path. To identity the deployment ID, use the **grep** command with the image name, which is used at the time of deployment of the AutoDeploy and AutoIT. For example : **grep -nr "64regression-image" ***



CHAPTER 7

Availability Zone and Host Placement Support for VPC on UEM

- Revision History, on page 25
- Feature Description, on page 26

Revision History

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UEM
Applicable Platform(s)	UGP
Feature Default	Enabled - Always-on
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.	6.8

Feature Description

The Ultra Element Manager (UEM) and Elastic Services Controller (ESC) together provide the ability to specify an availability zone or a host for a better placement control of the VPC VNFs.

To support the availability zone and host placement, the ESC version is updated from 4.4.0.88 to 4.5.0.112 and the CSAR package (for ETSI SOL003 based deployments) is modified. The availability zone and host placement are configurable per VNFC instance for a greater flexibility. New UEM and VPC parameters are introduced to provide this functionality.

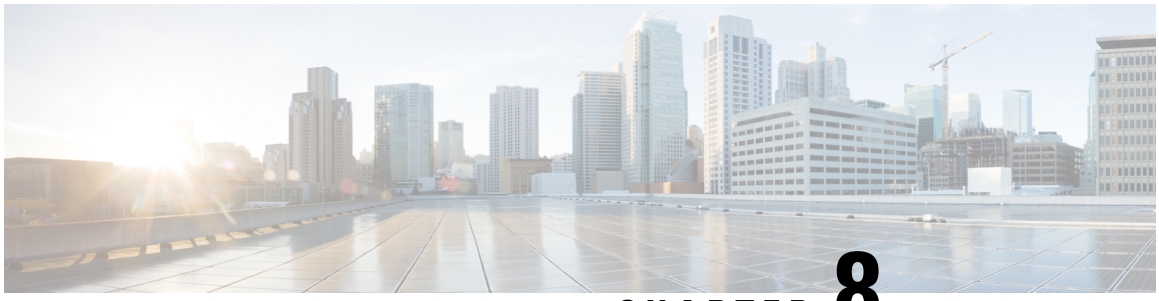
Each VM is deployed in the specified host or zone depending on the parameter configurations. When the VM_PLACEMENT_TYPE parameter is set to host value, the VM is deployed on the specified host. Similarly, when this parameter is set to zone, the VM is deployed in the specified available zone. The zone or host placement option is for an entire VM group. During the VPC deployment, each VM (CF or SF) is deployed as a separate VM group.

Important You can specify either a host or a zone value for placement of VMs.

If a specified host or a zone does not exist on the VIM, the deployment fails.

Anti-affinity placement can be used with the availability zone.

Availability zone or host placement is supported for the traditional EM-based VPC deployments and ETSI SOL003 flows. For configuration details related to the EM-based VPC deployments, contact your Cisco Accounts representative team.



CHAPTER 8

Buffer Usage Reduction on TCP Slow Start

- Feature Summary and Revision History, on page 27
- Feature Changes, on page 27

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	VPC-DI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not applicable
Related Documentation	*VPC-DI System Administration Guide*

Revision History

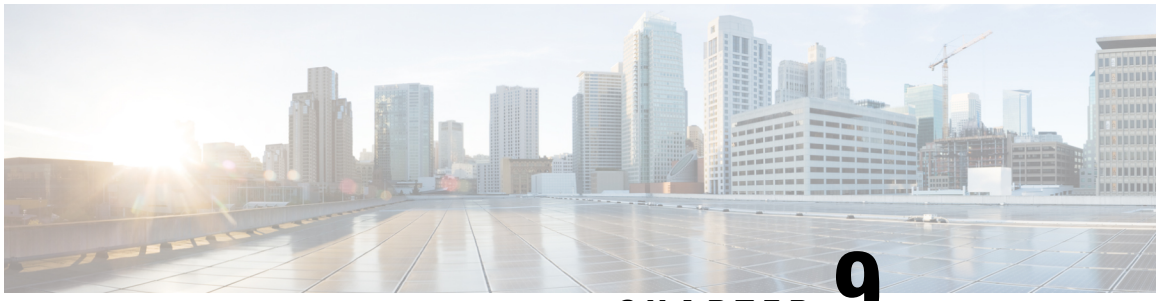
Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
With this release, the TCP parameters are modified to reduce buffer overflow.	21.14.10
First introduced.	Pre 21.2

Feature Changes

Previous Behavior: In releases earlier to 21.14.x, the TCP slow start after idle time does not transfer the data from the buffer, thereby causing a buffer overflow.

New Behavior: From this release onwards, the TCP slow start is implemented only for the first TCP transfer. The TCP parameters are modified to reduce buffer overflow.



CHAPTER 9

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

- Feature Summary and Revision History, on page 29
- Overview, on page 30
- How Cisco Ultra Traffic Optimization Works, on page 31
- Configuring Cisco Ultra Traffic Optimization, on page 34
- Multi-Policy Support for Traffic Optimization, on page 39
- Monitoring and Troubleshooting, on page 52

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • Ultra Gateway Platform
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

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

Revision Details	Release
The Cisco Ultra Traffic Optimization library version has been upgraded from 3.0.9 to 3.0.11.	21.14.2
With this release, new keywords **large-flows-only** and **managed-large-flows-only** are implemented as part of the **data-record** command to enable the CUTO library to stream respective statistics to the external server. New bulk statistics are added in support of this enhancement	21.14
With this release, Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.3.17
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.3.x
Multi-Policy support for Cisco Ultra Traffic Optimization solution.	21.6
Cisco Ultra Traffic Optimization solution is supported in Ultra Gateway Platform (UGP).	21.6
Cisco Ultra Traffic Optimization solution is enhanced to support basic Quick UDP Internet Connections (QUIC) UDP traffic along with the existing support for TCP traffic.	21.5
Reboot of chassis is no longer required to enable Cisco Ultra Traffic Optimization related configuration.	21.5
First introduced.	21.2

Overview

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

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

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.
- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

How Cisco Ultra Traffic Optimization Works

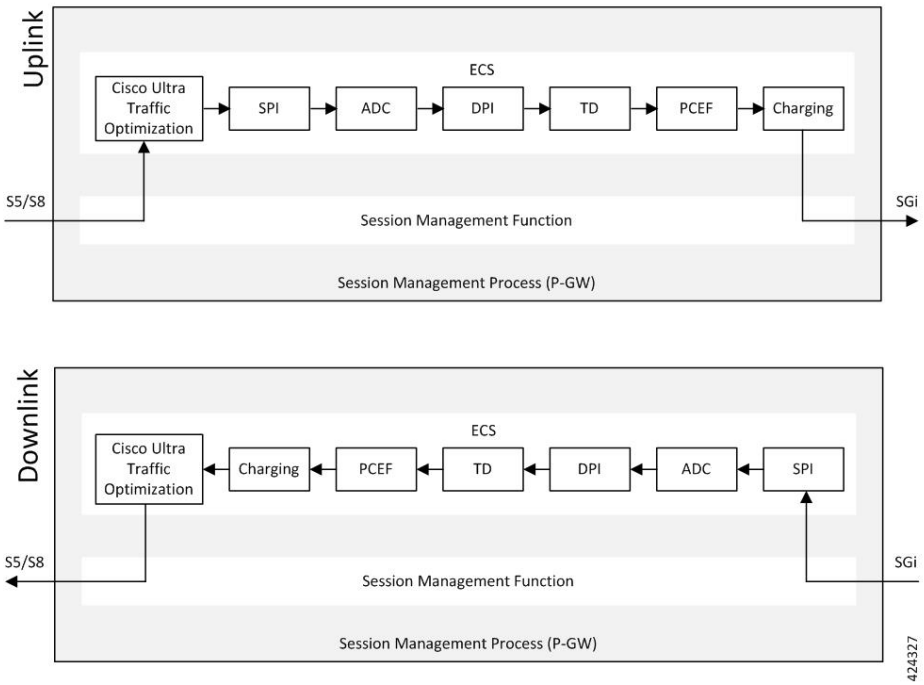
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested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

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

Architecture

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

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



Handling of Traffic Optimization Data Record

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

List of Attributes and File Format

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

Standard TODR

The following is the format of a Standard TODR:

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

Example:

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

Where:

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

Large TODR

The following is a sample output of a Large TODR.

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

Where:

- *instance_id*: Instance ID.

- *flow_type*: Large flow (1)
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_name*: Identifies the name of the configured traffic optimization policy.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.
- *large_detection_time_ms*: Indicates the timestamp when the flow was detected as Large.
- *avg_burst_rate_kbps*: Indicates the average rate in Kbps of all the measured bursts.
- *avg_eff_rate_kbps*: Indicates the average effective rate in Kbps.
- *final_link_peak_kbps*: Indicates the highest detected link peak over the life of the Large flow.
- *recovered_capacity_bytes*: Indicates the recovered capacity in Kbps for this Large flow.
- *recovered_capacity_ms*: Indicates the timestamp of recovered capacity for this Large flow.
- *phase_count*: Indicates the Large flow phase count.
- *min_gbr_kbps*: Indicates the Minimum Guaranteed Bit Rate (GBR) in Kbps.
- *max_gbr_kbps*: Indicates the Maximum Guaranteed Bit Rate (MBR) in Kbps.
- *phase_count_record*: Indicates the number of phases present in this record.
- *end_of_phases*: 0 (not end of phases) or 1 (end of phases).
- Large flow phase attributes:
  - *phase_type*: Indicates the type of the phase
  - *phase_start_time_ms*: Indicates the timestamp for the start time of the phase.
  - *burst_bytes*: Indicates the burst size in bytes.
  - *burst_duration_ms*: Indicates the burst duration in milliseconds.
  - *link_peak_kbps*: Indicates the peak rate for the flow during its life.
  - *flow_control_rate_kbps*: Indicates the rate at which flow control was attempted (or 0 if non-flow control phase).
  - *max_num_queued_packets*: Identifies the maximum number of packets queued.
  - *policy_id*: Identifies the traffic optimization policy ID.

Licensing

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

Limitations and Restrictions

- The values which the P-GW chooses to send to the Cisco Ultra Traffic Optimization engine are the values associated from the bearer GBR and bearer MBR.
- In the current implementation, only downlink GBR and MBR are sent to the engine for traffic optimization.
- UDP/QUIC based Traffic Optimization is supported only on PORT 443.

Configuring Cisco Ultra Traffic Optimization

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

Loading Traffic Optimization

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

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

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

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

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

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

Enabling Cisco Ultra Traffic Optimization Configuration Profile

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

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

NOTES:

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

Configuring the Operating Mode

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

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

Notes:

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

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

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

- **Subscriber-base** – This helps in associating subscribers with service-scheme based on the subs-class configuration.
  - **subs-class** – The conditions defined under subs-class enables in classifying the subscribers based on rule base, APN, v-APN name. The conditions can also be defined in combination, and both OR as well as AND operators are supported while evaluating them.

- **Service-scheme** – This helps in associating actions based on trigger conditions which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.
  - **trigger-condition** – For any trigger, the trigger-action application is based on conditions defined under the trigger-condition.
  - **trigger-actions** – Defines the actions to be taken on the classified flow. These actions can be traffic optimization, throttle-suppress, and so on.

Session Setup Trigger

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

Following is a sample configuration:

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

Bearer Creation Trigger

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

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
             exit
```

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

Flow Creation Trigger

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

The following is a sample configuration:

```
configure
   active-charging service service_name
       trigger-action trigger_action_name
           traffic-optimization
           exit
       trigger-condition trigger_condition_name1
           any-match = TRUE
           exit
       trigger-condition trigger_condition_name2
           qci = qci_value
           exit
       trigger-condition trigger_condition_name3
           rule-name = rule_name
           exit
       service-scheme service_scheme_name
           trigger bearer-creation
              priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
              exit
           exit
       subs-class sub_class_name
           apn = apn_name
           exit
       subscriber-base subscriber_base_name
          priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
           end
```

Notes:

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

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

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

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

Generating TODR

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

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

NOTES:

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

Multi-Policy Support for Traffic Optimization

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

This feature includes the following functionalities:

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

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

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

Important Location Change Trigger is not supported with IPSG.

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

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

How Multi-Policy Support Works

Policy Selection

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

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

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

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

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

Deleting a Policy

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

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

Configuring Multi-Policy Support

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

Configuring a Traffic Optimization Profile

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

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

NOTES:

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

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

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

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

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

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

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

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

- **efd-flow-cleanup-interval**: Configures the EFD flow cleanup interval. The interval value is an integer that ranges 10–5000 milliseconds.
- **stats-interval**: Configures the flow statistics collection and reporting interval in seconds. The interval value is an integer that ranges 1–60 seconds.
- **stats-options**: Configures options to collect the flow statistics. It only specifies whether the stream must be a Flow Trace or a Flow Analyst or both, to an external server.

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

Configuring a Traffic Optimization Policy

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

```
configure
  require active-charging
  active-charging service service_name
    [ no ] traffic-optimization-policy policy_name
      bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [ [
backoff-profile [ managed | unmanaged ] [ min-effective-rate effective_rate
 ] | [ min-effective-rate effective_rate ] [ backoff-profile [ managed |
unmanaged ] ] }
       [ no ] bandwidth-mgmt
       curbing-control { max-phases max_phase_value [ rate curbing_control_rate
 [ threshold-rate threshold_rate [ time curbing_control_duration ] ] ] | rate
```

```
curbing_control_rate [ max-phases [ threshold-rate threshold_rate [ time
curbing_control_duration ] ] ] | threshold-rate [ max-phases max_phase_value [
rate curbing_control_rate [ time curbing_control_duration ] ] ] | time [ max-phases
 max_phase_value [ rate curbing_control_rate [ threshold-rate threshold_rate] ] ]
}
        [ no ] curbing-control
        heavy-session { standard-flow-timeout [ threshold threshold_value |
threshold threshold_value [ standard-flow-timeout timeout_value ] }
        [ no ] heavy-session
        link-profile { initial-rate initial_seed_value [ max-rate
max_peak_rate_value [ peak-lock ] ] | max-rate [ initial-rate initial_seed_value
 [ peak-lock ] ] | peak-lock [ initial-rate initial_seed_value [ max-rate
max_peak_rate_value ] ] }
        [ no ] link-profile
        session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
        [ no ] session-params
        end
```

NOTES:

- **no**: Overwrites the configured parameters with default values. The operator must remove all associated policies in a policy profile before deleting a policy profile. Otherwise, the following error message is displayed:

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

- **bandwidth-mgmt**: Configures bandwidth management parameters.
- **backoff-profile**: Determines the overall aggressiveness of the back off rates.
- **managed**: Enables both traffic monitoring and traffic optimization.
- **unmanaged**: Only enables traffic monitoring.
- **min-effective-rate**: Configures minimum effective shaping rate in Kbps. The shaping rate value is an integer ranging 100–10000.
- **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion. The control rate value is an integer ranging 100–10000.
- **curbing-control**: Configures curbing flow control related parameters.
- **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. The maximum phase value is an integer ranging 2–10.
- **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate. The control rate value is an integer ranging 0–10000. To disable the fixed flow control rate, set the flow control rate value to 0.
- **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing. The threshold rate is an integer ranging 100–10000.
- **time**: Configures the duration of a flow control phase in milliseconds. The flow control duration value is an integer ranging 0–600000. To disable flow control, set the flow control duration value to 0.

- **heavy-session**: Configures parameters for heavy-session detection.
- **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows. The timeout value is an integer ranging 100–3000.
- **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed. The threshold value is an integer ranging 0–100000000.
- **link-profile**: Configures link profile parameters.
- **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session. The initial seed value is an integer ranging 100–30000.
- **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session. The max rate value is an integer ranging 100–30000.
- **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.
- **session-params**: Configures session parameters.
- **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic. The TCP ramp-up duration is an integer ranging 0–5000.
- **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic. The UDP ramp-up duration is an integer ranging 0–5000.

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

Traffic Optimization Policy - Default Values

```
Bandwidth-Mgmt:

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

Curbing-Control:

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

Heavy-Session:

   Threshold               : 4000000 (bytes)
   Standard-Flow-Timeout   : 500 (ms)

Link-Profile:

   Initial-Rate            : 7000 (kbps)
   Max-Rate                : 10000 (kbps)
   Peak-Lock               : Disabled

Session-Params:
```

```
Tcp-Ramp-Up              : 5000 (ms)
Udp-Ramp-Up              : 0 (ms)
```

Associating a Trigger Action to a Traffic Optimization Policy

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

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

NOTES:

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

Enabling TCP and UDP

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

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

NOTES:

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

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

Service-Scheme Configuration for Multi-Policy Support

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

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

Session Setup Trigger

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

Use the following configuration to setup a Session Trigger:

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

Sample Configuration

Following is a sample configuration for Session Setup Trigger:

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

Bearer Creation Trigger

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

Use the following configuration to configure a Bearer Creation Trigger:

```
configure
  active-charging service service_name
    service-scheme service_scheme_name
      trigger bearer-creation
```

```
          priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
          exit
        trigger-condition trigger_condition_name2
          qci = qci_value
          exit
        trigger-action bearer-creation
          traffic-optimization policy bearer-creation
          exit
```

Sample Configuration

The following is a sample configuration for Bearer Creation Trigger:

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

Flow Creation Trigger

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

Use the following configuration to configure a flow creation trigger:

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

Sample Configuration

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

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

```
      traffic-optimization
    #exit
```

Configuring: ecgi-change

The following demonstrates ecgi-change sample configuration:

Trigger Condition and Trigger Action in ACS Configuration

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

Service Schema Configuration

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

Local Policy Configuration

```
local-policy-service LP
    ruledef anymatch
      condition priority 1 imsi match *
    #exit
    ruledef ecgi-1
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AE7F0A 1AE7F0B 1AE7F28 1AE7F29
1AE7F46 1AE7F47 1AEAC00 1AEAC01 1AEAC02 1AEAC0A 1AEAC0B 1AEAC0C 1AEAC14 1AEAC15 1AEAC16
1AEAC28 1AEAC29 1AEAC2A 1AEAC46 1AEAC47 1AEAC48 1AEAC50 1AEAC51 1AEAC52 1AEAC6E 1AEAC6F
1AEAC70 1AEAC78 1AEAC79 1AEAC7A
    #exit
    ruledef ecgi-10
      condition priority 1 ecgi mcc 300 mnc 235 eci match 1F36C52 1F36C6E 1F36C6F 1F36C70
1F36C78 1F36C79 1F36C7A
    #exit
    ruledef ecgi-2
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBE01 1AEBE02 1AEBE0B 1AEBE0C
1AEBE15 1AEBE16 1AEBE29 1AEBE2A 1AEBE47 1AEBE48 1AEBF00 1AEBF01 1AEBF02 1AEBF0A 1AEBF0B
1AEBF0C 1AEBF14 1AEBF15 1AEBF16 1AEBF1E 1AEBF1F 1AEBF20 1AEBF28 1AEBF29 1AEBF2A 1AEBF46
    #exit
    ruledef ecgi-3
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBF47 1AEBF48 1AEBF50 1AEBF51
1AEBF52 1AEBF6E 1AEBF6F 1AEBF70 1AEBF78 1AEBF79 1AEBF7A 1AF0E00 1AF0E01 1AF0E02 1AF0E0A
1AF0E0B 1AF0E0C 1AF0E14 1AF0E15 1AF0E16 1AF0E28 1AF0E29 1AF0E2A 1AF0E46
    #exit
    ruledef ecgi-4
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF0E47 1AF0E48 1AF4A0A 1AF4A0B
```

```
1AF4A14 1AF4A15 1AF4A28 1AF4A29 1AF4A46 1AF4A47 1AF4D00 1AF4D01 1AF4D0A 1AF4D0B 1AF4D14
1AF4D15 1AF4D28 1AF4D29 1AF4D46 1AF4D47 1AF4D50 1AF4D51 1AF4D6E 1AF4D6F
    #exit
    ruledef ecgi-5
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF4D78 1AF4D79 1AF7200 1AF7201
1AF7202 1AF720A 1AF720B 1AF720C 1AF7214 1AF7215 1AF7216 1AF721E 1AF721F 1AF7444 1AF7228
1AF7229 1AF722A 1AF7246 1AF7247 1AF7248 1AF7250 1AF7251 1AF7252 1AF726E
    #exit
    ruledef ecgi-6
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF726F 1AF7270 1B04C00 1B04C01
1B04C02 1B04C03 1B04C0A 1B04C0B 1B04C0C 1B04C0D 1B04C14 1B04C15 1B04C16 1B04C17 1B04C1E
1B04C1F 1B04C20 1B04C21 1B04C28 1B04C29 1B04C2A 1B04C2B 1B04C46 1B04C47
    #exit
    ruledef ecgi-7
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B04C48 1B04C49 1B04C50 1B04C51
1B04C52 1B04C53 1B04C6E 1B04C6F 1B04C70 1B04C71 1B04C78 1B04C79 1B04C7A 1B04C7B 1B05300
1B05301 1B05302 1B0530A 1B0530B 1B0530C 1B05314 1B05315 1B05316 1B05328 1B05329
    #exit
    ruledef ecgi-8
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B0532A 1B05346 1B05347 1B05348
1B32F00 1B32F01 1B32F02 1B32F0A 1B32F0B 1B32F0C 1B32F14 1B32F15 1B32F16 1B32F28 1B32F29
1B32F2A 1B32F46 1B32F47 1B32F48 1B76400 1B76401 1B76402 1B7640A 1B7640B 1B7640C 1B76428
    #exit
    ruledef ecgi-9
      condition priority 1 ecgi mcc 111 mnc 444 eci match 1B76429 1B7642A 1B76446 1B76447
1B76448 1F36C00 1F36C01 1F36C02 1F36C0A 1F36C0B 1F36C0C 1F36C14 1F36C15 1F36C16 1F36C1E
1F36C1F 1F36C20 1F36C28 1F36C29 1F36C2A 1F36C46 1F36C47 1F36C48 1F36C50 1F36C51
    #exit
    actiondef activate_lp_action
      action priority 1 activate-lp-rule name ruledef-tai
    #exit
    actiondef activate_lp_action1
      action priority 3 event-triggers ecgi-change
    #exit
    actiondef ecgi_change
      action priority 1 activate-lp-rule name ruledef-ecgi
    #exit
    eventbase default
     rule priority 1 event new-call ruledef anymatch actiondef activate_lp_action1 continue

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

Traffic Optimization Policy Configuration

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

Local Policy Configuration

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

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

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

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

Service-Scheme Configuration

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

```
    traffic-optimization policy policy_name
    exit
```

Configuring L7 Rule

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

Use the following CLI to configure an L7 rule:

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

Sample Configuration

The following is a sample configuration for L7 Rules:

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

Ookla Speedtest

Use the configuration information discussed in the sectionConfiguring L7 Rule, on page 50.

Sample Configuration

The following is a sample configuration for Ookla Speedtest:

```
 service-scheme SS1
      trigger flow-create
        priority 1 trigger-condition ookla trigger-action ookla
      #exit
    trigger-condition ookla
      rule-name = speedtest
```

```
    #exit
    trigger-action ookla
      no traffic-optimization
    #exit
```

Location and App-based Configuration

Sample Configuration

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

Selective Configuration by Disabling TCP and UDP

Sample Configuration

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

L7/ADC and Location Trigger based Configuration

Sample Configuration

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

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

```
Service Scheme Configuration:
service-scheme SS1
trigger flow-create
  priority 1 trigger-condition speedtest-tc trigger-action speedtest-ta
  priority 2 trigger-condition location-tc trigger-action location-ta
```

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

Monitoring and Troubleshooting

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

Cisco Ultra Traffic Optimization Show Commands and/or Outputs

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

show active-charging traffic-optimization counters

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

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

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

Following are the new field/counters:

- Traffic Optimization Flows:
  - Active Normal Flow Count:
  - Active Large Flow Count:
  - Active Managed Large Flow Count:
  - Active Unmanaged Large Flow Count:
  - Total Normal Flow Count:

- Total Large Flow Count:
- Total Managed Large Flow Count:
- Total Unmanaged Large Flow Count:
- Total IO Bytes:
- Total Large Flow Bytes:
- Total Recovered Capacity Bytes:
- Total Recovered Capacity ms:

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

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

- TCP Traffic Optimization Flows:
  - Active Normal Flow Count:
  - Active Large Flow Count:
  - Active Managed Large Flow Count:
  - Active Unmanaged Large Flow Count:
  - Total Normal Flow Count:
  - Total Large Flow Count:
  - Total Managed Large Flow Count:
  - Total Unmanaged Large Flow Count:
  - Total IO Bytes:
  - Total Large Flow Bytes:
  - Total Recovered Capacity Bytes:
  - Total Recovered Capacity ms:

- UDP Traffic Optimization Flows:
  - Active Normal Flow Count:
  - Active Large Flow Count:
  - Active Managed Large Flow Count:
  - Active Unmanaged Large Flow Count:
  - Total Normal Flow Count:
  - Total Large Flow Count:

- Total Managed Large Flow Count:
- Total Unmanaged Large Flow Count:
- Total IO Bytes:
- Total Large Flow Bytes:
- Total Recovered Capacity Bytes:
- Total Recovered Capacity ms:

show active-charging traffic-optimization info

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

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

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

Following are the new fields/counters:

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

show active-charging traffic-optimization policy

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

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

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

Bulk Statistics

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

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

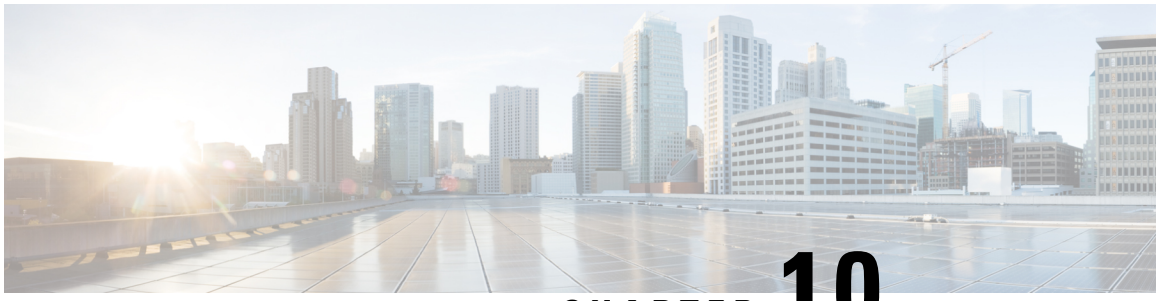
Bulk Statistics	Description
tcp-total-io-bytes	Indicates the number of TCP total-IO bytes for Cisco Ultra Traffic Optimization.
tcp-total-large-flow-bytes	Indicates the number of TCP total-large-flow bytes for Cisco Ultra Traffic Optimization.
tcp-total-recovered-capacity-bytes	Indicates the number of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

Bulk Statistics	Description
tcp-uplink-hold	Indicates the number of TCP uplink-hold for Cisco Ultra Traffic Optimization.
tcp-uplink-forward	Indicates the number of TCP uplink-forward for Cisco Ultra Traffic Optimization.
tcp-uplink-forward-and-hold	Indicates the number of TCP uplink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-uplink-hold-failed	Indicates the number of TCP uplink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-uplink-bw-limit-flow-sent	Indicates the number of TCP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-drop	Indicates the number of TCP downlink-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold	Indicates the number of TCP downlink-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward	Indicates the number of TCP downlink-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-forward-and-hold	Indicates the number of TCP downlink-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-hold-failed	Indicates the number of TCP downlink-hold-failed for Cisco Ultra Traffic Optimization.
tcp-dnlink-bw-limit-flow-sent	Indicates the number of TCP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-drop	Indicates the number of TCP downlink-async-drop for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold	Indicates the number of TCP downlink-async-hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward	Indicates the number of TCP downlink-async-forward for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-forward-and-hold	Indicates the number of TCP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
tcp-dnlink-async-hold-failed	Indicates the number of TCP downlink-async-hold-failed for Cisco Ultra Traffic Optimization.
tcp-process-packet-drop	Indicates the number of TCP process-packet-drop for Cisco Ultra Traffic Optimization.
tcp-process-packet-hold	Indicates the number of TCP process-packet-hold for Cisco Ultra Traffic Optimization.

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

Bulk Statistics	Description
udp-uplink-bw-limit-flow-sent	Indicates the number of UDP uplink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-drop	Indicates the number of UDP downlink-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-hold	Indicates the number of UDP downlink-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-forward	Indicates the number of UDP downlink-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-forward-and-hold	Indicates the number of UDP downlink-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-hold-failed	Indicates the number of UDP downlink-hold failed for Cisco Ultra Traffic Optimization.
udp-dnlink-bw-limit-flow-sent	Indicates the number of UDP downlink-bw limit-flow sent for Cisco Ultra Traffic Optimization.
udp-dnlink-async-drop	Indicates the number of UDP downlink-async-drop for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold	Indicates the number of UDP downlink-async-hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward	Indicates the number of UDP downlink-async-forward for Cisco Ultra Traffic Optimization.
udp-dnlink-async-forward-and-hold	Indicates the number of UDP downlink-async-forward and hold for Cisco Ultra Traffic Optimization.
udp-dnlink-async-hold-failed	Indicates the number of UDP downlink-async-hold failed for Cisco Ultra Traffic Optimization.
udp-process-packet-drop	Indicates the number of UDP process-packet-drop for Cisco Ultra Traffic Optimization.
udp-process-packet-hold	Indicates the number of UDP process-packet-hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward	Indicates the number of UDP process-packet-forward for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-failed	Indicates the number of UDP process-packet-forward failed for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold	Indicates the number of UDP process-packet-forward and hold for Cisco Ultra Traffic Optimization.
udp-process-packet-forward-and-hold-failed	Indicates the number of UDP process-packet-forward and hold failed for Cisco Ultra Traffic Optimization.

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



CHAPTER 10

Cisco Ultra Traffic Optimization Library Version Upgrade

This chapter describes the following topics:

- Feature Summary and Revision History, on page 61
- Feature Changes, on page 62

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	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

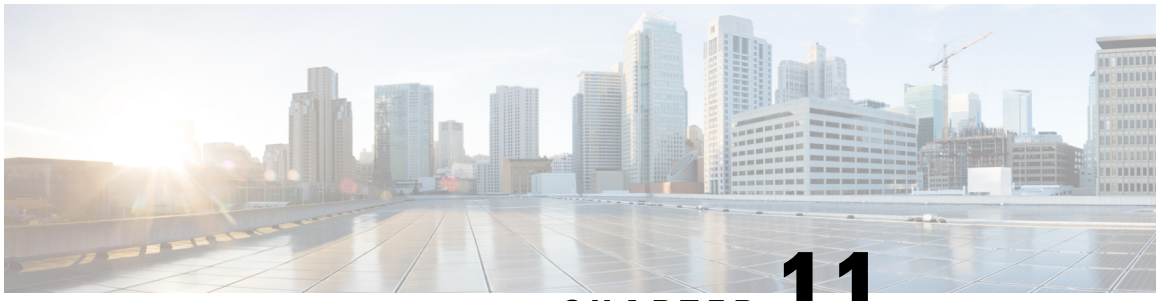
Revision Details	Release
The Cisco Ultra Traffic Optimization library version has been upgraded from 3.0.9 to 3.0.11.	21.14.2
First introduced.	21.14

Feature Changes

Previous Behavior: In earlier releases, the Cisco Ultra Traffic Optimization library version 3.0.9 was supported.

New Behavior: The Cisco Ultra Traffic Optimization library version is upgraded from 3.0.9 to 3.0.11.

Note Please ensure that the latest library version is installed on both Active and Standby chassis to avoid technical discrepancies.



CHAPTER 11

Co-Located SPGW Selection for Emergency Bearer

This chapter describes the following topics:

- Feature Summary and Revision History, on page 63
- Feature Changes, on page 64
- Command Changes, on page 64
- Performance Indicator Changes, on page 64

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First Introduced.	21.14.8

Feature Changes

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

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

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

Command Changes

pgw co-location

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

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

NOTES:

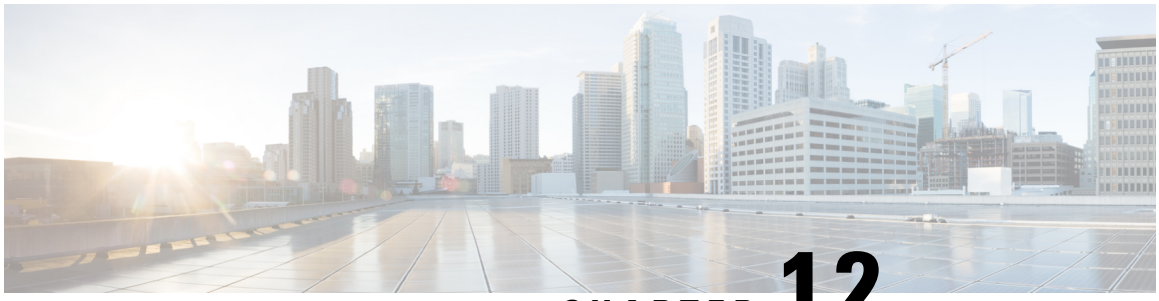
- **no** Disables the P-GW co-location configuration.
- **co-location** Configures to select the co-located S-GW/P-GW node based on static P-GW configuration and S-GW selected through DNS.

Performance Indicator Changes

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

The output of this command includes the following fields:

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



CHAPTER 12

Collision Handling of Last PDN Disconnect Connection Establishment

This chapter describes the following topics:

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

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
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
First introduced.	21.14.16

Feature Changes

Previous Behavior: When MME has only one PDN in connected state and a new PDN connection establishment is in progress, and if the MME receives a PDN disconnect for previously existing PDN, MME will reject PDN disconnect with cause 49.

New Behavior: MME will not reject the PDN Disconnect request, It will process the 2nd PDN connection establishment first, and then proceed with 1st PDN disconnection. A new CLI command **last-pdn-disconnect** is added in the MME Service Configuration mode to enable/disable this functionality.

Command Changes

Enabling PDN Disconnect by UE

Use the following configuration to enable PDN disconnect by UE.

```
configure
     context context_name
       mme-service mme_service_name
          [ no ] last-pdn-disconnect
          end
```

NOTES:

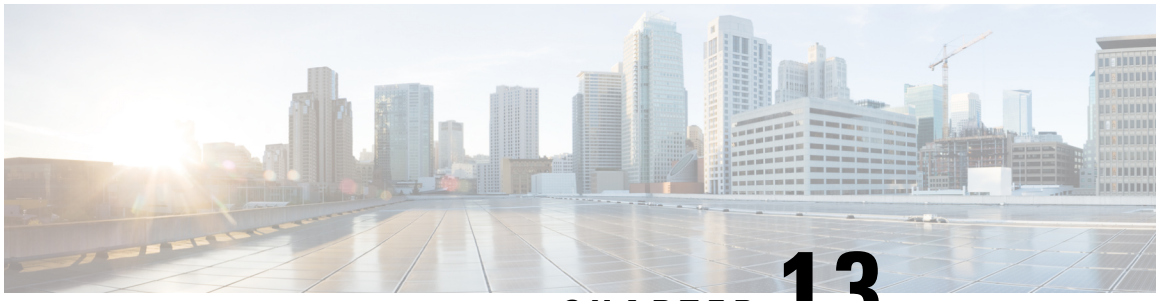
- **no**: Removes the PDN disconnect by UE configuration.
- **last-pdn-disconnect**: Allows the last PDN disconnection by UE while another PDN is under establishment.

Performance Indicator Changes

show mme-service all

The output of this command includes the following fields:

- Last PDN Disconnect by UE while another PDN is under establishment - Indicates whether Last PDN Disconnect by UE while another PDN is under establishment is enabled or disabled.



CHAPTER 13

Collision Handling for Path Update during Bearer Creation

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

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

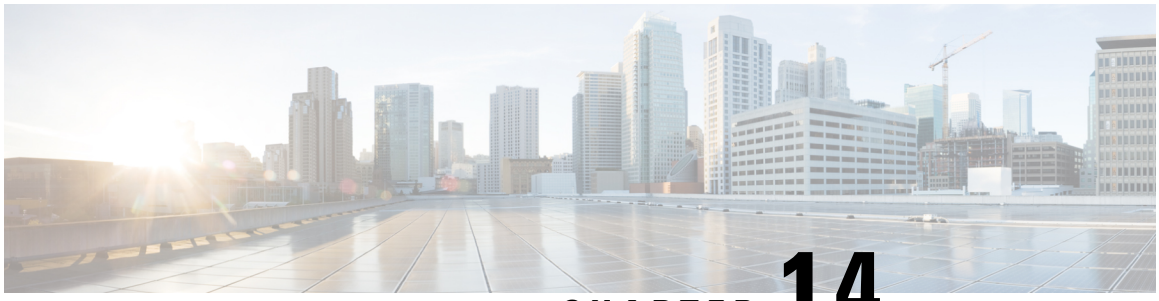
Feature Description

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 14

ConfD Upgrade Support

- Feature Summary and Revision History, on page 69
- Feature Description, on page 70

Feature Summary and Revision History

Summary Data

sion 6.3 to

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* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

Revision History

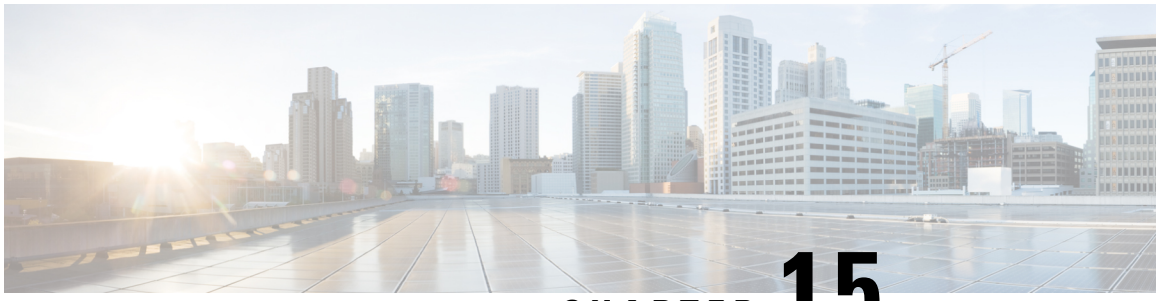
Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
With this release, ConfD is upgraded from Version 6.3 to Version 7.1.	21.14

Revision Details	Release
First introduced.	Pre 21.2

Feature Description

In Release 21.14, ConfD is upgraded from Version 6.3 to Version 7.1.



CHAPTER 15

Dedicated Core Networks on MME

This chapter describes the Dedicated Core Networks feature in the following sections:

- Feature Summary and Revision History, on page 71
- Feature Description, on page 73
- How It Works, on page 75
- Configuring DECOR on MME, on page 83
- Monitoring and Troubleshooting, on page 88

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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
In release 21.14, the DECOR feature is enhanced to support: • P-GW Selection based on ULAs UE Usage Type • Usage Type Deletion by DSR flag support added.	21.14
In release 21.8, the DECOR feature is enhanced to support: • Association of DCNs to a specific RAT Type under call-control-profile • Association of multiple DCN profiles (to designate dedicated or default core network) under call-control-profile • DNS selection of S-GW / P-GW / MME / S4-SGSN/ MMEGI lookup for specified UE Usage Type or DCN-ID • DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE result code for the S6a (HSS) interface • When UE moves from a service area where DCN is not used to another area where DCN is supported, then MME does not receive the UE-Usage-Type from peer. In this case, MME will do an explicit AIR towards HSS for UE-Usage lookup.	21.8
The enhancements to the DECOR feature in release 21.6 are fully qualified.	21.7
The enhancements to the DECOR feature in release 21.6 are not fully qualified and are available only for testing purposes. In release 21.6, the DECOR feature is enhanced to support: • DNS based MMEGI selection • DCN-ID IE in Attach/TAU Accept and GUTI Reallocation Command message towards UE • DCN-ID IE in INITIAL UE MESSAGE from eNodeB • HSS initiated DCN reselection • MME initiated DCN reselection • Network sharing with same MMEGI for different PLMNs • Network sharing with different MMEGIs for different PLMNs • Served DCNs Items IE in S1 Setup Response and MME Configuration Update messages towards eNodeBs	21.6
First introduced.	21.4

Feature Description

The Dedicated Core (DECOR) Networks feature allows an operator to deploy one or more dedicated core network within a PLMN, with each core network dedicated for a specific type of subscriber. The specific dedicated core network that serves a UE is selected based on subscription information and operator configuration, without requiring the UEs to be modified. This feature aims to route and maintain UEs in their respective DCNs.

The DECOR feature can either provide specific characteristics and functions to the UE or subscriber, or isolate them to a UE or subscriber. For example, Machine-to-Machine (M2M) subscribers, subscribers belonging to a specific enterprise or separate administrative domain, and so on.

Overview

Dedicated Core Networks (DCN) enable operators to deploy multiple core networks consisting of one or more MME/SGSN and optionally one or more S-GW/P-GW/PCRF.

If a network deploys a DCN selection based on both LAPI indication and subscription information (MME/SGSN), then DCN selection based on the subscription information provided by MME/SGSN overrides the selection based on the Low Access Priority Indication (LAPI) by RAN.

A new optional subscription information parameter, **UE Usage Type**, stored in the HSS, is used by the serving network to select the DCNs that must serve the UE. The operator can configure DCNs and its serving UE Usage Type as required. Multiple UE Usage Types can be served by the same DCN. The HSS provides the UE Usage Type value in the subscription information of the UE to the MME/SGSN/MSC. The serving network chooses the DCN based on the operator configured (UE Usage Type to DCN) mapping, other locally configured operator's policies, and the UE related context information available at the serving network.

Note One UE subscription can be associated only with a single UE Usage Type, which describes its characteristics and functions.

External Interfaces

The following components are enhanced to support the DECOR feature on the MME:

DNS

S-GW or P-GW Selection

MME performs S-GW or P-GW selection from DCNs serving UE Usage Type or DCN-ID, based on the configuration in the decor profile.

The existing service parameters of the SNAPTR records are enhanced by appending the character string "+ue-<ue usage type>" or "+ue-<dcn-id>" to the "app-protocol" name identifying the UE usage type(s) or DCN-ID for which the record applies.

For example: S-GW service parameter — x-3gpp-sgw:x-s11+ue-1.10.20 will represent the S-GW which is part of a DCN serving UE usage types or DCN-ID 1, 10, and 20.

For example: P-GW service parameter — x-3gpp-pgw:x-s5-gtp+ue-1.10.20:x-s8-gtp+ue-1.10.20 will represent the P-GW which is part of a DCN serving UE usage types or DCN-ID 1, 10, and 20.

MMEGI Retrieval

MME uses local configuration for MMEGI corresponding to the UE Usage Type and DNS SNAPTR procedures.

The configuration options for static (local) or DNS or both are provided under decor-profile. If both options are enabled, then DNS is given preference. When DNS lookup fails, static (local) value is used as fallback.

To retrieve the MMEGI identifying the DCN serving a particular UE usage type, the SNAPTR procedure uses the Application-Unique String set to the TAI FQDN. The existing service parameters are enhanced by appending the character string "+ue-<ue usage type>" or "+ue-<dcn-id>" to the "app-protocol" name identifying the UE usage type for which the discovery and selection procedures are performed.

For example: MME will discover the MMEGI for a particular UE usage type or DCN-ID by using the "Service Parameters" of "x-3gpp-mme:x-s10+ue-<ue usage type>" or "x-3gpp-mme:x-s10+ue-<dcn-id>". The service parameters are enhanced to identify the UE usage type(s) for which the record applies. The MMEGI will be provisioned in the host name of the records and MMEGI will be retrieved from the host name.

MME or S4-SGSN Selection

To perform MME/S4-SGSN selection from the same DCN during handovers, the existing service parameters are enhanced by appending the character string "+ue-<ue usage type>" or "+ue-<dcn-id>" to the "app-protocol" name identifying the UE usage type.

If the MME fails to find a candidate list for the specific UE Usage Type, it falls back to the legacy DNS selection procedure.

For example:

For an MME to find a candidate set of target MMEs — "x-3gpp-mme:x-s10+ue-<ue usage type>" or "x-3gpp-mme:x-s10+ue-<dcn-id>"

For an MME to find a candidate set of target SGSNs — "x-3gpp-sgsn:x-s3+ue-<ue usage type>" or "x-3gpp-sgsn:x-s3+ue-<dcn-id>"

Note I-RAT handovers between MME and Gn-SGSN is not supported in this release.

S6a (HSS) Interface

To request the UE Usage Type from HSS, MME sets the "Send UE Usage Type" flag in the AIR-Flags AVP, in the AIR command.

The AIR-Flag is set only if the **decor s6a ue-usage-type** CLI command is enabled under MME-service or Call-Control-Profile.

HSS may include the UE-Usage-Type AVP in the AIA response command in the case of DIAMETER_SUCCESS or DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE result code. MME will store the UE Usage Type in the UE context for both the result codes.

GTPv2 (MME or S4-SGSN)

MME supports the UE Usage Type IE in Identification Response, Forward Relocation Request, and Context Response Messages. If the subscribed UE Usage Type is available, it will be set to the available value, otherwise the MME encodes the length field of this IE with 0.

Similarly, MME will parse and store the UE Usage Type value when received from the peer node.

How It Works

MME obtains the UE Usage type and determines the MMEGI that serves the corresponding DCN.

The MME then compares this MMEGI with its own MMEGI to perform a reroute or process further. In case of reroute, the request message is redirected to the appropriate MME. Refer to the ATTACH/TAU Procedure, on page 77 call flow for more information.

The following deployment scenarios are supported when DECOR is enabled on the MME:

- MME can be deployed where the initial request is sent by RAN (eNodeB) when sufficient information is not available to select a specific DCN.
- MME can be deployed as a part of DCN to serve one or more UE Usage Types.
- MME can be deployed as part of a Common Core Network (CCN) or Default Core Network, to serve UE Usage Types for which specific DCN is not available.

Note An MME can service initial RAN requests and also be a part of a DCN or a CCN. However, a particular MME service can only belong to one DCN or CCN within a PLMN domain.

The Dedicated Core Network implements the following functionalities on the MME:

- NAS Message Redirection
- ATTACH and TAU and Handover Procedures
- UE Usage Type support on S6a and GTPv2 interfaces
- S-GW/P-GW DNS selection procedures with UE Usage Type or DCN-ID
- MME/S4-SGSN selection procedures with UE Usage Type or DCN-ID during handovers
- Roaming
- Network Sharing
- DNS based MMEGI selection with UE-Usage-Type or DCN-ID
- DCN ID Support
- HSS/MME initiated DCN reselection
- When UE moves from a service area where DCN is not used to another area where DCN is supported, then MME does not receive the UE-Usage-Type from peer. In this case, MME will do an explicit AIR towards HSS for UE-Usage lookup.

Flows

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

- P-GW Selection based on ULAs UE Usage Type, on page 76
- UE Assisted Dedicated Core Network Selection, on page 76
- NAS Message Redirection Procedure, on page 76
- ATTACH/TAU Procedure, on page 77
- HSS Initiated Dedicated Core Network Reselection, on page 80

P-GW Selection based on ULAs UE Usage Type

MME considers only the UE Usage Type received in ULA for gateway selection and UUT (UE Usage Type) received from peer MME/SGSN including reroute scenarios or in AIA message from HSS or locally configured UUT will not be considered. This feature can disabled or enabled by CLI, It is disabled by default.

UE Assisted Dedicated Core Network Selection

The UE assisted Dedicated Core Network Selection feature selects the correct DCN by reducing the need for DECOR reroute by using DCN-ID sent from the UE and DCN-ID used by RAN.

1. The DCN-ID will be assigned to the UE by the serving PLMN and is stored in the UE per PLMN-ID. Both standardized and operator specific values for DCN-ID are acceptable. The UE will use the PLMN specific DCN-ID whenever it is stored for the target PLMN.
2. The HPLMN may provision the UE with a single default standardized DCN-ID that will be used by the UE only if the UE has no PLMN specific DCN-ID of the target PLMN. When a UE configuration is changed with a new default standardized DCN-ID, the UE will delete all stored PLMN specific DCN-IDs.
3. The UE provides the DCN-ID to RAN at registration to a new location in the network, that is, in Attach, TAU, and RAU procedures.
4. RAN selects the serving node MME based on the DCN-ID provided by UE and configuration in RAN. For E-UTRAN, the eNodeB is conveyed with DCNs supported by the MME during setup of the S1 connection in S1 Setup Response.

UE Usage Type Deletion by DSR Flag

MME processes the User Equipment (UE) Usage Type if it is set in Dynamic Source Routing flag in the Delete Subscriber data at the Home Subscriber Server. MME initiates the 3GPP standard(23.401 section 5.19.3) procedure to redirect Network Access Storage (NAS)/UE if necessary.

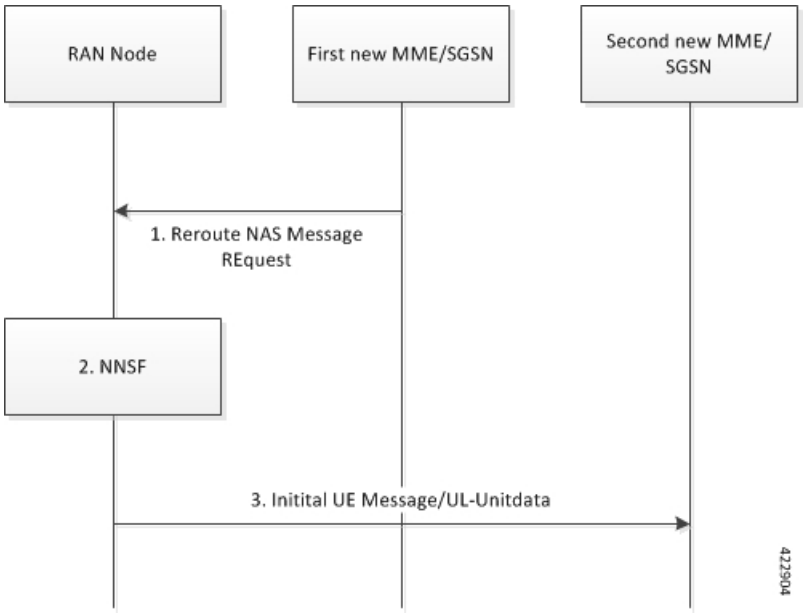
NAS Message Redirection Procedure

Reroute NAS message is used to reroute a UE from one CN node to another CN node during Attach, TAU, or RAU procedure. This is also used by the MME/SGSN or HSS initiated Dedicated Core Network Reselection procedure.

When the first MME determines the UE Usage Type, it fetches the DCN configuration serving the UE and the corresponding MMEGI (from configuration or DNS). If the MME's MMEGI is not the same as the MMEGI of the DCN, MME moves the UE to another MME using the NAS messaging redirection procedure.

The following call flow illustrates the NAS Message Redirection procedure:

Figure 1: NAS Message Redirection Procedure

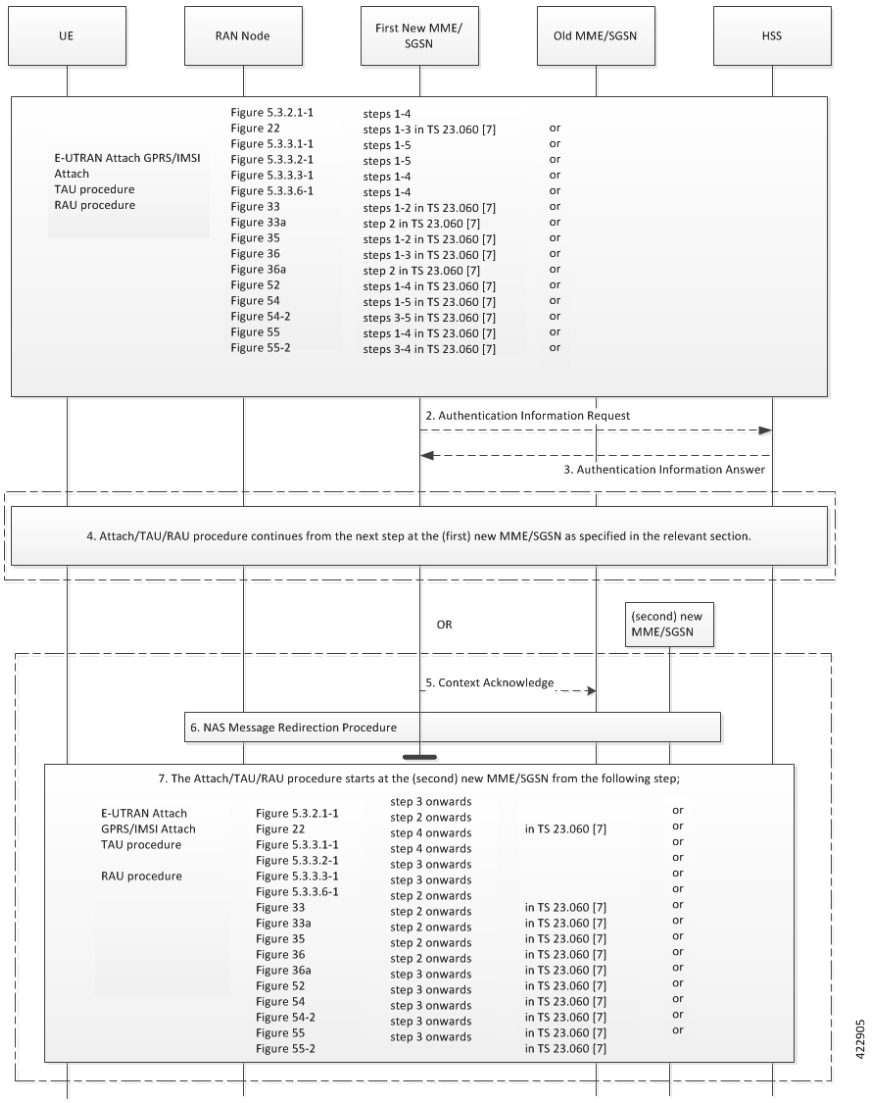


Step	Description
1	The first new MME sends a Reroute NAS Message Request to eNodeB including UE Usage Type and MMEGI among other parameters.
2	RAN selects a new MME based on MMEGI. If no valid MME can be obtained from MMEGI, it selects MME from the CCN or forwards to the same first MME.
3	The second new MME determines from the MMEGI field if the incoming request is a re-routed NAS request or not. Now, if the received MMEGI belongs to the second MME, the call is serviced, else the call is rejected. No further rerouting is performed. If the UE Usage Type is received by the second MME, it is used for S-GW/P-GW selection.

ATTACH/TAU Procedure

The following figure illustrates a detailed flow of the ATTACH or TAU procedure.

Figure 2: ATTACH and TAU Procedure



Step	Description
1	In the RRC Connection Complete message transferring the NAS Request message, the UE provides the DCN-ID, if available. If the UE has a PLMN specific DCN-ID. the UE provides this value and if no PLMN specific DCN-ID exists, then the pre-provisioned default standardized DCN-ID will be provided, if pre-provisioned in the UE. The RAN node selects a DCN and a serving MME/SGSN within the network of the selected core network operator based on the DCN-ID and configuration in the RAN node. The NAS Request message is sent to the selected node. The DCN-ID is provided by the RAN to the MME/SGSN together with the NAS Request message.

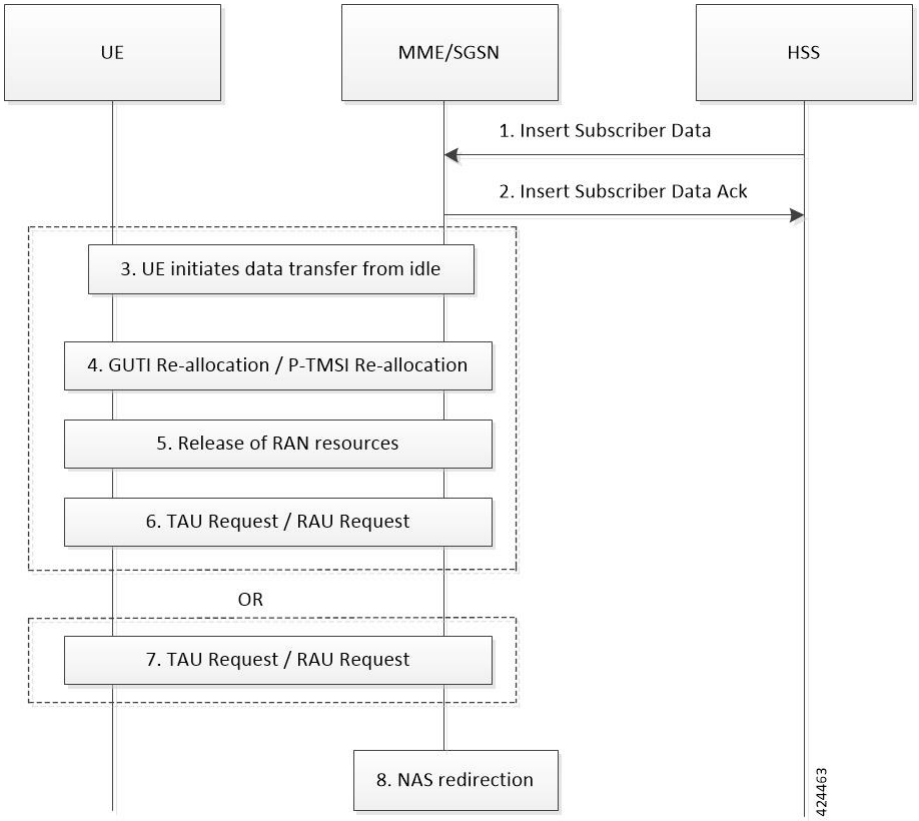
Step	Description
2	The first new MME does not receive the MMEGI from eNodeB. The MME determines the UE Usage Type as follows: **1.** It may receive the UE Usage Type from the peer MME/S4-SGSN. **2.** It may determine from the locally available UE context information. **3.** It sends an AIR message to the HSS requesting the UE Usage Type by adding the parameter "Send UE Usage Type" flag in the message. If authentication vectors are available in the database or received from peer, MME will not send the Immediate-Response-Preferred flag in the AIR message. **4.** It may determine from the local configuration.
3	When UE Usage Type is available, and if the MME has to send an AIR message to the HSS to fetch authentication vectors, then the “Send UE Usage Type” flag is not set in the AIR message.
4	The first new MME determines to handle the UE: **1.** When there is a configured DCN and the first new MME belongs to the MMEGI serving the DCN. **2.** It will continue with the call flow. **3.** The MME/SGSN sends the DCN-ID, if available, for the new DCN to the UE in the NAS Accept message. The UE updates its stored DCN-ID parameter for the serving PLMN if DCN-ID for serving PLMN is changed.
5	The first new MME determines to reject the UE: **1.** When UE Usage Type is available but without a matching DCN. **2.** The NAS message is rejected with parameters (for example: T3346 backoff timer) such that the UE does not immediately re-initiate the NAS procedure.
6	The first new MME determines to reroute the UE: **1.** When there is a configured DCN and the first new MME does not belong to the MMEGI. **2.** The first new MME sends a Context Acknowledge message with cause code indicating that the procedure is not successful. The old MME/SGSN will continue as if Context Request was never received. **3.** The first new MME performs the NAS redirection procedure and the request may be routed by RAN to a second new MME.
7	The second new MME determines to handle the UE or reject it; the MME does not perform another re-route. The process of handling the UE or rejecting the UE is similar to the procedure used in the case of the first new MME. The second new MME does not fetch the UE Usage Type from HSS. It is received either from the RAN node or the old MME.

HSS Initiated Dedicated Core Network Reselection

This procedure is used by the HSS to update (add, modify, or delete) the UE Usage Type subscription parameter in the serving node. This procedure may result in change of serving node of the UE.

The following call flow illustrates the HSS Initiated DCN Reselection procedure.

Figure 3: HSS Initiated Dedicated Core Network Reselection Procedure



Step	Description
1	The HSS sends an Insert Subscriber Data Request (IMSI, Subscription Data) message to the MME. The Subscription Data includes the UE Usage Type information.
2	The MME updates the stored Subscription Data and acknowledges the Insert Subscriber Data Request message by returning an Insert Subscriber Data Answer (IMSI) message to the HSS. The procedure ends if the MME/SGSN continues to serve the UE.

Step	Description
As per this callflow, one of the following steps occur: • Steps 3 through 6 occur in case the UE is already in connected mode or UE enters connected mode by initiating data transfer. • Step 7 occurs in case the UE is in idle mode and performs a TAU/RAU procedure. **Important** Paging is not supported in this release. If the UE is in idle mode, MME waits until the UE becomes active.	
3	The UE initiates NAS connection establishment either by uplink data or by sending a TAU/RAU Request.
4	The MME triggers the GUTI re-allocation procedure and includes a non-broadcast TAI.
5	The MME releases RAN resources and UE is moved to idle mode.
6	The non-broadcast TAI triggers the UE to immediately start the TAU procedure. The MME receives the TAU Request message.
7	The UE performs a TAU request. The MME receives the TAU Request message
8	The MME triggers the NAS Message redirection procedure to redirect the UE if: • the UE Usage Type for the UE has been added or modified and if it is not served by the MME • the UE Usage Type has been withdrawn from the HSS subscription data and subscriptions without UE Usage Type are not served by the MME **Note** HSS Initiated UE Usage Type withdrawal is not supported. The addition or change in usage type is supported.

Impact to Handover Procedures

This section describes the impact during handover procedures:

- In a forward relocation request, the source MME includes the UE-Usage-Type, if available.
- If an S-GW needs to be relocated, MME applies the UE-Usage-Type or DCN-ID based DNS selection, that is similar to the Attach/TAU procedure.
- MME or S4-SGSN selection during handover considers UE-Usage-Type or DCN-ID.
- The following two scenarios apply to DCNs deployed partially or heterogeneously:
  - Handover from service area where DCN is not used to an area where DCN is supported. In this case, MME does not receive the UE-Usage-Type from peer and MME does an Explicit AIR towards HSS for UE-Usage lookup.
  - The target MME or SGSN obtains the UE-Usage-Type information from the HSS during the subsequent TAU or RAU procedure.

- If the target MME/SGSN determines that the S-GW does not support the UE-Usage-Type, the target MME/SGSN must trigger the S-GW relocation as part of the handover procedure. S-GW relocation is not supported in this release.
- If the target MME/SGSN does not serve the UE-Usage-Type, the handover procedure must complete successfully and the target MME initiates the GUTI re-allocation procedure with non-broadcast TAI to change the serving DCN of the UE.

Roaming

MME in the visited PLMN provides an operator policy that allows to serve a UE whose home PLMN does not support DCNs. MME also provides operator policies that support the UE Usage Type parameter received from the HPLMN HSS.

Network Sharing

MME supports DCN selection based on the selected PLMN information received from the UE.

Limitations

The DECOR feature has the following limitations:

- Only one MMEGI can be configured per DCN.
- DCN deployments as part of a PLMN is not supported. The ability to configure DCN for a set of TAI/TAC is not supported.
- HSS Initiated UE usage type withdrawal is not supported. Only change in UE usage type is supported.
- DCNs can be deployed partially or heterogeneously.
  - The target MME or SGSN obtains the UE Usage Type information from the HSS during the subsequent TAU or RAU procedure. If the target MME/SGSN determines that the S-GW does not support the UE Usage Type, the target MME/SGSN must trigger the S-GW relocation as part of the handover procedures.

    In this release, S-GW relocation is not supported.

Standards Compliance

The DECOR feature complies with the following standards:

- 3GPP 23.401 Release 14.5.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 29.272 Release 14.6.0 - Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Diameter applications; 3GPP specific codes and identifiers

- 3GPP 29.274 Release 14.5.0 - Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP 29.303 Release 14.3.0 - Universal Mobile Telecommunications System (UMTS); LTE; Domain Name System Procedures; Stage 3

Configuring DECOR on MME

This section describes the CLI commands to configure the DECOR feature.

This feature supports the following configurations:

- DCN profile with
  - UE-Usage-Type
  - Static MMEGI
  - DNS lookup for MMEGI
  - PLMN
  - DCN-ID
  - Relative Capacity for the served DCN
  - DNS Service parameters using UE Usage Type or DCN-ID for S-GW / P-GW / MME / S4-SGSN selection / MMEGI lookup using DNS
- Associate DCNs to a specific RAT Type under MME service
- Associate multiple DCN profiles (to designate dedicated or default core network) under MME service
- Associate DCNs to a specific RAT Type under Call-Control-Profile
- Associate multiple DCN profiles (to designate dedicated or default core network) under Call-Control-Profile
- Non-broadcast TAI
- Request UE-Usage-Type from HSS on S6a interface
- UE-Usage-Type per IMSI/IMEI range

Configuring custom-actions ula gw-selection

Use the following configuration to enable GW selection based on UUT received in ULA.

```
configure
  mme-service mme_service_name
     [ no ] decor custom-actions ula gw-selection
     end
```

NOTES:

- **no**: Removes the DECOR configuration.
- **decor**: Specifies the DECOR configuration.
- **custom-actions** : Configures specific decor actions.
- **ula** :Configure UUT actions in ULA message
- **gw-selection**: Enables GW selection based on UUT received in ULA.

Configuring DECOR Profile

Use the following configuration to create and configure a DECOR profile by specifying the MMEGI hosting the DCN and the associated UE usage type using that DCN.

```
configure
  [ no ] decor-profile profile_name [ -noconfirm ]
    dcn-id dcn_id
    dns service-param ue-usage-type
    [ no ] mmegi { mmegi_value | dns }
    plmn-id mcc mcc_id mnc mnc_id
    served-dcn [ relative-capacity capacity ]
    [ no ] ue-usage-types num_ue_usage_types
    no { dcn-id | dns service-param | plmn-id | served-dcn }
    end
```

NOTES:

- **decor-profile** *profile_name*: Configures the DECOR feature as deployed by operator. A DECOR profile without any UE Usage Types configuration is treated as a Common Core Network. *profile_name* must be an alphanumeric string of 1 through 63 characters.

  Entering the **decor-profile** *profile_name* command results in the following prompt and changes to the Decor Profile Configuration mode:

  ```
  [context_name]host_name(config-decor-profile-<profile_name>)#
  ```

- **dns service-param ue-usage-type**: Configures the service parameter to select peer nodes using UE Usage Type or DCN-ID for S-GW / P-GW / MME / S4-SGSN / MMEGI lookup using DNS.
  - **service-param**: Configures the service parameter types used for DNS peer lookup.
  - **ue-usage-type**: Configures the UE Usage type that will be used for DNS service parameter.
  - For UE Usage Type based DECOR configuration:
    - If only UE-USAGE-TYPE is configured, DNS lookup uses UE-USAGE-TYPE.
    - If only DCN-ID is configured, DNS lookup uses DCN-ID without **dns service-param ue-usage-type** CLI command or UE-USAGE-TYPE with **dns service-param ue-usage-type** CLI (default profile).
    - If both UE-USAGE-TYPE and DCN-ID are configured, DCN-ID is used without **dns service-param ue-usage-type** CLI command or UE-USAGE-TYPE with **dns service-param ue-usage-type** CLI command.
    - If both UE-USAGE-TYPE and DCN-ID are not configured, DNS lookup uses UE-USAGE-TYPE (default profile).

- **dcn-id** *dcn_id*: Configures the DCN identifier for the specified DECOR profile. *dcn_id* must be an integer from 0 to 65535.
- **mmegi {** *mmegi_value* **| dns }**: Identifies the MME Group Identifier (MMEGI) of the configured DCN. *mmegi_value* must be an integer from 32768 to 65535.

  dns: Enables DNS for MMEGI retrieval using UE Usage Type.

  The **mmegi dns** command will work only when the **dns peer-mme** command is enabled under MME-service.
- **plmn-id mcc** *mcc_id* **mnc** *mnc_id*: Configures the PLMN identifier for the specified DECOR profile. This supports network sharing with different MMEGIs for different PLMNs.

  mcc *mcc_id*: Configures the mobile country code (MCC) for the specified DECOR profile. *mcc_id* must be a 3-digit number between 000 to 999.

  mnc *mnc_id*: Configures the mobile network code (MNC) for the specified DECOR profile. *mnc_id* must be a 2- or 3-digit number between 00 to 999.
- **served-dcn [relative-capacity** *capacity* **]**: Configures the MME that is serving the DCN and its relative capacity. These values are sent by MME to eNodeB during S1 Setup Response to indicate DCN-IDs served by the MME and their relative capacity.

  relative-capacity *capacity*: Set the relative capacity of this DCN. *capacity* must be an integer from 0 to 255. The default relative-capacity is 255.
- **ue-usage-types** *num_ue_usage_types*: Specifies the number of UE Usage Types in the dedicated core network. *num_ue_usage_types* is an integer from 0 to 255.

  A maximum number of 20 UE Usage Types are supported per DCN.
- **no**: Removes the specified DECOR parameters from the Global Configuration.
- MME will send the "MME CONFIGURATION UPDATE" message to all connected eNodeBs when a new DECOR profile is created with **served-dcn relative-capacity** and **dcn-id** CLI commands.
- MME will send the "MME CONFIGURATION UPDATE" message to all connected eNodeBs whenever there is a change in **served-dcn relative-capacity** or **dcn-id** CLI commands in a DECOR profile.

Associating a DECOR Profile under MME Service

Use the following configuration to associate a DECOR profile with an MME service.

```
configure
  context context_name
    mme-service service_name
      [ no ] associate decor-profile profile_name access-type { all | eutran
 | nb-iot }
       end
```

NOTES:

- **associate**: Associates a DECOR profile with an MME service.
- **decor-profile** *profile_name*: Specifies the DECOR profile that is associated with the MME Service.
- **access-type**: Configures the type of network access — E-UTRAN, NB-IoT, or both.

- **all** : Specifies to allow all access types.
- **eutran**: Specifies the access type as E-UTRAN.
- **nb-iot**: Specifies the access-type as NB-IoT.

- **no**: Removes the specified DECOR profile from the configuration.
- A maximum number of 16 DECOR profiles can be associated to an MME service.

Associating a DECOR Profile under Call Control Profile

Use the following configuration to associate a DECOR profile under call control profile.

```
configure
   call-control-profile profile_name
      [ remove ] associate decor-profile profile_name [ access-type { all |
eutran | nb-iot } ]
      end
```

NOTES:

- **associate**: Associates a DECOR profile under call control profile.
- **decor-profile** *profile_name*: Specifies the DECOR profile that is associated with the call control profile. *profile_name* must be an alphanumeric string of 1 through 63 characters.
- **access-type**: Configures the type of network access for the DECOR profile — E-UTRAN, NB-IoT, or both.
  - **all** : Specifies allows all access types.
  - **eutran**: Specifies the access type as E-UTRAN.
  - **nb-iot**: Specifies the access-type as NB-IoT.
- **remove**: Removes the specified DECOR profile from the configuration.
- A maximum number of 16 DECOR profile associations can be configured for the call control profile.

Configuring UE Usage Type over S6a Interface under MME Service

Use the following configuration to advertise or request UE Usage Type over S6a interface.

```
configure
   context context_name
      mme-service service_name
         [ no ] decor s6a ue-usage-type
         end
```

NOTES:

- **decor**: Specifies the DECOR configuration.
- **s6a**: Configures the S6a interface.

- **ue-usage-type**: Specifies the UE Usage Type that needs to be sent in the Authentication-Information-Request message over S6a interface.
- **no**: Disables the specified configuration.

Configuring UE Usage Type over S6a Interface under Call Control Profile

Use the following configuration to disable UE Usage Type requests over the S6a interface.

```
configure
  call-control-profile profile_name
    decor s6a ue-usage-type [ suppress ]
    remove decor s6a ue-usage-type
    end
```

NOTES:

- **decor**: Specifies the DECOR configuration.
- **s6a**: Enables the DECOR S6a configuration.
- **ue-usage-type**: Requests the UE Usage Type in S6a Authentication-Information-Request message.
- **suppress**: Suppresses sending the UE Usage Type in S6a Authentication-Information-Request message.
- **remove**: Removes the DECOR configuration.
- The configuration under call control profile overrides the MME service configuration.

Configuring UE Usage Type under Call Control Profile

Use the following configuration to locally configure the UE Usage Types for UEs matching the Call Control Profile criteria.

```
configure
  call-control-profile profile_name
    decor ue-usage-type usage_type_value
    remove decor ue-usage-type
    end
```

NOTES:

- **decor**: Specifies the DECOR configuration.
- **ue-usage-type** *usage_type_value*: Configures a UE Usage Type locally. *usage_type_value* must be an integer from 0 to 255.
- **remove**: Removes the specified configuration.

Configuring Non-Broadcast TAI

Use the following configuration to configure non-broadcast TAI. The configuration is added in support of HSS Initiated Dedicated Core Network Reselection.

When HSS sends ISDR with different UE-Usage-Type value other than what is already used by the subscriber and MME decides to move that UE to a new DCN, MME will send the GUTI Reallocation command with unchanged GUTI and non-broadcast TAI.

```
configure
  context context_name
    mme-service service_name
       tai non-broadcast mcc mcc_id mnc mnc_id tac tac_id
       no tai non-broadcast
       end
```

NOTES:

- **tai non-broadcast mcc** *mcc_id* **mnc** *mnc_id* **tac** *tac_id*: Specifies the Tracking Area Identity (TAI) which is not assigned to any area.

  mcc *mcc_id*: Configures the mobile country code (MCC) for the specified decor profile. *mcc_id* must be a 3-digit number between 000 to 999.

  mnc *mnc_id*: Configures the mobile network code (MNC) for the specified decor profile. *mnc_id* must be a 2- or 3-digit number between 00 to 999.

  tac *tac_id*: Configures the tracking area code (TAC) for the specified decor profile. *tac_id* must be an integer from 0 to 65535.

- **no**: Deletes the specified configuration.

Monitoring and Troubleshooting

This section provides information on the show commands available to support DECOR on MME.

Show Commands and/or Outputs

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

show decor-profile full all

The output of this command includes the following information

- Decor Profile Name — Displays the configured decor-profile name.
- UE Usage Types — Displays the configured UE usage types.
- MMEGI — Displays the MMEGI value.
- DNS — Indicates whether DNS is enabled or disabled.
- DCN Id — Displays the configured DCN identifier. Displays "Not Defined" if not configured.
- PLMN Id — Displays the configured PLMN identifier. Displays "Not Defined" if not configured.
- Serving DCN — Indicates whether MME is serving the DCN. Displays "Not Defined" if not configured.
  - Relative capacity — Indicates the configured relative capacity.

- DNS Service Param — Displays the configured DNS service parameter.

show mme-service all

The output of this command includes the following DECOR information:

- GW selection based on ULA - UUT - indicates if the GW selection based on ULA - UUT is enabled or disabled.

show mme-service name <mme_svc_name>

The output of this command includes the following information:

- Non-Broadcast TAI — Displays the configured values for MCC, MNC, and TAC.

show mme-service session full all

The output of this command includes the following DECOR information:

- DECOR Information:
  - UE Usage type
  - DCN Id

show mme-service statistics decor decor-profile <decor_profile_name>

This show command displays the DECOR statistics for a specified DECOR profile. The DECOR profile level statistics are pegged only if a DECOR profile is configured.

The output of this command includes the following information:

- Decor Statistics
  - Attached Calls
  - Initial Requests
    - ATTACH
      - Accepts
      - Reroutes
      - Rejects
  - TAU
    - Accepts
    - Reroutes
    - Rejects
  - Rerouted Requests

- ATTACH
  - Accepts
  - Rejects
- TAU
  - Accepts
  - Rejects

- UE-Usage-Type Source
  - HSS
  - UE Context
  - Peer MME
  - Peer SGSN
  - Config
  - eNB
- GUTI Reallocation Cmd due to UE-Usage-Type Change
  - Attempted
  - Success
  - Failures
- Handover from service area
  - DCN
  - Non DCN
- Explicit AIR
  - Attach
  - Inbound relocation
  - Inbound relocation using TAU procedure
- ISDR UE-Usage-Type Change
- MMEGI Selection
  - DNS
  - Local
  - Failure
- Node Selection

- SGW DNS
  - Common
  - Dedicated
- SGW Local Config
  - Common
- PGW DNS
  - Common
  - Dedicated
- PGW Local Config
  - Common
- MME DNS
  - Common
  - Dedicated
- MME Local Config
  - Common
- SGSN DNS
  - Common
  - Dedicated
- SGSN Local Config
  - Common

show mme-service statistics decor

The output of this command includes the following information:

- Decor Statistics
  - Attached Calls
  - Initial Requests
    - ATTACH
      - Accepts
      - Reroutes
      - Rejects

    - TAU
        - Accepts
        - Reroutes
        - Rejects

- Rerouted Requests
    - ATTACH
        - Accepts
        - Rejects
    - TAU
        - Accepts
        - Rejects

- UE-Usage-Type Source
    - HSS
    - UE Context
    - Peer MME
    - Peer SGSN
    - Config
    - eNodeB

- GUTI Reallocation Cmd due to UE-Usage-Type Change
    - Attempted
    - Success
    - Failures

- Handover from service area
    - DCN
    - Non DCN

- Explicit AIR
    - Attach
    - Inbound relocation
    - Inbound relocation using TAU procedure

- ISDR UE-Usage-Type Change

- MMEGI Selection
  - DNS
  - Local
  - Failure
- Node Selection
  - SGW DNS
    - Common
    - Dedicated
  - SGW Local Config
    - Common
  - PGW DNS
    - Common
    - Dedicated
  - PGW Local Config
    - Common
  - MME DNS
    - Common
    - Dedicated
  - MME Local Config
    - Common
  - SGSN DNS
    - Common
    - Dedicated
  - SGSN Local Config
    - Common

show mme-service statistics

The output of this command includes the following information at an MME service level:

- S1AP Statistics
  - Reroute NAS Requests

- Decor Statistics
  - Attached Calls
  - Initial Requests
    - ATTACH
      - Accepts
      - Reroutes
      - Rejects
    - TAU
      - Accepts
      - Reroutes
      - Rejects
  - Rerouted Requests
    - ATTACH
      - Accepts
      - Rejects
    - TAU
      - Accepts
      - Rejects
  - UE-Usage-Type Source
    - HSS
    - UE Context
    - Peer MME
    - Peer SGSN
    - Config
    - eNodeB
  - GUTI Reallocation Cmd due to UE-Usage-Type Change
    - Attempted
    - Success
    - Failures
  - Handover from service area

    - DCN
    - Non DCN
- Explicit AIR
    - Attach
    - Inbound relocation
    - Inbound relocation using TAU procedure
- ISDR UE-Usage-Type Change
- MMEGI Selection
    - DNS
    - Local
    - Failure
- Node Selection
    - SGW DNS
        - Common
        - Dedicated
    - SGW Local Config
        - Common
    - PGW DNS
        - Common
        - Dedicated
    - PGW Local Config
        - Common
    - MME DNS
        - Common
        - Dedicated
    - MME Local Config
        - Common
    - SGSN DNS
        - Common
        - Dedicated

- SGSN Local Config
  - Common

show mme-service statistics recovered-values

The output of this command includes the following information:

Decor Statistics:

- Initial Requests
  - ATTACH
    - Accepts
    - Reroutes
    - Rejects
  - TAU
    - Accepts
    - Reroutes
    - Rejects
- Rerouted Requests
  - ATTACH
    - Accepts
    - Rejects
  - TAU
    - Accepts
    - Rejects

Bulk Statistics

The MME schema and MME Decor schema include the supported bulk statistics for the DECOR feature.

MME Schema

The following bulk statistics are added in the MME schema:

Bulk Statistics	Description
mme-decor-attached-subscriber	Indicates the number of MME sessions attached that have an associated UE usage type.

Bulk Statistics	Description
mme-decor-initial-attach-req-accept	Indicates the total number of Initial Attach Requests accepted by the MME, which functions as a DCN.
mme-decor-initial-attach-req-reroute	Indicates the total number of Initial Attach Requests which are rerouted by the MME, which functions as a DCN.
mme-decor-initial-attach-req-reject	Indicates the total number of Initial Attach Rejects due to No Reroute data and not handled by the MME, which functions as a DCN.
mme-decor-reroute-attach-req-accept	Indicates the total number of Rerouted Attach Requests which are accepted by the MME, which functions as a DCN.
mme-decor-reroute-attach-req-reject	Indicates the total number of Rerouted Attach Requests which are rejected by the MME, which functions as a DCN.
mme-decor-initial-tau-req-accept	Indicates the total number of Initial TAU Requests accepted by the MME, which functions as a DCN.
mme-decor-initial-tau-req-reroute	Indicates the total number of Initial TAU Requests which are rerouted by the MME, which functions as a DCN.
mme-decor-initial-tau-req-reject	Indicates the total number of Initial TAU Rejects due to No Reroute data and not handled by the MME, which functions as a DCN.
mme-decor-reroute-tau-req-accept	Indicates the total number of Rerouted TAU Requests which are accepted by the MME, which functions as a DCN.
mme-decor-reroute-tau-req-reject	Indicates the total number of Rerouted TAU Requests which are rejected by the MME, which functions as a DCN.
mme-decor-ue-usage-type-src-hss	Indicates the number of MME subscriber sessions, where UE usage type was obtained from HSS/AUC.
mme-decor-ue-usage-type-src-ue-ctxt	Indicates the number of MME subscriber sessions, where UE usage type was obtained from MME DB record.
mme-decor-ue-usage-type-src-peer-mme	Indicates the number of MME subscriber sessions, where UE usage type was obtained from peer MME as part of handover.
mme-decor-ue-usage-type-src-peer-sgsn	Indicates the number of MME subscriber sessions, where UE usage type was obtained from peer SGSN as part of handover.
mme-decor-ue-usage-type-src-cfg	Indicates the number of MME subscriber sessions, where UE usage type was obtained from local configuration.
mme-decor-ue-usage-type-src-enb	Indicates the number of MME subscriber sessions, where UE usage type was obtained from the eNodeB, in the S1 message as part of reroute.

Bulk Statistics	Description
mme-decor-sgw-sel-dns-common	Indicates the number of times S-GW DNS selection procedures were performed with DNS RR excluding UE usage type. This counter increments only when the DNS RR with UE usage type is absent.
mme-decor-sgw-sel-dns-dedicated	Indicates the number of times S-GW DNS selection procedures were performed with DNS RR including UE usage type parameter(s). This counter increments only when the DNS RR with UE usage type is present.
mme-decor-sgw-sel-local-cfg-common	Indicates the number of times S-GW selection procedures were performed with locally configured S-GW address, without considering the UE usage type.
mme-decor-pgw-sel-dns-common	Indicates the number of times PGW DNS selection procedures were performed with DNS RR excluding UE usage type. This counter increments only when the DNS RR with UE usage type is absent.
mme-decor-pgw-sel-dns-dedicated	Indicates the number of times S-GW DNS selection procedures were performed with DNS RR including UE usage type parameter(s). This counter increments only when the DNS RR with UE usage type is present.
mme-decor-pgw-sel-local-cfg-common	Indicates the number of times P-GW selection procedures were performed with locally configured P-GW address without considering the UE usage type.
mme-decor-mme-sel-dns-common	Indicates the number of times MME DNS selection procedures were performed with DNS RR excluding UE usage type. This counter increments only when the DNS RR with UE usage type is absent.
mme-decor-mme-sel-dns-dedicated	Indicates the number of times MME DNS selection procedures were performed with DNS RR including UE usage type parameter(s). This counter increments only when the DNS RR with UE usage type is present.
mme-decor-mme-sel-local-cfg-common	Indicates the number of times MME selection procedures were performed with locally configured MME address without considering the UE usage type.

Bulk Statistics	Description
mme-decor-sgsn-sel-dns-common	Indicates the number of times SGSN DNS selection procedures were performed with DNS RR excluding UE usage type. This counter increments only when the DNS RR with UE usage type is absent.
mme-decor-sgsn-sel-dns-dedicated	Indicates the number of times SGSN DNS selection procedures were performed with DNS RR including UE usage type parameter(s). This counter increments only when the DNS RR with UE usage type is present.
mme-decor-handover-srv-area-dcn	Indicates the total number of inbound handovers from the service area where DCN is supported. This counter increments for every inbound handover from DCN service area.
mme-decor-handover-srv-area-non-dcn	Indicates the total number of inbound handovers from the service area where DCN is not supported. This counter increments for every inbound handover from non DCN service area.
mme-decor-explicit-air-attach	Indicates the number of explicit AIR messages during Attach. This counter increments when MME triggers an explicit AIR during Attach.
mme-decor-explicit-air-in-reallocation	Indicates the number of explicit AIR messages during inbound relocation. This counter increments when MME triggers explicit an AIR during inbound relocation.
mme-decor-explicit-air-tau-in-reallocation	Indicates the number of explicit AIR messages during inbound relocation using TAU. This counter increments when MME triggers an explicit AIR during inbound relocation using TAU.
mme-decor-sgsn-sel-local-cfg-common	Indicates the number of times SGSN selection procedures were performed with locally configured SGSN address without considering the UE usage type.
s1ap-transdata-reroutenasreq	Indicates the number of S1 Reroute NAS Request Message sent by MME.
mme-decor-mmegi-sel-dns	Indicates the total number of times MMEGI is selected through DNS from a dedicated pool (DNS records having UE Usage Type which is matching).
mme-decor-mmegi-sel-local-cfg	Indicates the total number of times MMEGI is selected from local configuration.

Bulk Statistics	Description
mme-decor-mmegi-sel-fail	Indicates the total number of times MMEGI is selected from failure.
mme-decor-guti-reallocation-attempted	This proprietary counter tracks the number of GUTI Reallocation procedures attempted due to UE-Usage-Type Change from HSS through ISDR OR after connected mode handover and UE-Usage-Type not served by the MME (NAS GUTI Reallocation Command message was sent by MME).
mme-decor-guti-reallocation-success	Tracks the number of GUTI Reallocation procedures successful.
mme-decor-guti-reallocation-failures	Tracks the number of GUTI Reallocation procedure failures.
mme-decor-isdr-ue-usage-type-change	Tracks the number of ISDR Messages received with different UE-Usage-Type from the HSS.
recovered-mme-decor-initial-attach-req-accept	Indicates the total number of Initial Attach Requests accepted by the MME, which functions as a DCN.
recovered-mme-decor-initial-attach-req-reroute	Indicates the total number of Initial Attach Requests which are rerouted by the MME, which functions as a DCN.
recovered-mme-decor-initial-attach-req-reject	Indicates the total number of Initial Attach Rejects without the reroute data and that are not handled by the MME, which functions as a DCN.
recovered-mme-decor-reroute-attach-req-accept	Indicates the total number of Rerouted Attach Requests which are accepted by the MME, which functions as a DCN.
recovered-mme-decor-reroute-attach-req-reject	Indicates the total number of Rerouted Attach Requests which are rejected by the MME, which functions as a DCN.
recovered-mme-decor-initial-tau-req-accept	Indicates the total number of Initial TAU Requests accepted by the MME, which functions as a DCN.
recovered-mme-decor-initial-tau-req-reroute	Indicates the total number of Initial TAU Requests which are rerouted by the MME, which functions as a DCN.
recovered-mme-decor-initial-tau-req-reject	Indicates the total number of Initial TAU Rejects due to No Reroute data and not handled by the MME, which functions as a DCN.
recovered-mme-decor-reroute-tau-req-accept	Indicates the total number of Rerouted TAU Requests which are accepted by the MME, which functions as a DCN.
recovered-mme-decor-reroute-tau-req-accept	Indicates the total number of Rerouted TAU Requests which are rejected by the MME, which functions as a DCN.

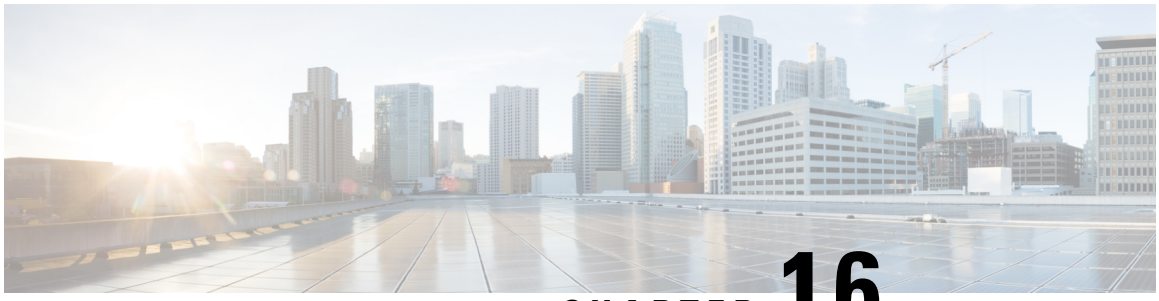
MME Decor Schema

The following bulk statistics for a specific decor-profile are added in the MME Decor schema:

Bulk Statistics	Description
mme-decor-profile-name	Indicates the name of the DECOR profile.
mme-decor-profile-attached-subscriber	Indicates the total number of subscribers on the MME which is acting as a DCN.
mme-decor-profile-initial-attach-req-accept	Indicates the total number of Initial Attach Requests accepted by the MME that is acting as a DCN.
mme-decor-profile-initial-attach-req-reroute	Indicates the total number of Initial Attach Requests which are rerouted by the MME that is acting as a DCN.
mme-decor-profile-initial-attach-req-reject	Indicates the total number of Initial Attach Rejects due to No Reroute Data and not handled by the MME that is acting as a DCN.
mme-decor-profile-reroute-attach-req-accept	Indicates the total number of Rerouted Attach Requests which are accepted by the MME that is acting as a DCN.
mme-decor-profile-reroute-attach-req-reject	Indicates the total number of Rerouted Attach Requests which are rejected by the MME that is acting as a DCN.
mme-decor-profile-initial-tau-req-accept	Indicates the total number of Initial TAU Reuquests accepted by the MME that is acting as a DCN.
mme-decor-profile-initial-tau-req-reroute	Indicates the total number of Initial TAU Reuquests which are rerouted by the MME that is acting as a DCN.
mme-decor-profile-initial-tau-req-reject	Indicates the total number of Initial TAU Rejects due to No Reroute Data and not handled by the MME that is acting as a DCN.
mme-decor-profile-reroute-tau-req-accept	Indicates the total number of Rerouted TAU Requests which are accepted by the MME that is acting as a DCN.
mme-decor-profile-reroute-tau-req-reject	Indicates the total number of Rerouted TAU Requests which are rejected by the MME that is acting as a DCN.
mme-decor-profile-ue-usage-type-src-hss	Indicates the total number of times UE Usage Type is received from the HSS and used by the MME.
mme-decor-profile-ue-usage-type-src-ue-ctxt	Indicates the total number of times UE Usage Type is fetched from the local DB Record and used by the MME.
mme-decor-profile-ue-usage-type-src-peer-mme	Indicates the total number of times UE Usage Type is received from the peer MME and used by the MME.
mme-decor-profile-ue-usage-type-src-peer-sgsn	Indicates the total number of times UE Usage Type is received from the peer SGSN and used by the MME.
mme-decor-profile-ue-usage-type-src-cfg	Indicates the total number of times UE Usage Type is fetched from the local configuration and used by the MME.

Bulk Statistics	Description
mme-decor-profile-ue-usage-type-src-enb	Indicates the total number of times UE Usage Type is received from the eNodeB and used by the MME.
mme-decor-profile-sgw-sel-dns-common	Indicates the total number of times S-GW is selected through DNS from a common pool (DNS records without UE Usage Type).
mme-decor-profile-sgw-sel-dns-dedicated	Indicates the total number of times S-GW is selected through DNS from a dedicated pool (DNS records with matching UE Usage Type).
mme-decor-profile-sgw-sel-local-cfg-common	Indicates the total number of times S-GW is selected from the local configuration without UE Usage Type.
mme-decor-profile-pgw-sel-dns-common	Indicates the total number of times P-GW is selected through DNS from a common pool (DNS records without UE Usage Type).
mme-decor-profile-pgw-sel-dns-dedicated	Indicates the total number of times P-GW is selected through DNS from a dedicated pool (DNS records with matching UE Usage Type).
mme-decor-profile-pgw-sel-local-cfg-common	Indicates the total number of times P-GW is selected from the local configuration without UE Usage Type.
mme-decor-profile-mme-sel-dns-common	Indicates the total number of times MME is selected through DNS from a common pool (DNS records without UE Usage Type).
mme-decor-profile-mme-sel-dns-dedicated	Indicates the total number of times MME is selected through DNS from a dedicated pool (DNS records with matching UE Usage Type).
mme-decor-profile-mme-sel-local-cfg-common	Indicates the total number of times MME is selected from the local configuration without UE Usage Type.
mme-decor-profile-sgsn-sel-dns-common	Indicates the total number of times SGSN is selected through DNS from a common pool (DNS records without UE Usage Type).
mme-decor-profile-sgsn-sel-dns-dedicated	Indicates the total number of times SGSN is selected through DNS from a dedicated pool (DNS records with matching UE Usage Type).
mme-decor-profile-sgsn-sel-local-cfg-common	Indicates the total number of times SGSN is selected from the local configuration without UE Usage Type.
mme-decor-profile-mmegi-sel-dns	Indicates the total number of times MMEGI is selected through DNS from a dedicated pool (DNS records with matching UE Usage Type).

Bulk Statistics	Description
mme-decor-profile-mmegi-sel-local-cfg	Indicates the total number of times MMEGI is selected from the local configuration.
mme-decor-profile-mmegi-sel-fail	Indicates the total number of times MMEGI selection failed.
mme-decor-profile-guti-reallocation-attempted	Indicates the number of GUTI Reallocation procedures attempted due to UE-Usage-Type Change from HSS through ISDR OR after connected mode handover and UE-Usage-Type not served by this MME (NAS GUTI Reallocation Command message was sent by MME).
mme-decor-profile-guti-reallocation-success	Indicates the number of successful GUTI Reallocation procedures.
mme-decor-profile-guti-reallocation-failures	Indicates the number of failed GUTI Reallocation procedures.
mme-decor-profile-isdr-ue-usage-type-change	Indicates the number of ISDR Messages received with different UE-Usage-Type from the HSS.
mme-decor-profile-explicit-air-attach	Indicates the number of explicit AIR messages during Attach.
mme-decor-profile-explicit-air-in-relocation	Indicates the number of explicit AIR messages during inbound relocation.
mme-decor-profile-explicit-air-tau-in-relocation	Indicates the number of explicit AIR messages during inbound relocation using TAU.
mme-decor-profile-handover-srv-area-dcn	Indicates the total number of inbound handovers from the service area where DCN is supported.
mme-decor-profile-handover-srv-area-non-dcn	Indicates the total number of inbound handovers from the service area where DCN is not supported.



CHAPTER 16

Deprecation of Manual Scaling

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

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	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*

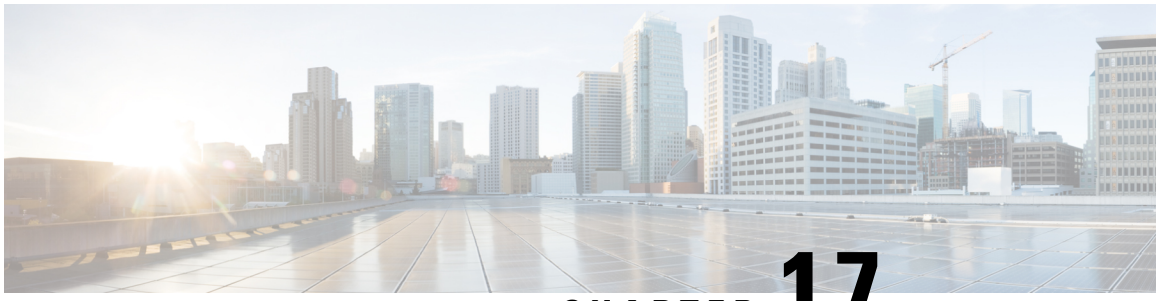
Revision History

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 17

Dynamic and Static Proxy Changes for IPv6 Flow Label

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

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	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

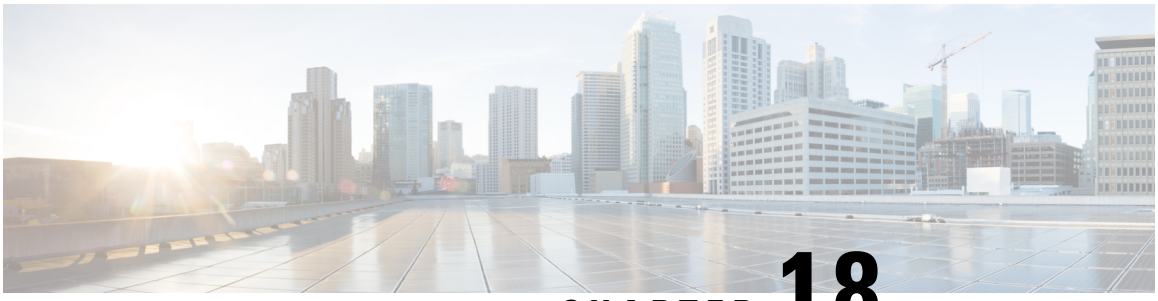
Revision Details	Release
IPv6 Flow labels are populated when TCP Acceleration is enabled.	21.14.5
First introduced.	21.8

Feature Changes

IPv6 Flow labels are populated when TCP Acceleration is enabled.

Previous Behavior: When TCP Acceleration is enabled, the dynamic and static proxy did not send the IPv6 flow labels received from the ISP and UE to the Gn and Gi interfaces, respectively.

New Behavior: When TCP Acceleration is enabled, the dynamic proxy sends IPv6 flow labels that are received from ISP and UE, to Gn and Gi interfaces respectively. In case of static proxy, a valid IPv6 flow label is sent to Gi side, and IPv6 Flow Label with “0” value is sent towards Gn.



CHAPTER 18

Enhanced Password Security

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

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 password security is enhanced with parameters like the maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user, group, and system levels. Also, instead of specifying intervals, administrators can selectively suspend a user either immediately or at a specific date, which is the suspend date.	21.14
First introduced.	Pre 21.2

Feature Changes

As a security measure for Cisco ASR 5500 and VPC products, the local login password is enhanced to secure the products. It is now possible to configure parameters like the maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user, group, and system levels.. By default, these parameters are enabled to secure the product. Administrators of the system can use the default values, change the values as per their need, or disable the parameters (though this is not recommended).

Previous Behavior: In releases earlier to 21.14, for local users, there was no option to configure the maximum life of a password, password expiry warning interval, and password expiry grace period for user and group levels.

New Behavior: In this release, for local users, it is possible to configure the maximum life of a password, password expiry warning interval, and password expiry grace period. These parameters are enabled by default. The Administrator can use the default values or change the values that are based on their requirement.

The parameters are configurable at the global level, user group level (operators, inspectors, administrators, and security administrators), and user level.

Also, instead of specifying intervals, administrators can selectively suspend a user either immediately or at a specific date, which is the suspend date.

The following keywords support the enhanced password functionality:

- The new **exp-grace-interval** and **[security-admin | administrator | inspector |operator]** keywords are added to the **local-user password** CLI command in Global Configuration Mode.
- The new **max-age**, **exp-grace-interval**, and **[security-admin | administrator | inspector |operator]** keywords are added to the **local-user username** CLI command in Global Configuration Mode.

Customer Impact:

The local user is notified with password expiry warnings and provided with password expired information.

Command Changes

local-user password

Use the following configuration to configure maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user group levels.

```
configure
  [ no | default ] local-user password { max-age days | exp-warn-interval
 days | exp-grace-interval days} { security-admin | administrator | inspector
 | operator }
  end
```

NOTES:

- **no** : Disables the specified parameter.
- **max-age** *days*: Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. After the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI. The default is 90 days.

  Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

  days is the number of days that passwords remain valid entered as an integer from 1 through 365.
- **exp-warn-interval** *days*: Specifies the password expiry warning interval in days.

  days is the number of days before which password expiry warning is issued. The valid values range from 7 to 90 days. The default is 30 days.
- **exp-grace-interval** *days*: Specifies the password expiry grace interval in days.

  days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The default is 3 days.
- **[security-admin | administrator | inspector | operator]**: Configures as follows:

  security-admin: Configures all local users with security administrator rights.

  administrator: Configures all local users with administrator rights.

  inspector: Configures all local users with inspector rights.

  operator: Configures all local users with operator rights.
- **default**: Sets or resets the corresponding parameter to its default value.

local-user username

Use the following configuration to selectively suspend a user either immediately or on the configured suspend date.

```
configure
  [ no | default ] local-user usernamename [ suspend-date YYYY:MM:DD:HH:MM:SS
 [ warn-date YYYY:MM:DD:HH:MM:SS ] ] [ max-age days [ exp-warn-interval days ]
 | [ exp-grace-interval  days ] ]
  end
```

NOTES:

- **no** : Disables the specified parameter.

- **suspend-date** *YYYY:MM:DD:HH:MM:SS*: Specifies the date and time when the local-user account should be suspended.

  YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

- **no warn-date** : Disables impending password expiry warnings.
- **warn-date** *YYYY:MM:DD:HH:MM:SS*: Specifies the date and time when the local-user account suspension warning notification starts.

  YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

- **max-age** *days*: Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. After the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.

  Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

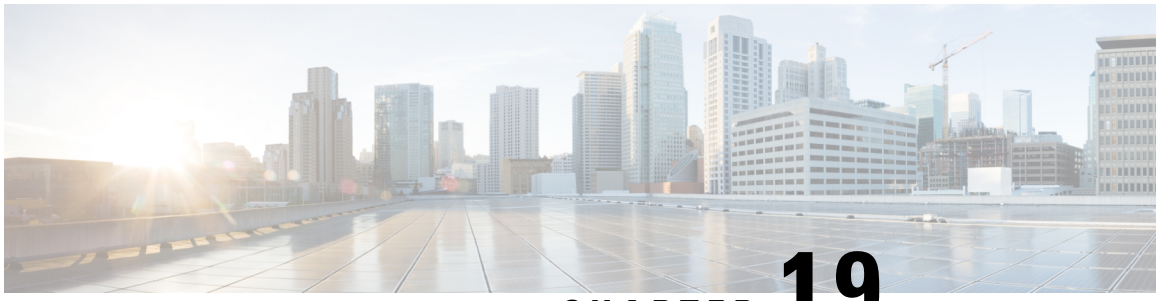
  days is the number of days that passwords remain valid entered as an integer from 1 to 365. The global or user group value is considered as the default value.

- **no exp-warn-interval** : Disables impending password expiry warnings.
- **exp-warn-interval** *days*: Specifies the password expiry warning interval in days.

  days is the number of days before which password expiry warning is issued. The valid values range from 7 to 90 days. The global or user group value is considered as the default value.

- **no exp-grace-interval** : Disables grace period of expired password.
- **exp-grace-interval** *days*: Specifies the password expiry grace interval in days.

  days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The global or user group value is considered as the default value.



CHAPTER 19

ERAB Setup Retry Handling

This chapter describes the following topics:

- Feature Summary and Revision History, on page 113
- Feature Changes, on page 114
- Command Changes, on page 114
- Performance Indicator Changes, on page 115

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

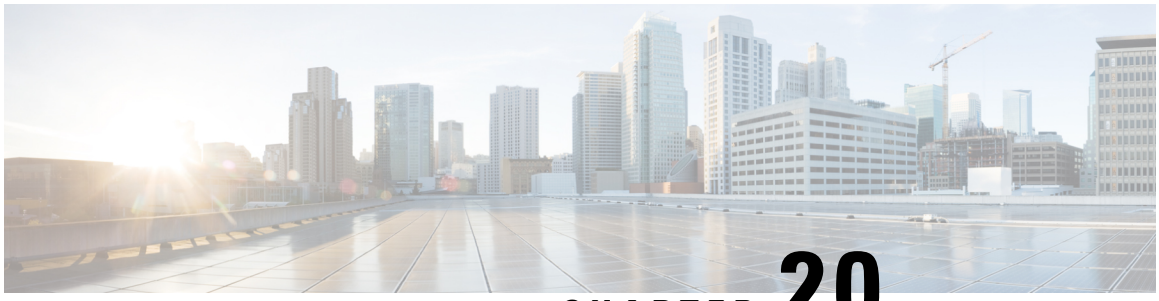
show mme-service name <mme_svc_name>

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

IPv6 Address Support for TACACS+ Server

- Feature Summary and Revision History, on page 117
- Feature Changes, on page 118
- Command Changes, on page 118

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* • *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, IPv6 addresses are supported along with IPv4 addresses for the receiver host system and network access server (NAS) on the TACACS+ server.	21.14
First introduced.	Pre 21.2

Feature Changes

The Terminal Access Controller Access-Control System Plus (TACACS+) AAA service-related parameters for use in authenticating StarOS administrative users via a TACACS+ server could be configured only with IPv4 addresses.

Previous Behavior: In releases earlier to 21.14, only IPv4 addresses were supported for the receiver host system and network access server (NAS) on the TACACS+ server.

New Behavior: In release 21.14 onwards, IPv4 and IPv6 addresses are supported for the receiver host system and network access server (NAS) on the TACACS+ server. The **ip-address** and **nas-source-address** keywords of the **server** CLI command are modified to support the IPv6 configuration.

Command Changes

server

Use the following configuration to specify external TACACS+ server with an IPv6 address.

```
configure
   tacacs mode
      [ no ] server priority priority_number ip-address ip-address
nas-source-address ip-address
     end
```

NOTES:

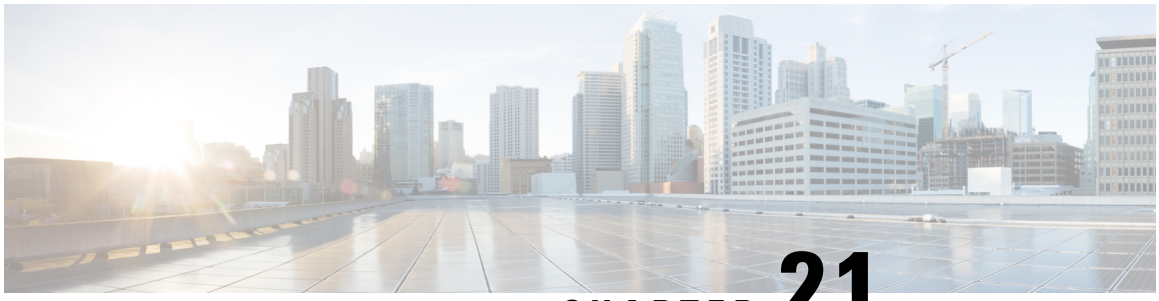
- **no**: Removes a specified server (by priority number) from the TACACS+ server list.
- **server priority** *priority_number*: Specifies the order in which TACACS+ servers are to be tried. The priority number corresponds to a configured TACACS+ server.

  For releases prior to 18.2, priority_number can be an integer from 1 (highest priority) to 3 (lowest priority).

  For releases 18.2+, priority_number can be an integer from 1 (highest priority) to 4 (lowest priority).

  If no server with priority 1 is specified, the next highest priority is used. If the specified priority matches that of a TACACS+ server already configured, any previously defined server configuration parameter(s) for that priority are returned to the default setting(s).
- **ip-address** *ip_address*: Specifies the IP address of the TACACS+ server in IPv4 or IPv4 dotted-decimal notation. Only one IP address can be defined for a given **server priority**.

- **nas-source-address** *ip_address*: Sets the IPv4 or IPv6 address to be specified in the Source Address of the IP header in the TACACS+ protocol packet sent from the NAS to the TACACS+ server. ip_address is entered using IPv4 dotted-decimal notation and must be valid for the interface.



CHAPTER 21

GMLC Interworking Support

- Feature Summary and Revision History, on page 121
- Feature Description, on page 122
- GMLC Interworking Support Configuration, on page 122
- Monitoring and Troubleshooting, on page 122

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
First introduced.	21.14

Feature Description

MME supports standard 3GPP defined GLMC interworking for location service. Last known location information is now sent when detach and no paging available state.

When the UE is in detached state or not-reachable state and the CLI is configured for the respective state(s) along with the experimental result code, the last known location info AVP's viz., "Location-Estimate, EUTRAN-Positioning-Data, ECGI and Age-Of-Location-Estimate (if the age is greater than 60 seconds)" will be sent.

GMLC Interworking Support Configuration

This section documents configuration of GMLC Interworking Support related functionality.

Including Experimental Result Code in PLA

Use the following configuration to Include experimental result code in PLA.

```
configure
   context context_name
      location-service service_name
        pla ue-state { detached | not-reachable } send
experimental-result-code experimental_result_code
        no pla ue-state { detached | not-reachable } send
experimental-result-code
        end
```

Important If there is any connection issue and PLA is not sent between SLG peer and MME, in that case if the UE is in detached or not reachable state and CLI for the experimental result code is configured, MME may not encode the experimental result code and the other AVP's in the PLA response message.

Notes:

- **detached**: Specifies the UE disconnecting.
- **not-reachable**: Specifies no paging response.
- **send experimental-result-code** *experimental_result_code*: Sends the result code value to be encoded in PLA depending on ue-state when PLR is received with GMLC Location type set to "Current/Last Known Location". *experimental_result_code* must be an integer from 1000 to 6000.
- **no**: Disables the inclusion of experimental result code in PLA.

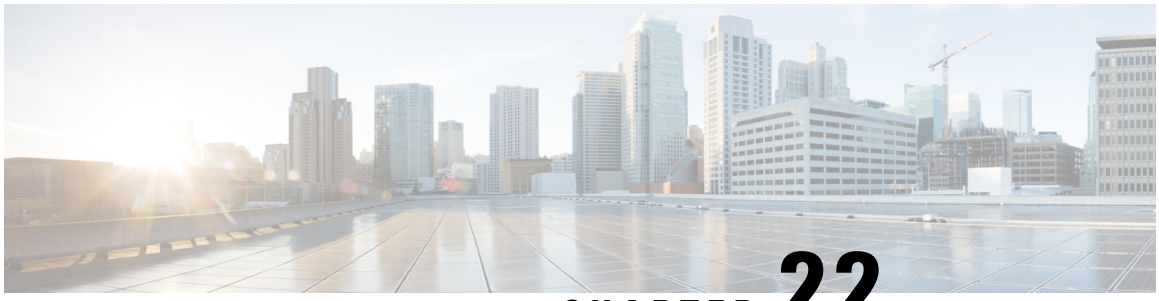
Monitoring and Troubleshooting

The following section describes commands available to monitor GMLC Interworking Support on the MME.

Show Commands and Outputs

show location service

A new show command out put "Experimental-Result-Code in PLA: Enabled(UE state not-reachable:4221, Detached:4223" is added to indicate Experimental Result Code in PLA is enabled or disabled.



CHAPTER 22

Implicit Update Location to HSS

- Feature Summary and Revision History, on page 125
- Feature Description, on page 126
- Configuring Implicit Update Location to HSS, on page 126
- Monitoring and Troubleshooting, on page 126

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.14

Feature Description

When the attach has a Globally Unique Temporary ID (GUTI), then MME queries for the subscriber information. If it has the subscriber information, then the Update Location Request (ULR) will not be executed because the UE information is updated already. Some of the customer devices cannot reset the old GUTI after returning to Home network from the visited network. This causes mismatch between Home Subscriber Server (HSS) and MME. Hence MME is expected to send ULR to HSS even when the subscriber Database(dB record) is present at the MME so that the HSS and the MME are in the sync.

Configuring Implicit Update Location to HSS

Enabling Implicit Update Location to HSS

Use the following configuration to implicitly send the ULR for local GUTI reattach.

```
configure
     call-control-profile call_control_profile_name
       [ no ] attach implicit-ulr
       end
```

NOTES:

- **attach implicit-ulr**: Attaches the implicit ULR.
- **no**: Removes the configuration to implicitly send the ULR for local GUTI reattach.

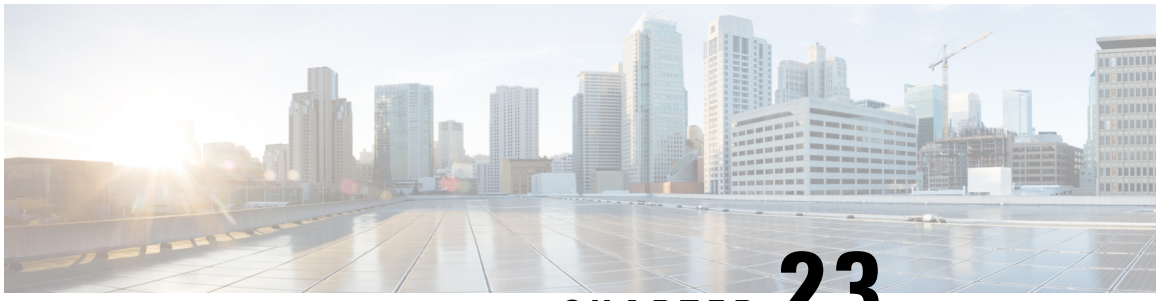
Monitoring and Troubleshooting

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

Show Commands and Outputs

show call-control-profile full all

A new show command out put "Implicit Sending of ULR during local GUTI attach" is added to indicate configured value (Enabled/Disabled).



CHAPTER 23

MME Clear Subscriber Enhancement

- Feature Summary and Revision History, on page 127
- Feature Description, on page 128
- MME Clear-Subscriber Enhancement, on page 128
- Monitoring and Troubleshooting, on page 128

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.	21.14

Feature Description

The `clear subscribers mme-only` command is enhanced with the `tai` (Tracking Area Identity), `mcc` (Mobile Country Code), `mnc` (Mobile Network Code) and (Tracking rea Code).

`tac`

The new command helps to clear the subscribers that are based on tracking area identify.

MME Clear-Subscriber Enhancement

This section provides information on the newly introduced CLI commands and configuration of MME "clear subscriber".

Configuring Clear Subscriber MME-Only

Use the following configuration to clear the subscriber using newly introduced keyword **tai** .

clear subscribers mme-only tai mcc *mobile_country_code* **mnc** *mobile_network_code* **tac** *tracking_area_code*
end

NOTES:

- **tai** : Specifies specific TAI Interface, must be followed by mcc, mnc, and tac.
- **mcc** *mobile_country_code*: Specifies mobile country code. *mobile_country_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc** *mobile_network_code*: Specifies mobile network code. *mobile_network_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **tac** *tracking_area_code*: Specifies tracking area code. *tracking_area_code* must be an integer value between 1 and 65535.

Monitoring and Troubleshooting

This section provides information regarding newly introduced show command and its output.

Show Commands and Outputs

show mme-service statistics tai taidb *taidb_name* mcc *mcc_value* tac *tac_value*

The output of this command includes the following fields:

Session Statistics:

Total Subscribers:

- Attached Calls

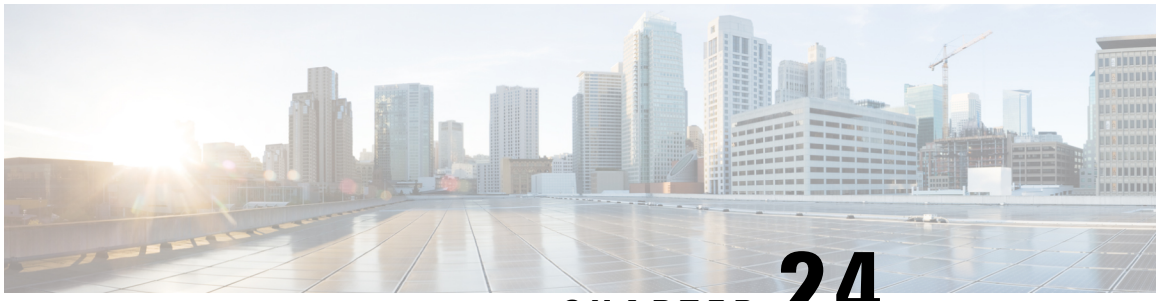
- Connected Calls
- Idle Calls

Important Above TAI level session statistics (Attached calls, Connected Calls & Idle Call) cannot be cleared by CLI command “clear mme-service statistics tai all” or “clear mme-service statistics taidb taidb_name” as they are current statistics.

Bulkstatistics

This section provides information on the bulk statistics introduced as part of MME Clear-Subscriber Enhancement feature in MME TAI Schema.

Bulkstatistics	Description
tai-sess-call-attached	The current total number of calls in attached per TAI.
tai-sess-call-connected	The current total number of calls in connected state per TAI.
tai-sess-call-idle	The current total number of calls in idle state.



CHAPTER 24

MME Double Counting Statistics of DECOR Rerouted Attach Accept

This chapter describes the following topics:

- Feature Summary and Revision History, on page 131
- Feature Changes, on page 132
- Command Changes, on page 132

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
First introduced.	21.14

Feature Changes

Previous Behavior: When ever DECOR is configured MME fills AIR-Flags to fetch UUT in AIR message towards HSS irrespective of whether UE Usage Type is present in MME-DB or not.

New Behavior: MME will not fetch UUT from HSS if it has already received from peer MME/SGSN and also in case of reroute scenarios.

In case of Initial attach (including local GUTI attach), when DECOR and new CLI are configured, MME will fill the AIR-Flags to fetch UUT from HSS, irrespective of the UUT stored in MME-DB.

Command Changes

This section describes the CLI configuration required to configure UUT actions in AIR messages.

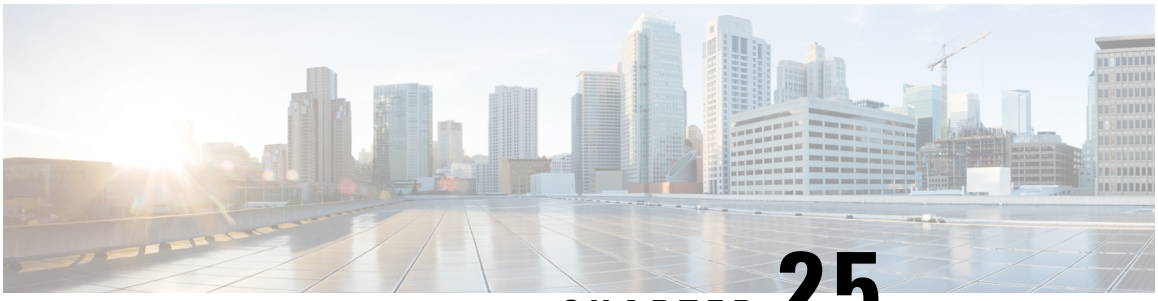
Configuring custom-actions air explicit-air-flags

Use the following configuration to configure Configures UUT actions in AIR message.

```
configure
     context context_name
       mme-service mme_service_name
          [ default | no ] decor custom-actions air explicit-air-flags
          end
```

NOTES:

- **default**: Configures default air-flags in AIR.
- **no**: Removes the DECOR configuration.
- **decor**: Specifies the DECOR configuration.
- **custom-actions** : Configures specific decor actions.
- **air** : Configures UUT actions in AIR message.
- **explicit-air-flags**: Fills air-flags in AIR, irrespective of UUT stored in DB.



CHAPTER 25

MME-MEF Interface

- Feature Summary and Revision History, on page 133
- Feature Description, on page 134
- How It Works, on page 134
- Configuring MME MEF Interface, on page 138
- Monitoring and Troubleshooting, on page 139

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.	21.14

Feature Description

A new service based on egtp-service supports MME's MEF functionality. This service handles a proprietary interface to deliver MEF events to MEF server based out of GTPv2 interface. This service creates a local end-point for the MEF interface which can be associated with the MME service. The maximum number of MEF services that can be created is limited to the maximum number of allowed egtp-service.

MME uses this interface to communicate with the peer MEF servers configured by the operator for each UP address. MME sends the MEF events to peer MEF server for only one PDN per UE, where it's created for MEC enabled APN along with UE-Usage-Type set to "PDN reconnection with MEF interworking". Following are list of messages defined for MEF interface:

- Subscriber-Activate-Request
- Subscriber-Modify-Request
- Subscriber-Delete-Request
- Subscriber-Audit-Request
- Subscriber-Audit-Response

Along with the list of above messages, ECHO-REQ and ECHO-RESPONSE are also supported for MEF interface path management.

How It Works

Architecture

Following messages are supported by MEF interface:

- Subscriber-Activate-Request
- Subscriber-Modify-Request
- Subscriber-Delete-Request
- Subscriber-Audit-Request
- Subscriber-Audit-Response

Subscriber-Activate-Request

MME sends a Subscriber-Activate-Request message to MEF server whenever the MEC PDN gets created for the UE either through Attach or PDN-Connect procedure. After Modify-Bearer-Request sent to SGW, MME sends this message to MEF with the following details:

Information Elements	Presence	Condition/Comment	IE Type	Ins
IMSI	M			

User Location Information (ULI)	M	Include ECGI and TAI.
PDN Address Allocation (PAA)	M	The PDN type field in the PAA must be set to IPv4, or IPv6 or IPv4v6.
Sender F-TEID for Control Plane	M	Sender F-TEID
Access Point Name (APN)	M	
UE Usage Type	M	This IE must be set to the subscribed UE Usage Type, if received from the HSS.

Subscriber-Modify-Request

MME sends Subscriber-Activate-Request message to the MEF server, whenever UE mobility occurs through Tracking-Area-Update (TAU), Service-Request, Handovers (S1/X2 Handover), and Location-Report with the ECGI change. MME does not send this event to MEF if any of the earlier procedures resulted only in the TAI change and no change in ECGI. Once the earlier mobility procedure compiled successfully with the ECGI change the MME sends the following details to MEF.

Information Elements	Presence	Condition/Comment	IE Type	Ins
IMSI	M		IMSI	0
User Location Information (ULI)	M	Include ECGI and TAI	ULI	0

Subscriber-Delete-Request

MME sends Subscriber-Delete-Request message to MEF server, whenever MEC PDN gets terminated for the UE either through Detach or PDN-Disconnect procedure. MME sends this message to MEF with the following details.

Information Elements	Presence	Condition/Comment	IE Type	Ins
IMSI	M		IMSI	0
User Location Information (ULI)	M	Include ECGI and TAI	ULI	0

PDN Address Allocation (PAA)	M	The PDN type field in the PAA must be set to IPv4, or IPv6 or IPv4v6.	PAA	0

MEF performs auditing for each UE periodically or when MEF receives MEC messages for unknown IMSI.

Subscriber-Audit-Request

MEF performs auditing for each UE periodically and when it receives MEC messages for unknown IMSI. It sends the Subscriber-Audit-Request message to MME with the IMSI of the subscriber for which it wants to perform an audit. In case of auditing for Unknown-IMSI, MEF sends the TEID as 0 in GTPv2 header, otherwise MEF fills the TEID information that is received in the Subscriber-Activate-Request from MME. MME responds with Subscriber-Audit-Response to MEF.

Information Elements	Presence	Condition/Comment	IE Type	Ins
IMSI	M		IMSI	0

Subscriber-Audit-Response

MME sends this message to MEF when it receives the Subscriber-Audit-Request for an IMSI. It responds with success or failure cause based on the availability of UE information. If MME does not have valid UE-Context for the IMSI received in Audit-Request, it responds with cause as “Context-Not-Found”, otherwise it sends the IMSI, PAA (IP address IPv4/v6), ECGI, TAI, APN-NI, UE-Usage-Type and so on.

Information Elements	Presence	Condition/Comment	IE Type	Ins
Cause	M		Cause	0
IMSI	M		IMSI	0
User Location Information (ULI)	CO	It includes ECGI and TAI.	ULI	0
PDN Address Allocation (PAA)	CO	The PDN type field in the PAA must be set to IPv4 or IPv6 or IPv4v6.	PAA	0
Access Point Name (APN)	CO		APN	0
UE Usage Type	CO	This IE must be set to the subscribed UE Usage Type, if received from the HSS.	Integer Number	0

REQ-ACCEPTED (Successful scenario where the MME can find the UE) and CONTEXT-NOT-FOUND (Failure cases where the MME is unable to find UE or invalid IMSI, and so on) are valid causes that are included in the Subscriber-Audit-Response's for different conditions.

Connection Auditing

MME/MEF performs the connection auditing by sending "ECHO-REQ" after the echo timer expiry which is configurable at MME under egtp-service.

ECHO Request: MME/MEF sends the ECHO-REQ whenever the configured echo-timer expires. MME initiates the ECHO-REQ when it has one valid session at-least towards the peer MEF server.

Information Elements	Presence	Condition/Comment	IE Type	Ins
Recovery	M		Recovery	0
Sending Node Features	CO	This IE sends towards a peer node on any GTPv2 interface if the sending node supports at least one feature on this interface or if the sending node supports at least one feature and does not know the interface type towards the peer node. This IE may be present otherwise.	Node Features	0
Private Extension	O	It includes ECGI and TAI.	Private Extension	VS

ECHO Response

MME/MEF responds with ECHO-RESPONSE whenever it receives ECHO-REQ from the peers.

Information Elements	Presence	Condition/Comment	IE Type	Ins
Recovery	M		Recovery	0
Sending Node Features	CO	This IE sends towards a peer node on any GTPv2 interface if the sending node supports at least one feature on this interface or if the sending node supports at least one feature and does not know the interface type towards the peer node. This IE may be present otherwise.	Node Features	0
Private Extension	O		Private Extension	VS

Limitations

- New MEF messages use the unused Message Type from GTPv2 specification. Any new message type defined by 3GPP for GTPv2 will impact the working of MEF interface.

- When MME requests PDN disconnection at GW-U area change, "Subscriber-Delete-Request" is sent and then re-selection of MEF is done at PDN connection establishment.
- MEF grouping and MEF redundancy (primary/secondary link) are not supported in this release.
- Run-time configuration change of MEF server address and disabling of MEF interworking will take effect only for the new subscribers.
- Run-time configuration change to remove association of MEF service under MME service and removal of MEF service will take effect immediately.

Configuring MME MEF Interface

This section provides information on the CLI commands to configure MME MEF Interface.

Configuring egtp-mef-service

Use the following configuration to associate the given egtp-service for MEF interface at the MME.

```
configure
  context context_name
    mme-service service_name
      associate egtp-mef-service  egtp_mef_service_name context context_name
      no associate egtp-mef-service
      end
```

NOTES:

- *no* Removes the association for MEF interface at the MME.
- **egtp-mef-service** *egtp_mef_service_name* : Associates the given egtp-service for MEF interface at the MME.

  egtp_mef_service_name must be a string from 1 to 63.
- **context** *context_name*: Specifies the context to which the service belongs.

  context_name must be a string from 1 to 79.

Configuring Peer MEF Address

Use the following configuration to configure peer MEF Address.

```
configure
  lte-policy
    tai-mgmt-db db_name
      tai-mgmt-obj obj_name
          [ no ] up-address ip_address mef-address ip_address
          end
```

NOTES:

- **no**: Disables the configuration of peer MEF address.

- **mef-address***ip_address*: Configures the peer MEF server address for MEF signalling. *ip_address* must be any IPV4 address of notation ##.##.##.## or IPV6 address of notation ####:####:####:####:####:####:####:#### . IPV6 also supports :: notation.

Monitoring and Troubleshooting

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

Show Commands and Outputs

show mme-service all

The output of this command includes the following fields:

- EGTP MEF Context
- EGTP MEF Service

show mme-service name <service-name>

The output of this command includes the following fields:

- EGTP MEF Context
- EGTP MEF Service

Show lte-policy tai-mgmt-db name <db-name>

- MEF-ADDRESS

Show lte-policy tai-mgmt-db name <db-name> tai-mgmt-obj name <obj-name>

- MEF-ADDRESS

Show egtpc statistics

The output of this command includes the following fields:

MEF Messages:

- MEF Subscriber Activate Request:
  - Initial TX:
- MEF Subscriber Modify Request:
  - Initial TX:
- MEF Subscriber Delete Request:

- Initial TX:

- MEF Subscriber Audit Response:
  - Initial TX:

- MEF Subscriber Audit Request:
  - Initial RX:

Important MEF statistics block is displayed only when the values are non-zero.

Show egtpc statistics event-statistics

The output of this command includes the following fields:

Event Statistics at EGTPC:

- MEF Subscriber Audit Indication Evt

Request Events (from SAP to EGTPC):

- MEF Subscriber Activate Request Evt
- MEF Subscriber Modify Request Evt
- MEF Subscriber Delete Request Evt

Response Events (from SAP to EGTPC)

- MEF Subscriber Audit Response Evt

Show mme-service statistics debug

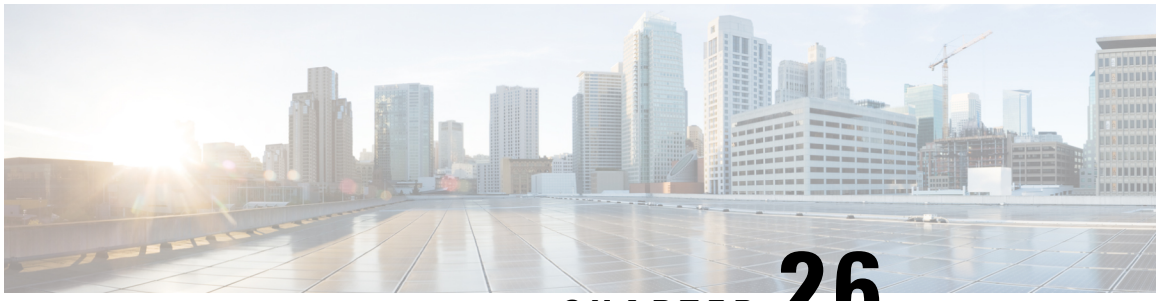
The output of this command includes the following fields:

Recovery:

- Failed MEF EGTPC Recovery
- Bad Peer MEF ctxt
- Failed MEF tunnel handles

Checkpoint:

- Bad MEF Ctxt



CHAPTER 26

Monitoring and Reporting of Stonith Service Failures

- Feature Summary and Revision History, on page 141
- Feature Description, on page 141

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UAS
Applicable Platform(s)	UGP
Feature Default	Enabled - Always on
Related Features in this Release	Not Applicable
Related Documentation	• *Ultra M Solutions Guide* • *Ultra Services Platform Deployment Automation Guide*

Revision History

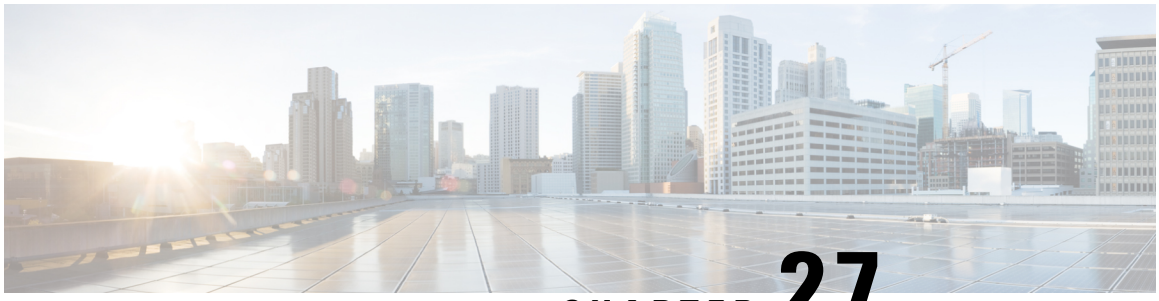
Revision Details	Release
First introduced.	6.8

Feature Description

Shoot The Other Node In The Head (STONITH) is a Linux service used for protecting user data from being corrupted by rogue nodes or concurrent access.

The Ultra M health monitoring feature is enhanced to monitor the STONITH service in overcloud controller nodes through pacemaker cluster (PCS) status.

Users can now use the *ultram_health_os.report* file located at the */var/log/cisco/ultram-health/* directory path to identify the STONITH service failures.



CHAPTER 27

Monitor Protocol Support for DCNR

This chapter describes the following topics:

- Feature Summary and Revision History, on page 143
- Feature Changes, on page 144

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*

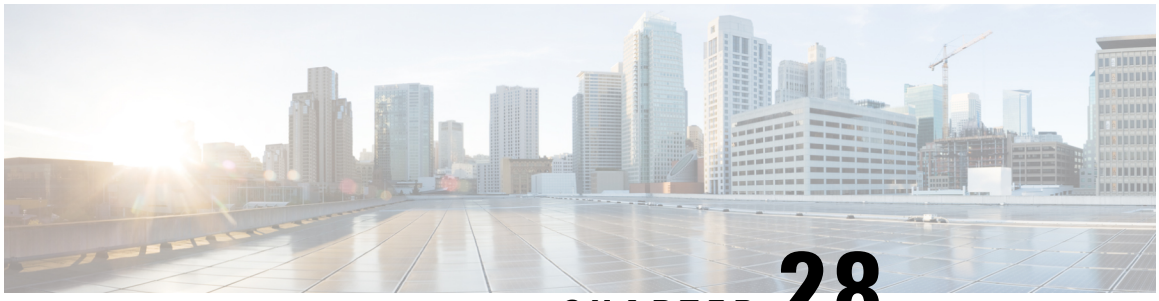
Revision History

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 28

NB-IOT EDRX Supported values in ATTACH/TAU Accept

This chapter describes the following topics:

- Feature Summary and Revision History, on page 145
- Feature Changes, on page 146

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*

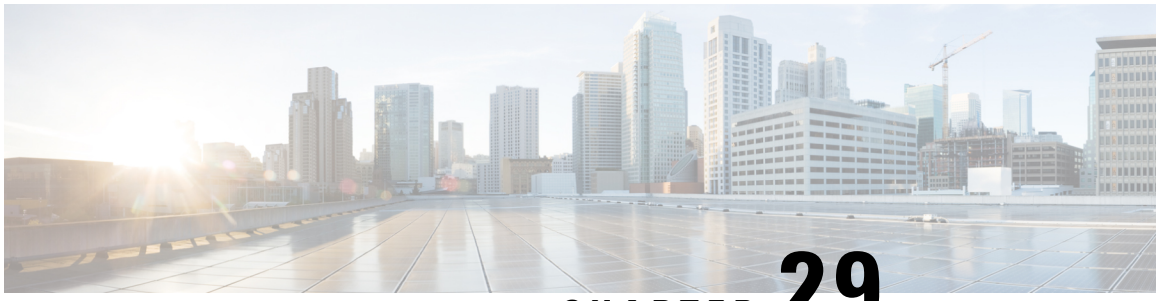
Revision History

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 29

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

This chapter describes the following topics:

- Feature Summary and Revision History, on page 147
- Feature Changes, on page 148
- Command Changes, on page 149

Feature Summary and Revision History

Summary Data

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

Revision History

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

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

Feature Changes

Previous Behavior:

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

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

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

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

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

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

Command Changes

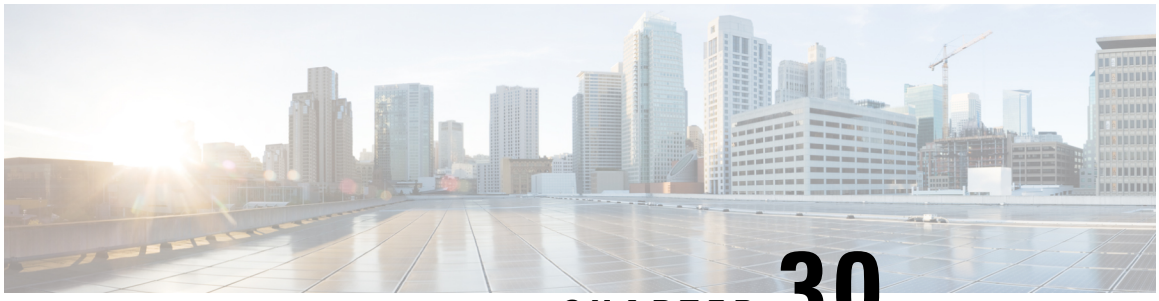
NR UE Security Capability IE

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

```
configure
  context context_name
    mme-service nr-ue-security-capability-ie service_name
      [ no ] nr-ue-security-capability-ie
      end
```

NOTES:

- **mme-service** *service_name*: Creates an MME service or configures an existing MME service in the current context. *service_name* specifies the name of the MME service must be a string 1–63 characters.
- **nr-ue-security-capability-ie**: Configures NR UE Security Capability IE for MME service users.
- **no**: Disables CLI **NR UE Security Capability IE** in an MME Service.



CHAPTER 30

P-GW Buffering Mechanism

- Feature Summary and Revision History, on page 151
- Feature Description, on page 152
- How It Works, on page 152
- Configuring the P-GW Buffering Mechanism Feature, on page 152

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.14

Feature Description

The P-GW can buffer a maximum of two policy (PCRF) messages when the Default-Bearer-QoS change is in pending state. With Presence Reporting Area (PRA) related call flows, two or more messages can be received when the Update Bearer Response (UBResp) is in pending state.

The P-GW Buffering Mechanism feature enables the P-GW to gracefully handle the RAR or CCA-U received from the PCRF when P-GW waits for the UBResp.

How It Works

Under Active Charging Service (ACS) mode, a CLI command - **pending-buffer-size**, is added to increase the buffer size. The PCRF messages are buffered until the P-GW receives a UBResp message while the Default-Bearer-QoS change is in pending state.

Configuring the P-GW Buffering Mechanism Feature

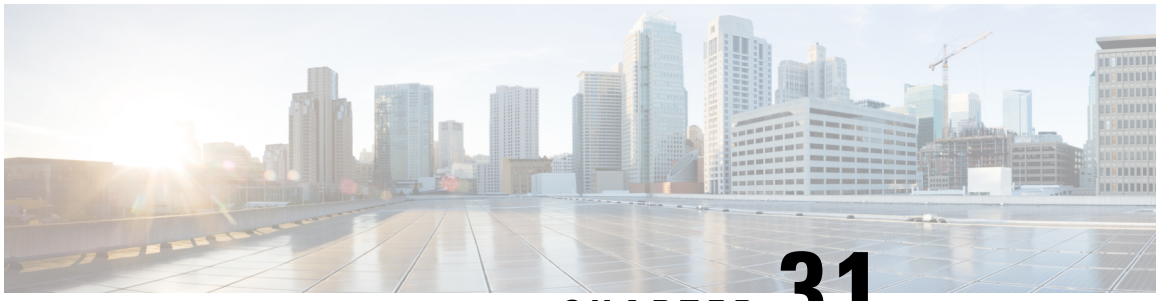
Use the following configuration to increase the buffer size for storing PCRF messages when the Default-Bearer-QoS change status is in pending.

```
configure
  active-charging service service_name
    policy control def-bearer-qos-change pending-buffer-size buffer_size
    end
```

NOTES:

- **def-bearer-qos-change**: Sets the Default-Bearer-QoS change parameters.
- **pending-buffer-size** *buffer_size*: Specifies the buffer size for storing the PCRF messages when Default-Bearer-QoS change is pending. The buffer_size is an integer ranging from 2 through 4.

  The minimum configured value is 2 and maximum is 4.
- The **no policy control def-bearer-qos-change** configures the command with its default setting. Default = 2.
- The default value suffices for most use-cases. However, higher values must be configured based on the use-case basis and by considering the memory usage.
- The CLI command takes effect for new calls.



CHAPTER 31

Sender FTEID IE in Modify Bearer Request Message

- Feature Summary and Revision History, on page 153
- Feature Changes, on page 154

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
With this release, the P-GW accepts the Modify Bearer Request message that is without Bearer Context, and with old FTEID.	21.14
First introduced.	Pre 21.2

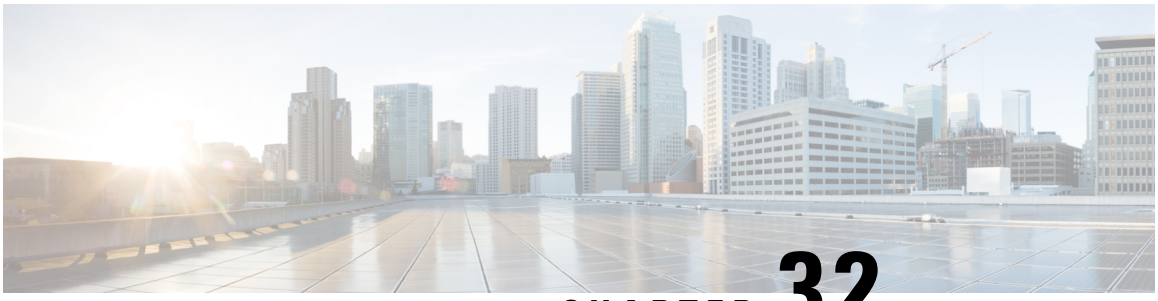
Feature Changes

The change in behavior is to comply with 3GPP TS 29.274 (C4-121937 CR-1254) that is related to Sender FTEID IE in the Modify Bearer Request (MBR) message. P-GW rejects the MBR request with a “Conditional IE Missing” message. With this release, the mandatory check is removed for Bearer Context at P-GW ingress along with Sender FTEID. Also, the P-GW deduces the old and new value of the Sender FTEID during validation.

Previous Behavior: P-GW rejected the MBR message that was without Bearer Context, and with old FTEID.

New Behavior: P-GW accepts the MBR message that is without Bearer Context, and with old FTEID.

Customer Impact: P-GW validates the FTEID and determines to either accept or reject the MBR message.



CHAPTER 32

SGSN Clear Subscriber Enhancement

- Feature Summary and Revision History, on page 155
- Feature Description, on page 156
- Configuring Clear Subscriber, on page 156

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	Enabled - 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.	21.14

Feature Description

New keyword ‘sgsn-only’ and ‘gprs-only’ keywords introduced under-existing "clear subscribers" to clear 3g and 2g subscriber, ‘lai’ CLI added under sgsn-only/gprs-only reads the location area identity parameters which are “mcc, mnc and lac.” These parameters are passed on to the existing ‘clear subscribers’ framework. The existing framework handles the new location parameters and finds the matching subscribers and all the matching subscribers (both 2g and 3g subscribers) are cleared.

Configuring Clear Subscriber

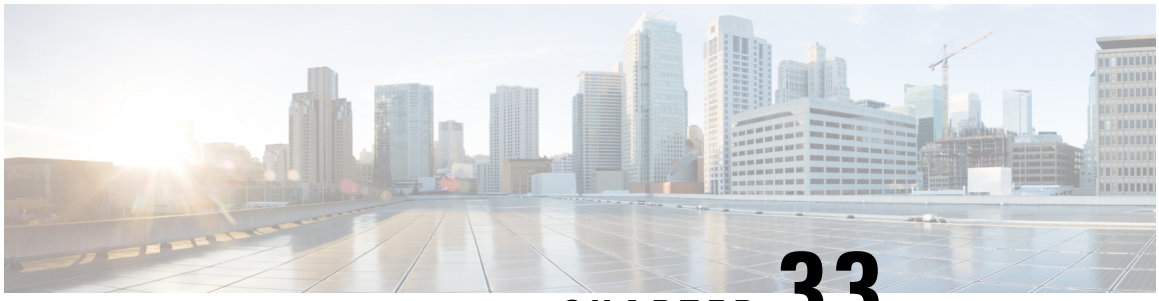
Clear Subscribers Enhancement

Below key words are introduced to clear subscriber.

clear subscribers { gprs-only | sgsn-only }lai mcc *mobile_country_code* **mnc** *mobile_network_code* **lac** *location_area_code*
end

Notes:

- **gprs-only**: Specifies the clearing of SGSN 2G subscribers only.
- **sgsn-only**: Specifies the clearing of SGSN 3G subscribers only.
- **lai**: Specifies location area identity.
- **mcc** *mobile_country_code*: Specifies mobile country code. *mobile_country_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc** *mobile_network_code*: Specifies mobile network code.*mobile_network_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **lac** *location_area_code*: Specifies location area code. *location_area_code* must be an integer from 1 to 65535.



CHAPTER 33

UEM as CF Active/Standby Arbitrator

- Revision History, on page 157
- Feature Description, on page 158
- How It Works, on page 158
- Configuring the UEM as CF Active/Standby Arbitrator, on page 158

Revision History

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*

Revision History

Revision Details	Release
First introduced.	6.8

Feature Description

This feature simulates a hardware reset line (similar to the support available on the ASR 5500) during the StarOS Control Function (CF) active/standby switchover event. The simulation occurs by requesting the UEM to perform a VM reboot operation for the currently active CF VDU instance with the VNFM.

How It Works

This section describes how this feature works.

The sequential workflow of this feature is as follows:

- The original Standby CF that is in an active role informs the UEM.
- The original Standby CF is now in the process of becoming the new Active CF.
- The UEM initiates the VM recovery operations with the ESC for the original Active CF.
- The ESC reboots the original Active CF.
- The UEM sends a switchover accept response to the original Standby CF.
- The original Standby CF then becomes the new Active CF.
- The UEM ignores all the requests from the original Active CF until the ESC reports VM Alive (that is, the ESC successfully reboots the original Active CF).
- The ESC informs the UEM about the successful reboot of original Active CF.
- After the ESC successfully reboots the original active CF, the original Active CF now becomes the new Standby CF.
- The new Standby CF informs the UEM that it is now the new Standby CF. Then, the UEM starts accepting the request from the new Standby CF.

Configuring the UEM as CF Active/Standby Arbitrator

This release introduces an optional UPP parameter "VNFM_PROXY_ARBITRATION" to control the operation of this feature. This feature gets disabled by default. The feature requires explicit configuration of this parameter. Set this parameter value to 1 to enable this feature.

Note Leaving the parameter unconfigured or setting the parameter value to 0 disables this feature.

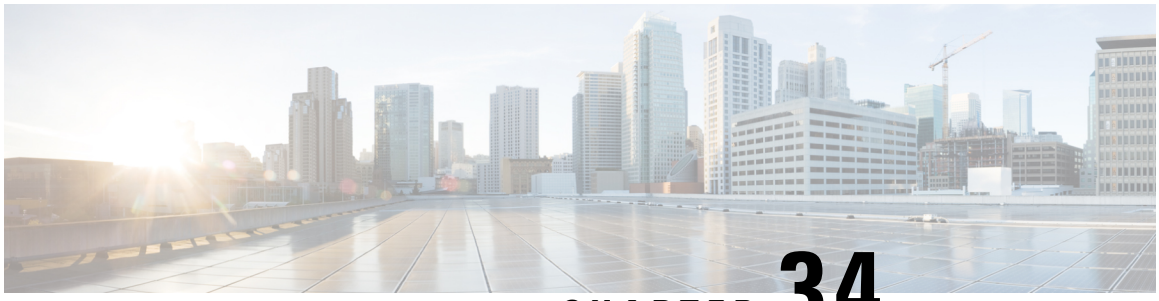
Verifying the Feature Configuration

Use the following command to verify the feature configuration on StarOS.

```
show cloud configuration
```

The following is a sample output of the show command:

```
[local]qvpc-di# show cloud configuration 1
Card 1:
  Config Disk Params:
-------------------------
CARDSLOT=1
CPUID=0
CARDTYPE=0x40010100
DI_INTERFACE=BOND:TYPE:ixgbevf-1,TYPE:ixgbevf-2
DI_INTERFACE_VLANID=1020
VNFM_INTERFACE=MAC:fa:16:3e:1f:19:fc
VNFM_PROXY_ADDRS=30.101.14.11,30.101.14.16
MGMT_INTERFACE=MAC:fa:16:3e:9f:75:46
VNFM_IPV4_ENABLE=true
VNFM_IPV4_DHCP_ENABLE=true
VNFD_NAME=rtice_autovnf-vPC-DI-rtice
VNFM_PROXY_ARBITRATION=1
  Local Params:
-------------------------
CARDSLOT=1
CARDTYPE=0x40010100
CPUID=0
```



CHAPTER 34

UEM Interworking with Generic VNFM

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

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.	6.8

Feature Description

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

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

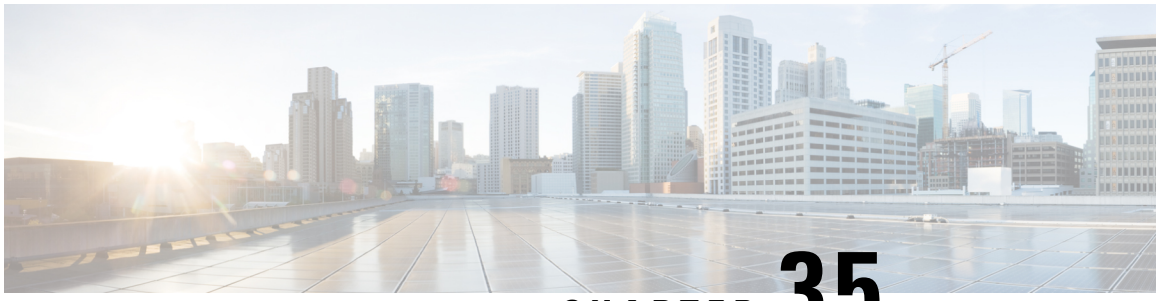
The Ve-VNFM interface for SOL002 is currently supported for VNF Lifecycle Management only. VNF Instantiation, VNF Termination, Notification Subscription, Notification Handling, and Authentication procedures are currently supported as part of the lifecycle management functions.

Important The Ve-VNFM interface is currently validated for use with only one particular generic VNFM (gVNFM) vendor. To support other gVNFM vendors, additional testing might be needed. Any vendor-specific implementation or procedures need an enhancement from the UEM side.

This feature is disabled by default. To enable this feature, the following configurations should be included in *proxy-params.txt* file located at the */opt/cisco/em/config* directory as part of the day-0 configuration in UEM.

```
vnfm-type:gvnfm
vnfm-proxy-username:em-user
vnfm-proxy-password:artlU@462
```

Wherein the `vnfm-proxy-username` and `vnfm-proxy-password` are new parameters introduced in this release. The value of `vnfm-type` parameter should be set to `gvnfm` to enable this feature.



CHAPTER 35

Unique Virtual Router ID for All UEM Deployments

- Feature Summary and Revision History, on page 163
- Feature Changes, on page 163

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	• *Cisco Ultra Services Platform NETCONF API Guide*

Revision History

Revision Details	Release
First introduced.	6.8

Feature Changes

In a multi-VNF deployment scenario, one of the UEMs for the VNFs fails to become active because of the common virtual router ID across all UEM deployments.

This release provides a solution to the issue by configuring a unique virtual router ID for all UEM deployments. To achieve this functionality, the current release uses a new configurable parameter **ha-cluster-id** for the VNF.

Previous Behavior: When instantiating two VPC VNFs and using one UEM per VNF, the UEM for the second VNF does not come up. This is due to the usage of the same virtual router ID across all UEMs.

New Behavior: Update the ESC configuration with the new parameter **ha-cluster-id** under VNFC of the UEM. This parameter allows the user to configure a unique HA cluster ID for the VNF within an allowed range of 91-100. The default value of the parameter is 91.

Note The **ha-cluster-id** parameter is optional.