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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

AAA Changes in Release 19  1
  AAA Enhancements for 19.6.2  1
    Handling IMEI or IMSI Mismatch During Handover  1
    Feature Changes  2
    Command Changes  2
  AAA Enhancements for 19.5  3
    Event Trigger Reporting to Local-Policy  3
    Feature Changes  3
    Framed-IP Allocation Based on Virtual APN  3
    Feature Changes  3
    Multiple Class Attribute Support  3
    Feature Changes  4
    Changes to Accounting-Policy  4
    Feature Changes  4
    Changes in no diameter endpoint Command Output  4
    Feature Changes  4
  AAA Enhancements for 19.4  5
    3GPP Rel.9 Compliance for Flow-Description AVP  5
    Feature Changes  5
    Called-Station-ID AVP in CoA and DM Messages  6
    Feature Changes  6
    Encoding of MIP6-Agent-Info AVP in AAR  6
    Feature Changes  6
    Enhancements for custom67 RADIUS Dictionary  7
    Feature Changes  7
    Handling Redirection Message in DRA Network  8
    Feature Changes  8
    Location Based Local-Policy Rule Enforcement  8
Feature Changes 8
Command Changes 9
   action priority 9
   rule priority 9
   condition priority 10
Performance Indicator Changes 10
   show local-policy statistics summary 10
New Fields in show aaa group Configuration Output 11
   Feature Changes 11
   Performance Indicator Changes 11
      show aaa group all 11
QoS Change for Default Bearer 11
   Feature Changes 11
Support for Delegated-IPv6-Prefix in RADIUS Accounting Messages 12
   Feature Changes 12
Support for TAI and ECGI Change Reporting 12
   Feature Changes 12
   Performance Indicator Changes 13
      show ims-authorization service statistics all 13
      show ims-authorization sessions full all 13
AAA Enhancements for 19.3 13
   Changes to Flow-Description AVP Flag 14
      Feature Changes 14
   Host and Realm Encoding based on Charging-Information AVP 14
      Feature Changes 14
AAA Enhancements for 19.2 14
   Customized Behavior for MSCC-Level Grant and FUI 15
      Feature Changes 15
   Destination-Host AVP in Redirected Requests 15
      Feature Changes 15
      Command Changes 16
         destination-host-avp 16
   Enhancements to Suppress USU in CCR for Blacklisted Content 17
      Feature Changes 17
      Command Changes 17
Contents

diameter msg-type 17
Gx based Virtual APN Selection 18
   Feature Changes 18
   Command Changes 19
diameter encode-supported-features 19
Performance Indicator Changes 19
   IMSA Schema 19
   System Schema 19
   show ims-authorization policy-control statistics 19
   show ims-authorization sessions full all 19
   show session disconnect-reasons 20
   show license information 20
New Custom Dictionaries for S6b and SWm Interfaces 20
   Feature Changes 20
Support for AAA Failure Indication 20
   Feature Changes 20
   Limitations and Dependencies 21
   Performance Indicator Changes 21
   Diameter Authentication Schema 21
   show diameter aaa-statistics 22
Support for ACCESS_NETWORK_INFO_REPORT Event Trigger in dpca-custom11 Dictionary 22
   Feature Changes 22
Support for MPS-Priority AVP 22
   Feature Changes 22
Support for New RADIUS Accounting Algorithm 22
   Feature Changes 22
   Command Changes 23
   radius accounting algorithm 23
   radius accounting algorithm 23
   Performance Indicator Changes 24
   show aaa group all 24
Support for SGSN-Address AVP and SGSN_CHANGE Event Trigger 24
   Feature Changes 24
AAA Enhancements for 19.1 24
Contents

Configuration Control for Stripping Leading Digit of User-Name AVP 25
Feature Changes 25
Command Changes 25
diameter authentication strip-leading-digit 25
Performance Indicator Changes 26
show aaa group name 26
AAA Enhancements for 19.0 26
Bulk Statistics for Rule Installation Failure 26
Feature Changes 26
Performance Indicator Changes 26
IMSA Schema 26
show ims-authorization policy-control statistics 27
Compliance Requirements to Customer Specification 27
Feature Changes 27
Concatenation of Rulebase Names for 3G Subscribers 28
Feature Changes 28
Command Changes 28
radius rulebase-format 28
radius rulebase-format 29
Performance Indicator Changes 29
RADIUS Schema 29
RADIUS Group Schema 29
show radius counters all 30
show session subsystem facility aaamgr instance 30
Configuration Control for Stripping Leading Digit of User-Name AVP 30
Feature Changes 30
Command Changes 30
diameter authentication strip-leading-digit 30
Performance Indicator Changes 31
show aaa group name 31
Default Setting for Failure Handling Action for aaa-custom2 Dictionary 31
Feature Changes 31
Diameter Overload Control on P-GW and ePDG 31
Feature Changes 31
Command Changes 33
diameter authentication 33
msg-type 33
Performance Indicator Changes 33
Diameter Authentication Schema 33
IMSA Schema 34
show diameter aaa-statistics 34
show ims-authorization policy-control statistics 35
Dynamic Dictionary for S6a and S6d Interfaces 35
Feature Changes 35
Encoding of AN-GW-Address AVP in dpcacustom28 Dictionary 35
Feature Changes 35
Encoding of User-Equipment-Info AVP for HRPD RAT Type 35
Feature Changes 36
Full Checkpointing of Diameter Peer Information During Session Recovery 36
Feature Changes 36
New Diameter Attributes for Detecting Stale Message Requests 36
Feature Changes 36
Command Changes 38
msg-type 38
Performance Indicator Changes 38
DCCA Group Schema 38
Diameter Authentication Schema 38
IMSA Schema 38
System Schema 39
show active-charging credit-control statistics 39
show diameter aaa-statistics 39
show session disconnect-reasons verbose 39
New Diameter AVPs for Rf Accounting Cumulative Usage Tracking 39
Feature Changes 39
Parsing of Terminal-Information AVP on SWm Interface 40
Feature Changes 40
RADIUS Enhancements to Support IPv6 Configuration 40
Feature Changes 40
Command Changes 41
radius accounting keepalive 41
radius accounting server 41
radius attribute 41
radius charging accounting server 42
radius charging server 42
radius server 42
Performance Indicator Changes 43
RADIUS Schema 43
RADIUS Group Schema 43
show radius accounting servers 43
show radius authentication servers 43
show radius charging servers 43
show radius client status 43
show radius counters all 43
show radius counters server 43
RTT Records for PMIP P-GW Calls 44
Feature Changes 44
Saving Failed CCR-Ts in HDD for Assume Positive Sessions 44
Feature Changes 44
Command Changes 45
diameter-event 45
diameter hdd 46
diameter-hdd-module 46
file 46
show diameter-hdd-module 47
Performance Indicator Changes 48
DCCA Group Schema 48
show active-charging service all 48
show active-charging credit-control statistics 48
show cdr statistics 48
show diameter-hdd-module file-space-usage 49
show diameter-hdd-module statistics 49
Securing Integrity of SDCs on Rf Interface 50
Feature Changes 50
Command Changes 51
diameter accounting sdc-integrity 51
Performance Indicator Changes 51
  show aaa group name default 51
S-GW Failure Reporting to PCRF 51
Feature Changes 52
Command Changes 53
  diameter encode-supported-features 53
Performance Indicator Changes 53
IMSA Schema 53
  show active-charging session full all 53
  show ims-authorization policy-control statistics 53
  show ims-authorization service name 54
  show ims-authorization sessions full all 54
Time Zone Information in RAA 54
Feature Changes 54

CHAPTER 2

ADC Changes in Release 19 55
ADC Enhancements for 19.2 55
SNI Detection Support 55
Feature Changes 55
Command Changes 56
  tls 56
    clear active-charging analyzer statistics name 57
    show active-charging analyzer statistics name 57
    show active-charging flows 57
Performance Indicator Changes 58
P2P Schema 58
  show active-charging analyzer statistics name cdp 58
  show active-charging flows type cdp 58
  show active-charging ruledef name 58
SNI Rule Variable Support in EDR 58
Feature Changes 59
Command Changes 59
  rule-variable 59
Performance Indicator Changes 59
  show active-charging edr-format all 59
 CHAPTER 3

ECS Changes in Release 19  61

ECS Enhancements for 19.4  61
  Tethering Database Load on Session Managers  61
    Feature Changes  61
  UA Database File Entry Limit  62
    Feature Changes  62

ECS Enhancements for 19.3  62
  Activation/Removal of GoR through Charging-Rule-Name AVP  62
    Feature Changes  62
  ADC Rule Support over Gx for ECS rules  63
    Feature Changes  63
  ADC Rule Support based on TOS/DSCP Bearer Mapping  64
    Feature Changes  64
  Rule match for Dynamic ADC Rules  64
    Feature Changes  65

ECS Enhancements for 19.2  65
  HTTP URL Percent Encoding  65
    Feature Changes  65
  Support for Splash Pages  66
    Feature Changes  66
  Command Changes  67
    http accept  67
    http  67
    rule-variable  68
    deactivate-predefined-rule  68

Performance Indicator Changes  68
  ECS Schema  68
    show active-charging charging-action all  68
    show active-charging charging-action statistics name  68
    show active-charging flows full all  68
    show active-charging rulebase statistics name  69

ECS Enhancements for 19.0  69
  Bulk Statistics for Rule Installation Failures  69
Feature Changes 69

Performance Indicator Changes 70

ECS Schema 70

show active-charging rulebase statistics name 71

Call Drop due to Checkpoint Mismatch 73

Feature Changes 73

Change in Display Output for sn-volume-dropped-amt Attribute 73

Feature Changes 73

Group-of-Ruledefs Support for Override Control 73

Feature Changes 74

Handling of Predefined Rules in Pending List 74

Feature Changes 74

Handling of Simultaneous Delete Bearer and Create Bearer Requests 74

Feature Changes 74

New TRM Statistic Support 74

Feature Changes 75

Performance Indicator Changes 75

show active-charging rulebase statistics 75

Reporting of Usage Data During APN-AMBR Change 75

Feature Changes 75

---

CHAPTER 4 77

ePDG Changes in Release 19 77

ePDG Enhancements for 19.4 77

Send DSReq if new PGW is Selected during Re-attach 78

Feature Changes 78

Command Changes 78

ePDG Enhancements for 19.2 78

SCTP support for SWM interface 79

ePDG Service Level Threshold Parameters Monitoring Support 79

Command Changes 79

threshold 79

epdg-ikev2-authentication-failures 80

epdg-ikev2-setup-attempts 80

epdg-ikev2-setup-failure 80

epdg-ikev2-setup-failure-rate 80
epdg-ikev2-setup-success 80

ePDG Enhancements for 19.0 80

  Multiple AAA-Groups Support 81
    Feature Changes 81
  PGW FQDN Per APN Configuration Support 81
    Feature Changes 81
    Command Changes 82
      pgw-address 82
  GTP-C Load and Overload Control on ePDG 82
    Feature Changes 82
    Command Changes 82
      message-prioritization 82
  Maintain Session Uniqueness and Avoid Stale Session Processing 82
    Feature Changes 82
  AVP Support on SWm Interface 83
    Feature Changes 83
  IKE SA Establishment Failure Bulkstats Support 83
    Feature Changes 83
  New Statistics Introduced to the ePDG Schema 83
    Feature Changes 83
    Performance Indicator Changes 84
      ePDG Schema 84
  Diameter Interface Overload Control 84
    Feature Changes 84
  APN Level Statistics for VoWiFi HO 85
    Feature Changes 85
  GTP Overload Control Support 85
    Feature Changes 85
    Command Changes 86
      associate 86
  GTP Load Control Support With Peer Load Value 86
    Feature Changes 86
      associate 86
  RLF Overload Control 86
    Feature Changes 86
CHAPTER 5

GGSN Changes in Release 19 87

GGSN Enhancements for 19.6.1 87
  Handling IMEI or IMSI Mismatch During Handover 88
    Feature Changes 88
    Command Changes 88
    Performance Indicator Changes 89
      show pgw-service name <service_name> 89
      show ggsn-service name <service_name> 89

GGSN Enhancements for 19.6 90
  MS to Change QoS Parameters 90
    Feature Changes 90
    Command Changes 91
    Performance Indicator Changes 91

GGSN Enhancements for 19.4.4 91
  Handling of DHCPv6 Unicast Messages 92
    Feature Changes 92

GGSN Enhancements for 19.4 93
  IPv6 Prefix Delegation from the RADIUS Server and the Local Pool 93
    Feature Description 93
      IPv6 Prefix Delegation from the RADIUS Server 94
        How It Works 94
        Configuring APN to Enable Prefix Delegation From RADIUS Server 96
        Verifying Prefix Delegation from the RADIUS Server 97

  IPv6 Prefix Delegation from the Local Pool 98
    How It Works 98
    Configuring APN to Enable Prefix Delegation From Local Pool 99

Configuration Overview 99
  Configuring APN for Private Pool Name 99
  Configuring Prefix Delegation on Destination Context 100
    Verifying Prefix Delegation from the Local Pool 100
traffic shape 109

Performance Indicator Changes 110
  show configuration verbose 110
  show subscriber pgw-only/ggsn-only/saegw-only full all 110

Virtual APN Selection Based On PDP-Type 111
  Feature Changes 111
  Command Changes 112
    virtual-apn preference 112
  Performance Indicator Changes 112
    show apn <apn_name> 112
    show pgw-service stats all 113
    show saegw-service stats all function pgw 113

Virtual APN Selection Based on CC-Behavior 113
  Feature Changes 113
  Command Changes 114
    virtual-apn preference 114
  Performance Indicator Changes 114
    show apn <apn_name> 114
    show config 115
    show config verbose 115
    show sub ggsn-only full all 115
    show sub pgw-only full all 115
    show sub saegw-only full all 116

GGSN Enhancements for 19.0 116
  Change to the 'show gtpc' CLI Command 116
    Feature Changes 116
      Performance Indicator Changes 117
        show gtpc 117
        show gtpc summary 117

MS-to-MS traffic for IPSec 117
  Feature Changes 117
  Command Changes 118
    framed-route local-switching 118

Change in the CLI Command Output 118
  Feature Changes 118
"Newcall policy reject" Enhancement for Releasing Existing Calls 119
  Feature Changes 119
  Command Changes 119
    newcall policy 119
  Performance Indicator Changes 119
    show egtpc statistics verbose 119
Syslogging of Reject Events 120
  Feature Changes 120
    Syslogging of Reject Events 120
  Command Changes 120
    logging 120
  Performance Indicator Changes 120
    show configuration 120
IMSI/IMEI Available in System Event Logs of Type Error and Critical 120
  Feature Changes 121
    IMSI/IMEI Available in System Event Logs of Type Error and Critical 121
  Command Changes 123
    logging 123
  Performance Indicator Changes 123
    show configuration 123
  Pre-Release 8 QoS Mapping 124
  Feature Changes 124

CHAPTER 6
GTPP Changes in Release 19 125
  GTPP Enhancements for 19.2 125
    Support for Low Access Priority Indicator in CDRs 125
      Feature Changes 125

CHAPTER 7
HA Changes in Release 19 127
  HA Enhancements for 19.0 127
    Subscriber Level Support for Periodical and Event Based Idle Microcheck Point 127
      Feature Changes 127
    Command Changes 128
      timeout idle 128
      Performance Indicator Changes 128
show subscribers configuration username 128
show configuration 129
show configuration verbose 129

CHAPTER 8

HeNBGW Changes in Release 19 131

HeNBGW Enhancements for 19.2 131
SCTP stats based on henb or lenb association peerid are incorrect. 132
Feature Changes 132
Multiple HENBGW Access Services 132
Feature Changes 132
Obsoleting Existing DSCP Marking CLI 132
Feature Changes 132
CLI Configuration for QCI to DSCP Mapping Table 133
Command Changes 133
henbgw qci-dscp-mapping-table 133
dscp-marking-default 133
qci 133
Multiple Access service 133
Feature Changes 134
"Enb Config Update Failure" msg is not handled in Henbgwmgr. 134
Feature Changes 134
HeNBGW sends Reset Message to MME when access service goes down 134
Feature Changes 134
Multi Access SVC With QoS Support 134
Feature Changes 134
HeNBGW Enhancements for 19.0 135
Increase in Number of LeNBs Towards MME 135
Feature Changes 135
X2 Handover With S1u Support 136
Feature Changes 136

CHAPTER 9

HNBGW Changes in Release 19 137

HNBGW Enhancements for 19.4 137
Encode Calling Party Address in SCCP Message 138
Feature Changes 138
CHAPTER 10

HSGW Changes in Release 19 143

HSGW Enhancements for 19.1 143

Updated Value Sent for 3GPP2-BSID AVP after ULI-CHANGE Event 144

Feature Changes 144

HSGW Enhancements for 19.0 144

PMIP Part of Maintain Session Uniqueness 145

Feature Changes 145

Command Changes 145

message-timestamp-drift 145

Performance Indicator Changes 146
CHAPTER 11
IPSec Changes in Release 19 151
IPSec Enhancements for 19.6 151
Certificate and Private Key Storage 152
Feature Changes 152

CHAPTER 12
IPSG Changes in Release 19 153
IPSG Enhancements for 19.2 153
IPSG vPC-DI Qualification 154
Feature Changes 154

CHAPTER 13
L-ESS Changes in Release 19 155
L-ESS Enhancements for 19.0 155
Configuring L-ESS Application To Be Monitored Based On PSMON Process 155
Feature Changes 155
L-ESS Support in Virtual Environment 155
Feature Changes 156

CHAPTER 14
MME Changes in Release 19 157
MME Enhancements for 19.6 157

Handling of LCS Message in Idle State of UE 158

Feature Changes 158

Modified LCS Procedure Handling 158

Feature Changes 158

MME Enhancements for 19.5 159

Configurable Cause Codes Based on ODB Condition 159

Feature Changes 159

Command Changes 160

local-cause-code-mapping 160

local-cause-code-mapping 160

Enhancements to APN Remapping 161

Feature Description 161

Configuring APN Override 161

Enabling MME to Send UE Requested APN 161

Rejecting UE Requested APN with Non-standard Characters 162

Remapping UE Requested APN with Non-standard Characters 162

Monitoring and Troubleshooting the APN Override Feature 163

show configuration 163

show mme-service all 163

show mme-service session full { all | imsi | mme-service } 164

Extended EMM cause IE - E-UTRAN not allowed 164

MME Re-try of HSS initiated QoS Modification Procedure 165

MME Allows PDN-CONNECTIVITY-REQUEST with PDN-Type IPv4v6 166

New Configurable Result Codes for Mapping to EMM Cause Code 167

Feature Changes 167

Command Changes 167

diameter-result-code-mapping 167

S1 NAS Cause Code Mapping 167

Feature Description 168

How It Works 168

Configuring S1 NAS Cause Code Mapping 168

Verifying S1 NAS Cause Code Mapping 169

MME Enhancements for 19.4 170

Checking for S5/S8 PGW Data IP Address in Received CSR 170
Configurable Deactivation of PDN when CC Changes 171
Connection for Responding CLA 172
DDN Option in 'network-overload-protection' Configuration 173
Deactivation of Dedicated GBR Bearers on SCTP Failure 173
Disabling MSC Fallback on Failure Based on SRVCC Cause 174
Displaying NPU Flow-related Information for SGs Service 175
Emergency Call Support Irrespective of UE’s Advertised Algorithm Support 176
Enhanced IMEI-TAC-based Operator Policy Selection 177
Handling of CLR on Different Diameter Proxy Connections 179
HO Continues Despite Illegal ME Indication 179
IMSI_Detach_Indication Retried If UE Moves to Idle State 179
IMSI Manager Overload Control 180
Feature Description 180
Monitoring and Troubleshooting IMSI Manager Overload Control 181
Show Command(s) and/or Outputs 181
show demuxmgr statistics imsimgr all 181
Integrity and Confidentiality Algorithms for UE 182
Feature Description 182
Configuration Information 183
LI Cell Based IRI Reporting 183
Lowercase Displayed for Received APN Names 183
Disabling MSC Fallback on Failure Based on SRVCC Cause 183
Processing PDN Disconnect Requests from UE 184
Rejection of Additional PDN Connectivity Procedures 185
S1-AP Inbound and Outbound Error Statistics 185
SCTP Peer Receive Window Size 187
UE-Radio-Capability Length Increased 187
MME Enhancements for 19.3 187
Create Bearer Request during X2 HO 188
Emergency Bearer Support per TAC 188
Feature Changes 188
Command Changes 189
emergency-services-not-supported 189
Performance Indicator Changes 190
show mme-service all 190
show lte-policy tai-mgmt-db name db_name  190
show mme-service statistics mme-service mmesvc  190

Limiting ’network-feature-support-ie’  190

Paging Pre-Emption  191

SMS Behavior When VLR Is Unreliable  191

MME Enhancements for 19.2  192

Cause Code Mapping for UE-CONTEXT-RELEASE Sent from MME  192
  Feature Changes  192
  Command Changes  193
    s1-ue-context-release  193

Emergency Bearer Support per TAC  194
  Feature Changes  194
  Command Changes  195
    emergency-services-not-supported  195

Performance Indicator Changes  195
  show mme-service all  195
  show lte-policy tai-mgmt-db name db_name  195
  show mme-service statistics mme-service mmesvc  195

Event Logging  196
  Feature Changes  196
  Command Changes  196
    reporting-action  196

Performance Indicator Changes  197
  show call-control-profile full name <profile_name>  197

MME QoS Profile  197
  Feature Changes  197
  Command Changes  198
    quality-of-service-profile  198
    bearer-control-profile  199
    associate  199
    qci-reject  200
    apn-ambr  200
    dedicated-bearer or default-bearer  201
    associate  205

Operator Policy Selection Based on IMEI-TAC  206
Feature Changes 206
Command Changes 206
precedence 206

Paging Priority IE 207
Feature Changes 207
Command Changes 208
paging-priority cs 208
mpcs cs-priority 208

Performance Indicator Changes 209
show call-control profile full all 209

Purge Request Behavior 209
Feature Changes 209

TAC to LAC Mapping 209
Feature Changes 210

Target Access Restriction 210
Feature Changes 210
Command Changes for the MME 211
access-restriction-data 211
Command Changes for the SGSN 211
access-restriction-data 211

Performance Indicator Changes 212
show call-control-profile 212
show configuration verbose 212

UDPC2 Support for SGSN/MME 212
Feature Changes 213
Command Changes 213

task facility mmemgr per-sesscard-density { high | normal } 213
task facility mmemgr per-sesscard-count 214
task facility mmemgr max 215

MME Enhancements for 19.0 216

Cause Code Mapping of ESM #66 by SGSN and MME 217
Feature Changes 217
Command Changes 217
restrict access-type 217
local-cause-code-mapping apn-not-supported-in-plmn-rat 218
local-cause-code-mapping apn-not-supported-in-plmn-rat 219

Performance Indicator Changes 220
  MME Schema 220
    show configuration 220
    show apn-profile full 221
    show call-control-profile full 221
    show gmm-sm statistics verbose 221
    show mme-service name 222

CSFB for 1xRTT 222
  Feature Changes 222
  Command Changes 222
    s102-service 222
    mme-service 225

Performance Indicator Changes 225
  MME Schema 225
  S102 Schema 225
  Traps 226

DDN Throttling 226
  Feature Changes 226
  Command Changes 227
    reject 227
    ddn sgw-throttling 227

Performance Indicator Changes 228
  show lte-policy congestion-action-profile name <profile_name> 228
  show congestion-control statistics mme critical 228
  show congestion-control statistics mme major 228
  show congestion-control statistics mme minor 228
  show congestion-control statistics mme full 229

Enhanced Multimedia Broadcast Multicast Services 229
  Feature Changes 229
  Command Changes 230
    mme-embms-service 230

Performance Indicator Changes 230
  show mme-embms-service 230

GUTI Re-allocation 230
Feature Description 230
  Overview 230
How It Works 231
  Limitations 231
  Flows 232
Configuring GUTI Re-allocation 232
Monitoring and Troubleshooting GUTI Re-allocation 233
  GUTI Re-allocation Show Command(s) and/or Outputs 233
    show call-control-profile full all 233
    show session disconnect-reasons verbose 233
    show mme-service statistics 233
    show mme-service db record all 234
    show mme-service db record imsi 234
  GUTI Re-allocation Bulk Statistics 234
HSS-based P-CSCF Restoration 235
  Feature Changes 235
  Command Changes 235
    pcsf-restoration 235
  Performance Indicator Changes 236
    show call-control-profile full all 236
    show apn-profile full all 236
    show mme-service statistics 237
Local Emergency Numbers List 237
  Feature Changes 237
  Command Changes 237
    local-emergency-num 237
    local-emergency-num-ie 238
  Performance Indicator Changes 238
    show lte-policy lte-emergency-profile 238
Selective Authentication 238
  Feature Changes 239
  Command Changes 239
    authenticate attach 239
    authenticate tau 240
    authenticate all-events 240
authenticate service-request 241

Performance Indicator Changes 241

show call-control-profile full all 241

Single Level Redirection of NAPTR Requests 243

Feature Changes 243

SRVCC for 1xRTT 243

Feature Changes 244

Command Changes 244

s102-service 244

mme-service 246

Performance Indicator Changes 246

MME Schema 246

S102 Schema 247

Traps 248

Timer-based GBR Bearer Deactivation 248

Feature Changes 248

Command Changes 248

gbr-bearer-preservation-timer 248

Performance Indicator Changes 249

show call-control-profile full name <profile_name> 249

VPLMN Allowed/Not Allowed Implementation 249

Feature Changes 249

CHAPTER 15

NAT Changes in Release 19 251

NAT Enhancements for 19.0 251

Bulks Statistics Support for NBRs 251

Feature Changes 251

Performance Indicator Changes 251

ECS Schema 251

Port Chunk Count in show subscribers full Command Output 252

Feature Changes 252

Reduction of Port Chunk Size 252

Feature Changes 252

Command Changes 253

ip pool 253
Support for Dynamic Configuration of Users per NAT IP 253
Feature Changes 253
Support for Dynamic Port Chunk Size Configuration 254
Feature Changes 254

CHAPTER 16
PDSN Changes in Release 19 255
PDSN Enhancements for 19.2 255
PDSN vPC-DI Qualification 256
Feature Changes 256

CHAPTER 17
P-GW Changes in Release 19 257
P-GW Enhancements for 19.6.6 257
Re-transmitted HTTP Packet Not Dropped by ECS Even with Zero Balance 258
Feature Changes 258
Rule Matching of Re-transmitted HTTP Data Packets 258
Feature Changes 258
P-GW Enhancements for 19.6.1 259
Handling IMEI or IMSI Mismatch During Handover 259
Feature Changes 259
Command Changes 260
Performance Indicator Changes 261
show pgw-service name <service_name> 261
show ggsn-service name <service_name> 261
Handling TAU Modify Bearer Request Scenarios 261
Feature Changes 261
P-GW Enhancements for 19.5 261
Packet With Unexpected GTP Version 262
Packet With Unexpected GTP Version 262
P-GW Enhancements for 19.4.4 262
Handling of DHCPv6 Unicast Messages 263
Feature Changes 263
P-GW Enhancements for 19.4 264
IPv6 Prefix Delegation from the RADIUS Server and the Local Pool 265
Feature Description 265
IPv6 Prefix Delegation from the RADIUS Server 265
show config verbose output 276
show apn <apn_name> 277
Retaining Old IMEI Values 277
Feature Changes 277
P-GW Enhancements for 19.2 277
GTP S5/S8, S2a, and S2b Interface Specific Bulkstats for P-GW 278
Feature Changes 278
Command Changes 279
clear egtpc statistics 279
show egtpc statistics 279
Performance Indicator Changes 280
P-GW Schema 280
pgw-egtpc-s2a Schema 281
pgw-egtpc-s2b Schema 282
pgw-egtpc-s5s8 Schema 282
SAEGW Schema 282
clear egtpc statistics 283
show egtpc statistics header-decoder-errors 283
clear egtpc statistics interface-type interface-pgw-ingress 284
show pgw-service statistics all 285
show saegw-service statistics all function pgw 287
Same Packet Updated in Forwarded and Dropped Sections in APN Statistics 289
Feature Changes 289
Default Configuration Differences Between StarOS 16.3.1 and 16.4.3 289
Feature Changes 289
Performance Indicator Changes 289
show configuration 289
DHCPv6 Unicast Address Support 290
Feature Changes 290
Command Changes 290
dhcpv6-client-unicast 290
Performance Indicator Changes 291
show configuration 291
show configuration 291
show configuration verbose 291
show dhcpv6-client-profile all 291
Traffic Shaping at the APN-AMBR Data Rate Level 292
  Feature Changes 292
  Command Changes 292
    apn-ambr 292
    apn-ambr 293
    apn-ambr 293
    traffic shape 293
  Performance Indicator Changes 294
    show configuration verbose 294
    show subscriber pgw-only/ggsn-only/saegw-only full all 294
Virtual APN Selection Based On PDP-Type 296
  Feature Changes 296
  Command Changes 296
    virtual-apn preference 296
  Performance Indicator Changes 297
    show apn <apn_name> 297
    show pgw-service stats all 297
    show saegw-service stats all function pgw 297
Virtual APN Selection Based on CC-Behavior 297
  Feature Changes 297
  Command Changes 298
    virtual-apn preference 298
  Performance Indicator Changes 298
    show apn <apn_name> 298
    show config 299
    show config verbose 299
    show sub ggsn-only full all 299
    show sub pgw-only full all 299
    show sub saegw-only full all 300
P-GW Enhancements for 19.1 300
  GTP-C Load and Overload Control on P-GW 300
    Feature Changes 300
  New trap in the SNMP MIBs Reference 301
    Feature Changes 301
P-GW Enhancements for 19.0 301
  Adding Cause in the UBRsp and CBRsp 302
    Feature Changes 302
  Performance Indicator Changes 302
    eGTP-C Schema 302
    APN Schema 302
    show egtpc statistics verbose 302
Bulkstat Process Retries for Connection Attempt After Transfer Interval 303
  Feature Changes 303
  eGTP-C Statistics 303
    Feature Changes 303
Event-Based Idle Second Micro-Checkpoint Generation for P-GW 303
  Feature Changes 303
  Command Changes 304
    timeout idle 304
  Performance Indicator Changes 305
    show apn name apn_name 305
    show configuration 305
Grep Option Removed from "clear subscriber" Command 305
  Feature Changes 305
  Command Changes 305
    clear subscriber 305
GTP-C Collision Handling on P-GW 305
  Feature Changes 305
  Command Changes 306
    collision-handling dbcmd-over-mbreq 306
  Performance Indicator Changes 307
    show configuration 307
    show egtp-service all 307
GTP-C Load and Overload Control on P-GW 307
  Feature Changes 307
  Command Changes 308
    load-control-handling 308
    load-control-publishing 308
    message-prioritization 309
overload-control-handling 309
overload-control-publishing 310
self-protection-behavior 310
Performance Indicator Changes 310
show configuration 310
show gtpc-load-control-profile full all 311
show gtpc-overload-control-profile full all 311
show egtpc statistics egtp-service <egtp-service name> 312

IMSI/IMEI Available in System Event Logs of Type Error and Critical 313
Feature Changes 313
Command Changes 315
logging 315
Performance Indicator Changes 316
show configuration 316

Inclusion of Sender F-TEID in DSReq 316
Feature Changes 316
IPMS Configuration Update During VPN-ctrl Start 316
Feature Changes 316
Log Cause Values Corrected 316
Feature Changes 317

LTE to 3G Handover 317
Feature Changes 317
Maintain Session Uniqueness 317
Feature Changes 317
Command Changes 318
message-timestamp-drift 318
Performance Indicator Changes 318
LMA Schema 318
show lma-service statistics 319

"Newcall policy reject" Enhancement for Releasing Existing Calls 319
Feature Changes 319
Command Changes 319
newcall policy 319
Performance Indicator Changes 320
show egtpc statistics verbose 320
Newcall Policy Retained After Demux Migration 320
  Feature Changes 320
P-GW Overcharging Protection 320
  Feature Changes 320
Removal of APN-AMBR from the Modify Bearer Response 321
  Feature Changes 321
  Command Changes 321
    egtp 321
  Performance Indicator Changes 321
    show pgw-service all 321
RTT Support Expanded to Include PMIPv6 (S2a) 322
  Feature Changes 322
  Performance Indicator Changes 322
    System Schema 322
    show event-record statistics pgw 322
Setting of HI bit in the CSReq 322
  Feature Changes 322
Syslogging of Reject Events 323
  Feature Changes 323
  Command Changes 323
    logging 323
  Performance Indicator Changes 323
    show configuration 323

---

CHAPTER 18

PSF Changes in Release 19 325
PSF Enhancements for 19.0 325
  Support for Client and Server Port in Access Ruledefs 325
    Feature Changes 325
    Command Changes 326
      tcp client-port 326
      tcp client-port 326
      tcp server-port 326
      tcp server-port 326
      udp client-port 327
      udp client-port 327
 udp server-port 327
 udp server-port 327
 Performance Indicator Changes 327
 show active-charging ruledef firewall 327

CHAPTER 19

SAEGW Changes in Release 19 329

SAEGW Enhancements for 19.6.6 329
 Configuration for HTTP Packets with Partial Headers 330
 Feature Changes 330
 Command Changes 330
 HTTP Version Check Not Done in HTTP Analyzer 331
 Feature Changes 331
 SAEGW Enhancements for 19.5 331
 Packet With Unexpected GTP Version 332
 Packet With Unexpected GTP Version 332
 SAEGW Enhancements for 19.4.x 332
 Handling of DHCPv6 Unicast Messages 333
 Feature Changes 333
 SAEGW Enhancements for 19.4 334
 IPv6 Prefix Delegation from the RADIUS Server and the Local Pool 334
 Feature Description 334
 IPv6 Prefix Delegation from the RADIUS Server 335
 How It Works 335
 Configuring APN to Enable Prefix Delegation From RADIUS Server 337
 Verifying Prefix Delegation from the RADIUS Server 338
 show dhcpv6 statistics 338
 show sub ggsn-only full all 338
 show sub pgw-only full all 338
 show sub saegw-only full all 339
 IPv6 Prefix Delegation from the Local Pool 339
 How It Works 339
 Configuring APN to Enable Prefix Delegation From Local Pool 340
 Configuration Overview 340
 Configuring APN for Private Pool Name 340
 Configuring Prefix Delegation on Destination Context 341
Verifying Prefix Delegation from the Local Pool 341
show dhcpv6 statistics 341
show sub ggsn-only full all 342
show sub pgw-only full all 342
show sub saegw-only full all 342
IPv6 Interface ID from the RADIUS Server 342
show apn statistics 342
Limitations 343
Correction to GTPV2 Cause Source Being Incorrectly Set as S-GW 343
ECS Rules Written for IP Protocol 344
Feature Changes 344
P-GW Anchored and Co-located PDNs Incorrect Counters 344
Feature Changes 344
SPGW Incorrectly Sending UDPv6 Packets 345
Feature Changes 345
P-GW to Initiate CRA IE in UBReq Immediately 345
Feature Changes 345
IPv4v6 PDN Rejection 345
Feature Changes 346
L2TP Password Behavior Parity Between P-GW and GGSN 346
Feature Changes 346
Command Changes 347
l2tp allow-auth-without-pco 347
Performance Indicator Changes 347
show apn <apn_name> | all 347
show config verbose output 347
show apn <apn_name> 348
Retaining Old IMEI Values 348
Feature Changes 348
SAEGW Enhancements for 19.3 348
SAEGW Enhancements for 19.2 348
Enforcing Throttling to Avoid Overusage 349
Feature Changes 349
License Control for Standardized PMIP Protocol Support for NEMO 349
Feature Changes 350
Traffic Shaping at the APN-AMBR Data Rate Level 350
  Feature Changes 350
  Command Changes 351
    apn-ambr 351
    apn-ambr 351
    apn-ambr 351
    traffic shape 352
  Performance Indicator Changes 352
    show configuration verbose 352
    show subscriber pgw-only/ggsn-only/saegw-only full all 353
Virtual APN Selection Based on CC-Behavior 354
  Feature Changes 354
  Command Changes 354
    virtual-apn preference 354
  Performance Indicator Changes 355
    show apn <apn_name> 355
    show config 355
    show config verbose 356
    show sub ggsn-only full all 356
    show sub pgw-only full all 356
    show sub saegw-only full all 356
Virtual APN Selection Based On PDP-Type 356
  Feature Changes 356
  Command Changes 357
    virtual-apn preference 357
  Performance Indicator Changes 357
    show apn <apn_name> 357
    show pgw-service stats all 358
    show saegw-service stats all function pgw 358
SAEGW Enhancements for 19.1 358
SAEGW Enhancements for 19.0 358
IMSI Added to Error Logs 359
  Feature Changes 359
IMSI/IMEI Available in System Event Logs of Type Error and Critical 359
  Feature Changes 359
Command Changes 362
  logging 362
Performance Indicator Changes 362
  show configuration 362
"Newcall policy reject" Enhancement for Releasing Existing Calls 362
Feature Changes 362
Command Changes 363
  newcall policy 363
Performance Indicator Changes 363
  show egtpc statistics verbose 363
Support for S2a Standard-Based Call Flow on the SAEGW 363
Feature Changes 363
Command Changes 364
  interface-type interface-pgw-ingress 364
Performance Indicator Changes 364
  SAEGW Schema 364
  show saegw-service statistics all 364
  show saegw-service statistics all function pgw 366
  show session subsystem facility sessmgr service-type pgw-ingress debug-info verbose 367
  show subscribers saegw-only full all 369
  show subscribers saegw-only interface-type S2aGTP 370
  show subscribers summary pgw-address 370
  show subscribers summary interface-type S2aGTP 371
S-GW Collision Handling Enhancement 372
Feature Changes 372
Performance Indicator Changes 373
  show egtp statistics verbose 373
Standardized PMIP Protocol Support for NEMO on the ASR 5500 374
Feature Changes 374
Command Changes 375
  permission 375
Performance Indicator Changes 375
  show subscribers all 375
  show subscribers debug-info <pmipv6call_call_id> 375
show lma session full all 375
Syslogging of Reject Events 376
Feature Changes 376
Command Changes 376
logging 376
Performance Indicator Changes 376
show configuration 376

CHAPTER 20

SaMOG Changes in Release 19 377
SaMOG Enhancements for 19.3 377
IPv6 Transport Support Using EoGRE Access Type 378
Feature Changes 378
Command Changes 378
bind 378
DHCPv6 Service Configuration 379
Performance Indicator Changes 379
SaMOG Schema 379
show cgw-service all 380
show subscribers samog-only full 380
show samog-service all 380
show samog-service statistics 380

SaMOG Enhancements for 19.0 381
SaMOG Inter-chassis Session Recovery 381
Feature Changes 382
IPv6 Transport Support Using PMIPv6 Access Type 382
Feature Changes 382
Command Changes 382
bind (CGW Service Configuration Mode) 382
bind (MRME Service Configuration Mode) 383
Performance Indicator Changes 383
SaMOG Schema 383
show mrme-service 384
show samog-service 384
show samog-service statistics 384
show subscribers samog-only full 385
show twan-profile all 385
HTTPS Redirection for SaMOG Web Authorization 386
Feature Changes 386

CHAPTER 21

SecGW Changes in Release 19 387
SecGW Enhancements for 19.0 387
L3-ICSR Enhancement 387
Feature Changes 387
RRI and SRI Inserted Under the Particular VRF Table 388
Feature Changes 388
SecGW to Send the DNS Server IP Address to the Peer 388
Feature Changes 388
Command Changes 388
dns-server 388

CHAPTER 22

SGSN Changes in Release 19 391
SGSN Enhancements for 19.6 391
EPC ARP and Gn-Gp ARP Parameter Mapping in S4-SGSN 392
Feature Changes 392
ISRAUs Over GTPv2 for Roaming Subscribers Restricted 392
Feature Changes 392
Performance Changes 393
Processing of RAU Request On Context Response Received via GTPv2 394
Feature Changes 394
Purge Request on RAU Timer Expiry During 2G/3G to 4G TAU 395
Feature Changes 395
SGSN Enhancements for 19.5 395
Enhancement for Extended Usage of Configured Static SGSN Address 396
Feature Description 396
Configuring the SGSN-NRI Feature 397
Monitoring and Troubleshooting the SGSN-NRI Feature 397
Show Command(s) and/or Outputs 397
show gmm-sm statistics verbose 398
show call-control-profile full name 398
SGSN Enhancements for 19.4 398
APN-OI-Replacement for Gn-SGSN 398
   Feature Description 399
   How It Works 400
   Monitoring and Troubleshooting 401
Assertion Failure in Function 402
Direct Tunnel Interface Selection 402
Disc-Reason Pegging for Same R-TLLI 404
Excluding GMLC Address from UGL 405
IMSI Manager Broadcast Control 405
   IMSI Manager Broadcast Control 405
   Feature Description 406
   How It Works 406
   Configuring IMSI Manager Broadcast Control 408
   Monitoring and Troubleshooting IMSI Manager Broadcast Control 408
      Show Command(s) and/or Outputs 408
         show demuxmgr statistics imsimgr all 408
IMSI Manager Overload Control 409
   Feature Description 409
   Monitoring and Troubleshooting IMSI Manager Overload Control 410
      Show Command(s) and/or Outputs 410
         show demuxmgr statistics imsimgr all 410
IMSI Manager Attach Rate Throttling Queue 410
UPC Requests from GGSN 411
XID Requests Received during Ongoing Authentication 411
Stats Track Attach Rejects due to Same R-TLLI Collision 411
SGSN Enhancements for 19.3 411
   RTLLI Management for 2G M2M Devices 412
      Feature Description 412
      How It Works 412
      Configuring RTLLI Management 413
      Monitoring and Troubleshooting 414
SGSN Enhancements for 19.2 415
   GTPU Error Indication Enhancement 415
      Feature Description 415
      Identity Procedure for Authentication Failure 417
Feature Changes 417
Command Changes 417
  gmm perform-identity-on-auth-failure 417
Performance Indicator Changes 418
  show gmm-sm statistics verbose 418
  show gmm-sm statistics 418
Target Access Restriction 418
Feature Changes 418
Command Changes for the MME 419
  access-restriction-data 419
Command Changes for the SGSN 420
  access-restriction-data 420
Performance Indicator Changes 420
  show call-control-profile 420
  show configuration verbose 421
UDPC2 Support for SGSN/MME 421
Feature Changes 421
Command Changes 422
  task facility mmemgr per-sesscard-density { high | normal } 422
  task facility mmemgr per-sesscard-count 422
  task facility mmemgr max 423
SGSN Enhancements for 19.0 424
Cause Code Mapping of ESM #66 by SGSN and MME 425
Feature Changes 425
Command Changes 426
  restrict access-type 426
  local-cause-code-mapping apn-not-supported-in-plmn-rat 426
  local-cause-code-mapping apn-not-supported-in-plmn-rat 427
Performance Indicator Changes 428
  MME Schema 428
  show configuration 429
  show apn-profile full 429
  show call-control-profile full 429
  show gmm-sm statistics verbose 430
  show mme-service name 430
EPC QoS Attributes 430
  Feature Changes 430
  Command Changes 431
    epc-qos-params-in-gtpv1 431
    class 432
    prefer-as-cap 432
    override-arp-with-ggsn-arp 432
  Performance Indicator Changes 432
    show quality-of-service-profile full all 432
    show subscriber sgsn-only full all 433
IMSI Range Support Expanded 433
  Feature Changes 433
  Command Changes 433
    imsi-range 433
Uplink Data Status IE in Service Request 434
  Feature Changes 434
  Command Changes 434
    ignore-ul-data-status 434
  Performance Indicator Changes 435
    show call-control-profile full 435
    show gmm-sm statistics 435

CHAPTER 23
S-GW Changes in Release 19 437
  S-GW Enhancements for 19.6.6 437
    HTTP Injector Fraud When There Is No User-Agent in the HTTP 438
      Feature Changes 438
  S-GW Enhancements for 19.5 438
    Packet With Unexpected GTP Version 439
      Packet With Unexpected GTP Version 439
  S-GW Enhancements for 19.4 439
    SPGW Incorrectly Sending UDPv6 Packets 440
      Feature Changes 440
  S-GW Enhancements for 19.3 440
    Correction for Unexpected Session Deletion on the S-GW 441
  S-GW Enhancements for 19.2 441
Command Output to Show Subscriber Throughput per TAC/RAC and APN 442

Feature Changes 442
Command Changes 442
  show sgw-service statistics all 442
  show saegw-service statistics all func sgw 443
Performance Indicator Changes 443
  show sgw-service statistics all 443
  show saegw-service statistics all func sgw 443

S-GW Enhancements for 19.1 443
128k eNodeB Support 444
Feature Changes 444

S-GW Enhancements for 19.0 445
Event-Based Idle Second Micro-Checkpoint Generation for S-GW 445
Feature Changes 445
Command Changes 446
  timeout idle 446
Performance Indicator Changes 447
  show configuration 447
  show sgw-service name service_name 447

IMSI/IMEI Available in System Event Logs of Type Error and Critical 447
Feature Changes 447
Command Changes 449
  logging 449
Performance Indicator Changes 450
  show configuration 450

"Newcall policy reject" Enhancement for Releasing Existing Calls 450
Feature Changes 450
Command Changes 450
  newcall policy 450
Performance Indicator Changes 451
  show egtpc statistics verbose 451
S-GW Collision Handling Enhancement 451
Feature Changes 451
Performance Indicator Changes 452
  show egtp statistics verbose 452
CHAPTER 24

SNMP MIB Changes in Release 19 455

SNMP MIB Object Changes for 19.5 455
New SNMP MIB Objects 456
Modified SNMP MIB Objects 456
Deprecated SNMP MIB Objects 456

SNMP MIB Alarm Changes as of 19.5 456
New SNMP MIB Alarms 456
Modified SNMP MIB Alarms 456
Deprecated SNMP MIB Alarms 457

SNMP MIB Conformance Changes for 19.5 457
New SNMP MIB Conformance 457
Modified SNMP MIB Conformance 457
Deprecated SNMP MIB Conformance 457

SNMP MIB Object Changes for 19.4 457
New SNMP MIB Objects 458
Modified SNMP MIB Objects 458
Deprecated SNMP MIB Objects 458

SNMP MIB Alarm Changes as of 19.4 459
New SNMP MIB Alarms 459
Modified SNMP MIB Alarms 459
Deprecated SNMP MIB Alarms 459

SNMP MIB Conformance Changes for 19.4 459
New SNMP MIB Conformance 459
Modified SNMP MIB Alarms 460
Deprecated SNMP MIB Conformance 460

SNMP MIB Object Changes for 19.2 460
New SNMP MIB Objects 460
Modified SNMP MIB Objects 460
Deprecated SNMP MIB Objects 460
SNMP MIB Alarm Changes as of 19.2 461
  New SNMP MIB Alarms 461
  Modified SNMP MIB Alarms 461
  Deprecated SNMP MIB Alarms 462
SNMP MIB Conformance Changes for 19.2 462
  New SNMP MIB Conformance 462
  Modified SNMP MIB Conformance 462
  Deprecated SNMP MIB Conformance 463
SNMP Command Changes for 19.2 463
  SNMPV3 querie resulting unknows User. 463
  Feature Changes 463
    Secure SNMPv3 Support for SNMP Trap Handling 463
SNMP MIB Object Changes for 19.0 463
  New SNMP MIB Objects 463
  Modified SNMP MIB Objects 464
  Deprecated SNMP MIB Objects 464
SNMP MIB Alarm Changes as of 19.0 464
  New SNMP MIB Alarms 464
  Modified SNMP MIB Alarms 465
  Deprecated SNMP MIB Alarms 465
SNMP MIB Conformance Changes for 19.0 465
  New SNMP MIB Conformance 465
  Modified SNMP MIB Conformance 465
  Deprecated SNMP MIB Conformance 465
SNMP Command Changes for 19.0 466
  Increase Default Number of Notifications Required Before Propagation to SNMP Users 466
  Command Changes 466
    snmpnotif-threshold 466

CHAPTER 25
System Changes in Release 19 467
System and Platform Enhancements for Release 19.6 467
  Bounced Authentication Requests Cause Call Reject with Session Disconnect Reason 'Internal Error’ 467
  Feature Changes 468
Diagnostics Added for Nameservice Issues When Tables on CPUs Are Suspected of Containing Missing Entries 468

Feature Changes 468

System and Platform Enhancements for Release 19.3 469

Improving core transfer impact during SM recovery 469

Feature Changes 469

Command Changes 469

    crash enable async-core-transfer 469

Increase number of SSH public keys 469

Feature Changes 470

Inspector is not allowed to activate crypto-group 470

Feature Changes 470

System and Platform Enhancements for Release 19.2 470

Chassis Key must be entered for a Chassis ID to be created 470

Feature Changes 470

CLI Confirmation for Specific Exec Mode Configuration Commands 471

Feature Changes 471

Command Changes 471

    commandguard exec-command 471

Conceal/Remove ssh server Configuration Options 472

Feature Changes 472

Command Changes 473

    ssh 473

        ssh key-size 473

        ciphers 474

Only FSC Slots with Available HD Arrays Can Be Selected 474

Feature Changes 474

Command Changes 475

    hd raid 475

        hd-raid select 475

Remove obsolete-encryption Keyword in show configuration and save configuration Commands 475

Feature Changes 475

Remove showsecrets Keyword in show configuration and save configuration Commands 475
Feature Changes 475
Resetting tech-support Password Now Requires Entry of Old Password 476
Feature Changes 476
Command Changes 476
tech-support test-commands password 476
Quick Setup Wizard 477
System and Platform Enhancements for Release 19.1 477
Reload DDF device upon receipt of DDF FPGA EDCRC SEU event instead of initiating an unplanned DPC card migration 477
Feature Changes 477
Reprogramming of DDF FPGA on DPC to Reduce Outage Time 477
Feature Changes 478
System and Platform Enhancements for Release 19.0 478
Add bucket-intervals to Output of show session disconnect-reasons 478
Feature Changes 478
Command Changes 480
session disconnect-reasons bucket-interval 480
Performance Indicator Changes 480
show configuration 480
show session disconnect-reasons 481
clear session disconnect-reasons buckets 481
ASR 5500 Egress Traffic Prioritization 481
Feature Changes 481
Performance Indicator Changes 482
show npu tm 482
Automatic Reset of FSC Fabric 482
Feature Changes 482
Command Changes 483
fabric fsc-auto-recovery 483
Bulkstats to Track the Number of NEMO/Framed Routes and Total Routes per VRF 483
Feature Changes 483
Performance Indicator Changes 483
vrf Schema 483
CLI Command to Track NEMO/Framed Routes and Total Routes per VRF 484
Feature Changes 484
Command Changes 484
  threshold route-service vrf-framed-routes 484
  threshold route-service vrf-total-routes 485
Configuring a VPN Context for TACACS+ Authentication 485
  Feature Changes 485
  Command Changes 486
    on-unknown-user 486
Critical Alarm Generated for Call Reject at the Session Manager with Full Capacity 486
  Feature Changes 486
  Feature Changes 486
  Performance Indicator Changes 487
    icsrSchema 487
Improved Monitoring of NEMO Prefixes and Routes 487
  Feature Changes 487
  Performance Indicator Changes 487
    show ip framed-prefixes 487
    show ip route 488
LAG is Usable When a Minimum Number of Links are Available 488
  Feature Changes 488
  Command Changes 488
    link-aggregation 488
  Performance Indicator Changes 489
    show configuration errors 489
    show configuration link-aggregation group 489
    show configuration port 489
    show link-aggregation info group 489
    show link-aggregation table 489
    show port info 489
    show port table 489
New Version of FSC with Single 400GB SSD 490
  Feature Changes 490
  Performance Indicator Changes 490
    show card table 490
    show hd raid verbose 490
Non-blocking Message Pacing on Send Requests to Session Managers 490
  Feature Changes 490
Optimize Garbage Collection for Large Memory Block Arrays 490
  Feature Changes 491
ping and ping6 Send Configurable DSCP Value with ICMP Request 491
  Feature Changes 491
  Command Changes 491
    ping/ping6 491
  Performance Indicator Changes 491
    Output of ping/ping6 491
Reduction in Sync-Up Time with Standby ICSR Chassis 491
  Feature Changes 492
  Command Changes 492
    standby database-recovery 492
SaMOG-GW Now Supports ICSR 492
  Feature Changes 492
StarOS Authorizations for TACACS+ Users 493
  Feature Changes 493
  Command Changes 493
    priv-lvl 493
    user-id 494
  Performance Indicator Changes 494
    show tacacs priv-lvl 494
Support for LZ4 Compression Algorithm 494
  Feature Changes 494
  Command Changes 495
    checkpoint session compression 495
  Performance Indicator Changes 495
    show session subsystem facility sessmgr 495

CH A P T E R 2 6

VPC-DI Changes in Release 19 497
VPC-DI Feature Changes for 19.1 497
  Scale up distribution of BFD sessions 497
  Feature Changes 497
AAA Changes in Release 19

This chapter identifies accounting management features and functionality added to, modified for, or deprecated from AAA in StarOS 19 software releases.

- AAA Enhancements for 19.6.2, page 1
- AAA Enhancements for 19.5, page 3
- AAA Enhancements for 19.4, page 5
- AAA Enhancements for 19.3, page 13
- AAA Enhancements for 19.2, page 14
- AAA Enhancements for 19.1, page 24
- AAA Enhancements for 19.0, page 26

AAA Enhancements for 19.6.2

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the AAA Interface Administration and Reference for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Handling IMEI or IMSI Mismatch During Handover

CSCty78882 - Add Configurable option for sending CCR-U after RAR even when no categories are active

Applicable Products: GGSN, P-GW
Feature Changes

When RAR request is received and no active-category [MSCC] is present, then the P-GW sends RAR with Result-Code: Diameter Success (2001) indicating closure of transaction. The P-GW does not send any Credit-Control-Request Update (CCR-U) message as a follow up due to absence of any active categories when a Re-Authorization Request [RAR] is received from the OCS server. This may lead in billing loss. A new CLI command has been introduced, which when configured, a CCR-U is initiated following the RAR/RAA transaction, without any MSCC information in it.

**Previous Behavior**: When a RAR request is received from the OCS server and if no active-MSCCs are present, then the RAR is responded with Result-Code 2001 and no CCRU is sent.

**New Behavior**: A new CLI command has been introduced under the credit-control-group, which when configured, a CCR-U is always initiated following the RAR/RAA transaction. If there are no active-MSCCs present, then the CCR-U following the RAR will not have any MSCC.

Command Changes

diameter send-ccru on-rar

A new CLI command, **diameter send-ccru on-rar**, has been added under the credit-control-group to enable sending CCR-U (without any MSCC). The CLI ensures that a CCR-U is always sent following the RAR request. If there are no active-MSCC present, then the CCR-U is sent without MSCCs.

```bash
configure
c context context_name
 active-charging service_name
 [ default ] diameter send-ccru on-rar [ always ]
end
```

Notes:

- **default**: Resets the command to the default setting.
- **send-ccru**: Configures P-GW to send CCR-U.
- **on-rar**: Behavior on receiving RAR. Default behavior is sending CCR-U only when active Category/MSCC present.
- **always**: Always CCR-U on receiving RAR. If there are no MSCC present, then an Empty-CCRU will be sent.

Sample Configuration

credit-control group default
diameter origin endpoint cisco.com
diameter session failover
diameter dictionary dcca-custom5
failure-handling initial-request retry-and-terminate
diameter send-ccru on-rar always
exit
AAA Enhancements for 19.5

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *AAA Interface Administration and Reference* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

### Event Trigger Reporting to Local-Policy

CSCva07042 - No action taken on event(location-change) when fall back to local policy

**Applicable Products**: GGSN, P-GW

**Feature Changes**

**Previous Behavior**: When multiple events occur, only one event trigger was sent to local-policy engine. For example, when both location-change and qos-change occur, only location-change trigger was sent to local-policy.

**New Behavior**: With this release, all the event triggers are reported to the local-policy.

### Framed-IP Allocation Based on Virtual APN

CSCva14222 - frame-route and framed-ip-address AVP assignment with virtual-apn AVP

**Applicable Products**: GGSN, P-GW

**Feature Changes**

**Previous Behavior**: Framed-IP AVP value is used based on previous RADIUS authentication through the actual APN.

**New Behavior**: Framed-IP AVP is now allocated based on virtual APN configuration in the RADIUS authentication.

### Multiple Class Attribute Support

CSCva16612 - Inconsistent RADIUS Class (25) Attribute accounting handling in 3G and 4G

**Applicable Products**: P-GW
Feature Changes

In 4G, during bearer activation, when multiple class attributes are returned in RADIUS Access-Accept, only one of them was sent by P-GW towards RADIUS accounting server in Accounting-Request.

**Previous Behavior:** For custom33 dictionary and P-GW service, multiple class attributes were not supported.

**New Behavior:** With this release, for custom33 dictionary and P-GW service, multiple class attributes are supported.

Changes to Accounting-Policy

CSCva75905 - Configuration Change Caused Memory Leak in SESSMGR Process

**Applicable Products:** P-GW

Feature Changes

**Previous Behavior:** In case of multiple context, configuration of duplicate accounting-policy was allowed.

**New Behavior:** With this release, configuring duplicate accounting-policy is not allowed.

Changes in no diameter endpoint Command Output

CSCva95826 - sessmgr crashes in deletion/creation endpoints.

**Applicable Products:** All

Feature Changes

To avoid an undefined system behavior while removing diameter endpoints, a change in the output of the no diameter endpoint endpoint_name CLI command is introduced.

**Previous Behavior:** The output of the no diameter endpoint endpoint_name CLI command did not display warning message or prompted user for confirmation.

**New Behavior:** In 19.5, 21.0 and later releases, deleting the endpoint using the no diameter endpoint endpoint_name CLI command throws the following warning message and prompts for user's confirmation:

Warning: It is not recommended to remove the diameter endpoint when there are active calls on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint. Otherwise, the system behavior would be undefined.

Are you sure? [Yes|No]:

**Method of Procedure:** The following two steps should be performed in the same order to remove the Diameter endpoint:

1. To disable/breakdown the link/transport connections:
   a. Disable all the peers in the endpoint by using the diameter disable endpoint endpoint_name peer peer-name CLI command. Repeat this command for all the peers in the endpoint. This will trigger the Disconnect-Peer-Request (DPR) towards the peers with the configured disconnection cause, that is to indicate, graceful shut down.
b Remove the endpoint in the respective context, under Diameter configuration, by using the `no endpoint endpoint-name` CLI command.

2 To enable/bring up the transport connections, follow the standard procedure of adding the endpoints and corresponding peers in it.
   a Add the endpoints with "use diamproxy" option. Else, the links will be established from Session Manager via diabase library.
   b Add the corresponding peers in the endpoints.

AAA Enhancements for 19.4

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *AAA Interface Administration and Reference* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

3GPP Rel.9 Compliance for Flow-Description AVP

CScun50355 - PGW: Gx Rel10 Flow Direction AVP and GTPv2 TFT mismatch

**Applicable Products**: GGSN, P-GW, SAEGW

**Feature Changes**

Currently, PCEF is 3GPP Rel. 8 compliant for IPFilterRule in Flow-Description AVP. When PCRF sends the CCA-U/RAR with Flow-Description in Rel. 9 format during a network-initiated dedicated bearer creation or modification, PCEF was misinterpreting the source and destination IP address, resulting in sending a wrong TFT to UE.

To make the PCEF 3GPP Rel. 9 compliant for Flow-Description AVP, the following changes are implemented:

- Interpretation of the source and destination IP address in IPFilterRule in Flow-Description AVP is changed to maintain 3GPP Rel.9 compliancy. That is, when a Rel. 9 Flow-Description for UPLINK is received during a network-initiated bearer creation or modification, the source IP address is interpreted as remote and the destination as local IP address.

- Traffic flow direction is interpreted from a new Diameter AVP "Flow-Direction". This new AVP indicates the direction/directions that a filter is applicable, downlink only, uplink only or both downlink and uplink (bidirectional).

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.
Per the 3GPP Rel. 8 standards, during a network-initiated bearer creation or modification, the IPFilterRule in Flow-Description is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are sent as "permit out" and hence the usage of "permit in" is deprecated.

This behavior is applicable for 3GPP Rel. 9 compliant PCEF and PCRF only when the supported feature negotiated in CCA-I is rel. 9 or above through the `diameter update-dictionary-avps {3gpp-r9 | 3gpp-r10}` CLI command.

### Called-Station-ID AVP in CoA and DM Messages

CSCuy67680 - Ignore called-station-id received in radius CoA/DM messages

**Applicable Products:** GGSN, HA, PDSN, P-GW, SAEGW

**Feature Changes**

The gateway responds with Disconnect-Nak "Unsupported attribute" upon receiving "Called-Station-ID" attribute in the Change-of-Authorize (CoA) or DM RADIUS messages. In this release, the existing behavior is modified to ignore the value of this attribute instead of discarding the message. This change is implemented to be compliant with the RFC requirements.

**Previous Behavior:** Any CoA or DM RADIUS messages that include "Called-Station-ID" attribute were rejected and the gateway that received this message sent an acknowledgment containing Disconnect-Nak "Unsupported attribute".

**New Behavior:** If gateway receives CoA or DM RADIUS message with "Called-Station-ID" attribute, then the message is accepted and the Called-Station-ID attribute value is ignored.

This change is independent of the dictionary being configured.

### Encoding of MIP6-Agent-Info AVP in AAR

CSCuz64504 - MIP6-Agent-Info AVP shall not be present in AAR during Re-auth update

**Applicable Products:** GGSN, P-GW

**Feature Changes**

**Previous Behavior:** MIP6-Agent-Info AVP carrying P-GW identity information was sent in all AAR messages to AAA server over S6b interface. Due to the presence of this AVP in all AAR messages, the AAA server updates a wrong P-GW information on the HSS resulting in a HO failure.

AAA-Failure-Indication AVP was also encoded in the AAR message.
New Behavior: In this release, MIP6-Agent-Info and Visited-Network-Identifier AVPs are encoded only in the first AAR message, and the Visited-Network-Identifier AVP is added to aaa-custom21 dictionary. AAA-Failure-Indication AVP is not encoded as part of AAR message. This behavior change is implemented to comply with 3GPP 29.273 specification.

Customer Impact: This behavior change impacts only the customers using aaa-custom21 dictionary.

Enhancements for custom67 RADIUS Dictionary

CSCux84744 - Custom67 RADIUS dictionary enhancements

Applicable Products: GGSN, P-GW

Feature Changes

In this release, the following AVPs are added to custom67 RADIUS dictionary.

- MS-Primary-DNS-Server: This attribute indicates the IP address of primary DNS server that is used by User Equipment (UE) for the session.
- MS-Secondary-DNS-Server: This attribute indicates the IP address of secondary DNS server that is used by UE for the session.
- Acct-Input-Gigawords: This attribute indicates how many times the Acct-Input-Octets attribute has wrapped within its 32-bit field length. In effect, the number of octets received is a 64-bit integer, with this attribute representing the high 32 bits, and the Acct-Input-Octets attribute representing the low 32 bits. This attribute is not included unless it has a non-zero value.
- Acct-Output-Gigawords: This attribute indicates how many times the Acct-Output-Octets attribute has wrapped within its 32-bit field length. In effect, the number of octets received is a 64-bit integer, with this attribute representing the high 32 bits, and the Acct-Output-Octets attribute representing the low 32 bits. This attribute is not included unless it has a non-zero value.

Previous Behavior: In the case of custom67 RADIUS dictionary, MS-Primary-DNS-Server and MS-Secondary-DNS-Server AVPs were not supported in Access-Accept message. Also, the Accounting interim and Accounting stop messages did not include Acct-Input-Gigawords and Acct-Output-Gigawords AVPs.

New Behavior: MS-Primary-DNS-Server and MS-Secondary-DNS-Server AVPs are added to Access-Accept message for custom67 RADIUS dictionary. In addition to this, Acct-Input-Gigawords and Acct-Output-Gigawords AVPs are also added to Accounting-Interim and Accounting-Stop messages.

When the MS-Primary-DNS-Server and MS-Secondary-DNS-Server AVPs are received in Access-Accept, the same attributes are forwarded to UE. Accounting-Interim and Accounting-Stop messages include Acct-Input-Gigawords and Acct-Output-Gigawords AVPs whenever the input and output octets wrap around the 32-bit boundary.

Customer Impact: The changes are applicable only to custom67 RADIUS dictionary. So, this change will impact only the customers using custom67 RADIUS dictionary. In the case of accounting, peer entity also supports Acct-Input-Gigawords and Acct-Output-Gigawords AVPs. During authentication, peer node sends MS-Primary-DNS-Server and MS-Secondary-DNS-Server AVPs to UE.
Handling Redirection Message in DRA Network

CSCuy57493 - Disable checking/validation of port presence in Redirect-Host AVP

**Applicable Products**: ePDG, GGSN, HSGW, P-GW, SaMOG

### Feature Changes

**Previous Behavior**: On receiving a redirection request, the gateway checks for the presence of port number in Redirect-Host AVP. If the port is not available, the default port (3868) is used for forwarding the redirected message. Though this behavior is as per the RFC 3588, the redirection might fail when the host is connected through a DRA and the DRA uses non-default-port (i.e., port other than 3868).

**New Behavior**: The gateway no longer uses the default port (3868) in a DRA network if the port is absent in Redirect-Host AVP, but it uses the port configured within Diameter endpoint for redirection. That is, in the DRA network, the redirection will be successful even if the port is not specified in the redirect-url or the port specified does not match the value configured in the Diameter peer entity.

Location Based Local-Policy Rule Enforcement

CSCuy77896 - Location Based Local Policy Rule enforcement

**Applicable Products**: P-GW, SAEGW

### Feature Changes

This feature is introduced to activate different predefined rules for different E-UTRAN Cell Global Identifiers (ECGIs) when the subscriber is connected to a corporate APN. The subscriber has to explicitly bring down the connection with the corporate APN and re-establish session with Internet APN when out of the company area. It is assumed that corporate APN does not use PCRF and use only Local-Policy. In this case, all calls matching the APN is directed to the Local-Policy.

**Important**: For this feature to work, the license to activate Local-Policy must be configured. For more information on the licensing requirements, contact your local Cisco account representative.

To activate different predefined rules for ECGI, Local-Policy configurations are enhanced to support:

- Configuration and validation of a set of ECGIs
- Installation of ECGI_CHANGE event trigger through Change Reporting Action (CRA) event
- Detection of ECGI_CHANGE event

This feature supports the following actions to be applied based on the ECGI match with Local-Policy rule-defined condition:

- Enable a redirect rule on ECGI_CHANGE event notification when the ECGI belongs to a certain group
- Enable a wild card rule for any other ECGIs
This feature has a dependency on TAI and ECGI Change Reporting feature, which provides a framework to report ECGI-Change from session manager module to IMSA/Local-Policy module.

**Limitations**

This section identifies the known limitations of this feature.

- ECGI Change detection and triggering is a pre-requisite for this feature.
- This feature is supported for Local-Policy-only (lp-only) mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF. That is, this feature does not work in Local policy fallback mode and dual mode wherein both PCRF and Local-Policy co-exist.

**Command Changes**

**action priority**

A new keyword `ecgi-change` has been added to the existing actiondef configuration of local-policy to support ECGI-CHANGE event trigger installation.

```
configure
  local-policy-service service_name
    actiondef actiondef_name
      action priority priority event-triggers ecgi-change
    end
end
```

Notes:

- `priority priority`: Specifies a priority for the specified action. `priority` must be unique and an integer from 1 to 2048.
- `ecgi-change`: This keyword specifies to install ECGI-CHANGE event trigger. If enabled, ECGI-CHANGE event trigger is sent from local-policy.
- This CLI command is configured in local-policy if operator wants to enable ECGI-Change notification in MME by sending a CRA value.

**rule priority**

A new keyword `ecgi-change` has been added to the existing eventbase configuration of local-policy to allow taking specific action for ECGI-CHANGE event reported by MME.

```
configure
  local-policy-service service_name
    eventbase eventbase_name
      rule priority priority event ecgi-change ruledef ruledef_name actiondef actiondef_name | continue
    end
end
```

Notes:

- `priority priority`: Specifies a priority for the specified rule. `priority` must be unique and an integer from 1 to 2048.
- `ruledef ruledef_name`: Associates the rule with a specific ruledef. `ruledef_name` must be an existing ruledef within this local QoS policy service.
• **actiondef actiondef_name**: Associates the rule with a specific actiondef. *actiondef_name* must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

• **ecgi-change**: Enables a new event to detect ECGI-CHANGE and applies specific action for the ECGI-CHANGE event as defined in actiondef configuration.

• **continue**: Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

### condition priority

New keywords *ecgi*, *mcc*, *mnc*, and *eci* have been added to the existing ruledef configuration of local-policy to support matching ECGI while taking action based on event.

```bash
configure
  local-policy-service service_name
  ruledef ruledef_name
      condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq | ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value | set }
end
```

Notes:

• **priority priority**: Specifies a priority for the specified condition. *priority* must be unique and an integer from 1 to 2048.

• **ecgi mcc mcc_num mnc mnc_num eci**: Configures ECGI with values for MCC, MNC and ECI.
  * **mcc mcc_num**: MCC is a three digit number between 001 to 999. It is a string of size 3 to 3.
  * **mnc mnc_num**: MNC is a two/three digit number between 01 to 999. It is a string of size 2 to 3.
  * **eci**: ECI is a hexadecimal number between 0x1 to 0xfffffff. It is a string of size 1 to 7.

• This CLI command is configured in local-policy if operator wants to take specific action based on certain ECGI value received in ECGI-Change event notification by MME.

## Performance Indicator Changes

### show local-policy statistics summary

The following statistics are added to the output of this show command to support the ECGI-CHANGE event trigger installation:

• **Event Statistics**
  * ECGI Change - Displays the number of ECGI-CHANGE event triggers that has been received by Local-Policy.

• **Variable Matching Statistics**
  * ECGI - Displays the number of times the ECGI is matched and the specific action is applied based on the event.
New Fields in show aaa group Configuration Output

CSCux32746 - Unable to see attribute description/HD-MOde in UI & CLI show O/P for AAA

Applicable Products: ePDG, GGSN, HSGW, P-GW, SaMOG

Feature Changes

Previous Behavior: The Upgrade-dict-avps, HD-mode and HD-policy fields were not displayed in the show aaa group all command output.

New Behavior: These fields are displayed as part of the show aaa group all CLI command output. The Upgrade-dict-avps field is added to both Diameter Accounting and Authentication whereas the other two fields are displayed only under Diameter Accounting. If these parameters are configured in AAA group, then the corresponding values are displayed in the show CLI output. If they are not configured, then the default values are displayed in the show CLI output.

Performance Indicator Changes

show aaa group all

The following fields are newly added to the output of this show command.

- Diameter Authentication
  - Upgrade-dict-avps

- Diameter Accounting
  - HD-mode
  - HD-policy
  - Upgrade-dict-avps

QoS Change for Default Bearer

CSCux21694 - Unexpected Normal Release INTERIM for dedicated bearer

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Previous Behavior: In a multi-bearer call, when an update message (CCA-U or RAR) from PCRF changes the QoS (QCI/ARP) of default bearer and in the same message installs a predefined or dynamic rule on the newly updated default bearer, spurious Normal Release (NR) Service Data Volume (SDV) containers were added to Rf interim records for the dedicated bearers. In this scenario, the system used to send Normal Release buckets for the non-default bearers even if these bearers were not changed.
**New Behavior:** For a change in the QoS of default bearer, NR SDV containers will not be observed unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e., the default bearer.

### Support for Delegated-IPv6-Prefix in RADIUS Accounting Messages

CSCuz15871 - DHCPv6 PD Prefix Delegation RADIUS prefix support

**Applicable Products:** GGSN, P-GW

**Feature Changes**

Currently GGSN and P-GW support both Framed IPv6 Prefix and Delegated IPv6 Prefix from different IP pools. This feature adds support to accept both Delegated-IPv6-Prefix and Framed-IPv6-Prefix AVPs in RADIUS Access-Accept message and also encode these AVPs in RADIUS Accounting messages, if supported in the configured RADIUS dictionary.

**Previous Behavior:** The existing CLI commands `radius attribute accounting framed-ipv6-prefix` and `no radius attribute accounting framed-ipv6-prefix` were applicable for framed-ipv6-prefix only.

**New Behavior:** These CLI commands are extended to enable/disable RADIUS accounting attribute for framed ipv6 prefix and delegated ipv6 prefix, provided they are supported in the configured RADIUS dictionary.

For more information on the DHCPv6 Prefix Delegation RADIUS Prefix Support feature, see the *P-GW Enhancements for 19.4* section in this document.

### Support for TAI and ECGI Change Reporting

CSCuy73322 - User Location reporting to PGW -- IMSA Changes

**Applicable Products:** P-GW

**Feature Changes**

For activating User Location Reporting for a UE over Gx, PCRF sends RAR/CCA with the "USER_LOCATION_CHANGE (13)" event trigger. On receiving this event trigger, P-GW typically sends Change Reporting Action (CRA) Information Element (IE) with "Start Reporting" towards MME to enable the Location-Change reporting for the UE in MME.

In the current architecture, the "USER_LOCATION_CHANGE (13)" trigger is used to report the changes in User Location Information (ULI), Tracking Area Identity (TAI) and E-UTRAN Cell Global Identifier (ECGI). In release 19.4 and beyond, separate event triggers TAI_CHANGE (26) and ECGI_CHANGE (27) are supported for reporting the changes in TAI and ECGI correspondingly. CLI changes are done to display the new event triggers in show configuration commands.

**Important**

For TAI reporting to work, the `diameter map usage-report` CLI command must be configured in Policy Control configuration mode to use the value 33.

PCRF subscribes to the CRA event for reporting change of TAI and ECGI. P-GW sends event trigger in CCR-U only if it is subscribed by PCRF. When PCRF installs the event trigger for ECGI Change and/or TAI change, any change in ECGI and TAI (based on installed triggers) is reported.
The TAI and ECGI Change Reporting feature complies with 3GPP TS 29.212 v9.7.0. This feature is supported on Gx interface so that UE can be tracked on ECGI/TAI change and reported to PCRF. For more information on the User Location Information Reporting feature, see the administration guide for the product that you are deploying.

**Previous Behavior**: The CRA event included in Create Session Response (CSRsp) for reporting location change was always set to START_REPORTING_ECGI (4).

**New Behavior**: The CRA value varies based on the event triggers received from PCRF.

Change Reporting Support Indication (CRSI) and ULI are also supported in Bearer Resource Command. P-GW sends the ULI received in Delete Bearer Command from MME to PCRF when the corresponding Delete Bearer Response is received. When the ULI is included in both Delete Bearer Command and Delete Bearer Response, the ULI in Delete Bearer Response is sent to the PCRF. In the absence of ULI in Delete Bearer Response, then the ULI received in Delete Bearer Command is sent to PCRF.

**Performance Indicator Changes**

**show ims-authorization service statistics all**

The following statistics are added to the output of this show command in support of this feature:

- TAI Change - Displays the total number of times P-GW has reported TAI_CHANGE (26) event trigger to PCRF.
- ECGI Change - Displays the total number of times P-GW has reported ECGI_CHANGE (27) event trigger to PCRF.

**show ims-authorization sessions full all**

The following fields are added to the output of this show command in support of this feature:

- TAI-Change - Displays this event trigger when TAI has changed for a subscriber session.
- ECGI-Change - Displays this event trigger when ECGI has changed for a subscriber session.

**AAA Enhancements for 19.3**

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *AAA Interface Administration and Reference* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.
Changes to Flow-Description AVP Flag

CSCux33057 - Dynamic rule failing if only TOS class AVP is configured

**Applicable Products:** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

**Feature Changes**

**Previous Behavior:** IMSA used to reject PCC rules when PCRF sends the Flow-Information AVP without including Flow-Description AVP. The Flow-Description AVP was defined as a mandatory AVP in r8-gx-standard and dpca-custom15 dictionaries.

**New Behavior:** Flow-Description AVP is made optional in the Flow-Information grouped AVP for r8-gx-standard and dpca-custom15 dictionaries. This change is implemented to be compliant with 3GPP TS 29.212 V9.3.0 (2010-06) specification.

With this change, the rules are passed to ECS for further processing.

**Customer Impact:** Flow-Information AVP can be sent without Flow-Description AVP too.

Host and Realm Encoding based on Charging-Information AVP

CSCuw42110 - OCS realm and host should be separable based on Gx-Charging-Information

**Applicable Products:** GGSN, HA, IPSG, PDSN, P-GW

**Feature Changes**

In this release, ASR5k provides the flexibility to extract the destination host and destination realm from Charging-Information AVP received from PCRF through Gx interface. This functionality is supported to be compliant with 3GPP standard spec 29.212 and 29.229.

**Important**

This functionality is currently applicable only to dcca-custom32 and dcca-custom26 dictionaries.

**Previous Behavior:** In the case of HTTP Redirection, Destination-Host and Destination-Realm AVPs were encoded based on the values obtained through CLI configuration and not the value received from PCRF or OCS server.

**New Behavior:** Both the Destination-Host and Destination-Realm AVPs are encoded based on the values received from PCRF or OCS in Charging-Information or Redirect-Host AVP.

AAA Enhancements for 19.2

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *AAA Interface Administration and Reference* for this release.
Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Customized Behavior for MSCC-Level Grant and FUI

CSCuw38105 - FUI behavior incorrect with both CC-Time and CC-Total-Octets

Applicable Products: GGSN, HA, IPSG, PDSN, P-GW

Feature Changes

A new Diameter dictionary "deca-custom31" is defined to support the customized FUI behavior when multiple granted quota types are available at MSCC.

Important This behavioral change is applicable to 18.3.5 and later releases.

Previous Behavior: When FUI AVP (only TERMINATE action is applied) is received at command level, then the gateway waits for all MSCCs to exhaust its quota before the session is terminated. No special treatment was available for quota grants. For example, a GSU grant with "CC-Total-Octets = 0" and a non-zero value of CC-Time was treated as "normal quota".

This behavior remains the same for the FUI received at MSCC level, but supporting all the three FUI actions (TERMINATE, REDIRECT and RESTRICT_ACCESS).

New Behavior: When command-level FUI is received and FUA is TERMINATE, and MSCC-level GSU is received along with FUI in CCA-U, then the gateway treats the MSCC for which "CC-Total-Octets =0" as quota expired and it waits until all the MSCCs exhaust any of the available quotas before the final action is taken.

When MSCC level FUI is received with multiple grant quota types, and CC-Total-Octets =0 irrespective of the CC-Time value in GSU, the PCEF immediately executes the specified FUI action only for deca-custom31 dictionary.

Destination-Host AVP in Redirected Requests

CSCuu63094 - Supporting an option to include Destination-Host AVP during redirection

Applicable Products: ePDG, P-GW, SaMOG

Feature Changes

Important This enhancement is applicable to 18.4.3 and later releases.
When an application receives the Result-Code 3006 -DIAMETER_REDIRECT_INDICATION from the AAA server, the Diameter request message is forwarded to the Redirect-Host specified in the server's response. The message gets routed properly in case the Diameter host is directly connected to the AAA server. If there is a DRA between P-GW/ePDG and AAA server, the message goes into a loop as DRA always routes the packet to the AAA server which had redirected the message. To overcome this problem, the Destination-Host AVP should be included in the redirected messages. This functionality is supported by extending the existing CLI command "destination-host-avp" to include "redirected-request" as an optional configuration.

This option "redirected-request" encodes Destination-Host AVP in any type of Diameter redirected messages. Since any redirected request is considered as retried request, if the option "retried-request" is used, by default Update (Interims) or Terminate (Stop) redirected-request will be encoded with Destination-Host AVP without the "redirected-request" option being configured. The reason to configure "redirected-request" as part of "retried-request" option is, in case of Initial-Retried request the Destination-Host AVP is not encoded if "retried-request" option alone is configured. To enable encoding Destination-Host AVP for Initial-Retried request, "redirected-request" is supported as an extension to "retried-request" as well.

**Previous Behavior**: Destination-Host AVP was encoded in the redirected message only if the original request included Destination-Host AVP.

**New Behavior**: The encoding of Destination-Host AVP in redirected message is based on the new configurable option redirected-request in "destination-host-avp" CLI command. If the CLI command is enabled, Destination-Host AVP will be included in any type of Diameter redirected messages. As per the current implementation, it is not possible to send retried messages to a different host using the same peer. This behavior is applicable for normal retry and failure-handling scenarios.

### Command Changes

**destination-host-avp**

The existing destination-host-avp CLI command has been enhanced to include an optional keyword redirected-request to enable encoding of Destination-Host AVP in the redirected message.

```bash
configure
call-context context_name
diameter endpoint endpoint_name
destination-host-avp { always | initial-request | retried-request | redirected-request | | retried-request | | session-binding | redirected-request | }
default destination-host-avp
end
```

**Notes:**

- **redirected-request**: Encodes the Destination-Host AVP in any redirected request message.
- **always**: Encodes the Destination-Host AVP in all types of request messages.
- **initial-request**: Encodes the Destination-Host AVP in initial request but not in retried request.
- **retried-request**: Encodes the Destination-Host AVP in retried request but not in initial request.
- **session-binding**: Encodes the Destination-Host AVP after the Diameter session is bound with a host.
Enhancements to Suppress USU in CCR for Blacklisted Content

CSCuv73663 - Suppressing USU in subsequent CCR for 4012/4010 cases

**Applicable Products:** GGSN, HA, IPSG, PDSN, P-GW

**Feature Changes**

ASR5K has the capability of enabling/disabling the FINAL reporting for blacklisted (4010/4012) content only in the CCR-U message. In the case of CCR-T message, there is no way to ignore the FINAL reporting for blacklisted (4010/4012) content if the FINAL was previously disabled in CCR-U. This feature is introduced to selectively control the reporting of FINAL Used-Service-Unit (USU) in CCR-T for a Rating-Group (RG) which is blacklisted using 4010 and 4012 transient result-codes. This customization is required for a seamless integration with the operator network.

This enhancement is applicable to 18.3.1 and later releases.

**Important**

**Previous Behavior:** Configuration control was available for filtering FINAL USU reporting in CCR-U for blacklisted content and in CCR-T for Final-Unit-Indication (REDIRECT/RESTRICT-ACCESS) activated content.

**New Behavior:** The current CLI configuration is enhanced to disable FINAL reporting in CCR-T message for blacklisted (4010/4012) content. The `diameter msg-type ccrt` CLI command includes a new keyword "suppress-blacklist-reporting" to support this enhancement. The default behavior of CCR-T is to send the FINAL reporting to be sent for blacklisted (4010/4012) content, if not reported already in CCR-U.

**Customer Impact:** The default behavior of this CLI configuration remains the same. When the `diameter msg-type ccrt suppress-blacklist-reporting` CLI command is configured, the FINAL report for blacklisted content is ignored in CCR-T if not sent already in CCR-U.

**Command Changes**

`diameter msg-type`

A new keyword `suppress-blacklist-reporting` is added to the `diameter msg-type ccrt` CLI command to suppress FINAL reporting in CCR-T for blacklisted content.

```cli
configure
  require active-charging
  active-charging service service_name
  credit-control group group_name
    [ no ] diameter msg-type { ccru { suppress-final-reporting } | ccrt { suppress-final-reporting | suppress-blacklist-reporting } }
end
```

**Notes:**

- **suppress-final-reporting:** When used with the `diameter msg-type ccru` command, this keyword disables immediate FINAL reporting for result code 4010/4012. When used with the `diameter msg-type ccrt` command, this keyword disables FINAL reporting for no-quota FUA Redirect/Restrict-access.
• suppress-blacklist-reporting: Disables FINAL reporting for blacklisted (4010/4012) content in CCR-T.

Gx based Virtual APN Selection

CSCuu88649 - Gx based virtual APN selection at QoS handling

Applicable Products: GGSN, P-GW, SAEGW

Related ID = CSCuu88647, CSCuu90751

Feature Changes

The current implementation supports Virtual APN (VAPN) Selection through RADIUS or local configuration. In this release, ASR5K uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

A new supported feature "virtual-apn" with feature bit set to 4 is added to the IMSA configuration. This configuration enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF sends the new APN through the Called-Station-Id AVP in CCA-I along with the Diameter Experimental Result Code 5999 (DIAMETER_GX_APN_CHANGE). The existing call is then disconnected and reestablished with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.

Important

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements. Also, note that enabling this feature might have CPU impact (depending on the number of calls using this feature).

Limitations:

• Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.

• Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.

• When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.

• If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.

• If virtual-apn is received in local-policy initiated initial message then the call will be terminated.

• When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

• This feature is not supported with DHCP relay based deferred IP address allocation and also for PPP calls.
Command Changes

diameter encode-supported-features

A new keyword virtual-apn is added to this CLI command to enable the Virtual APN Selection through PCRF.

configure context context_name
  ims-auth-service imsa-service-name
  policy control
diameter encode-supported-features virtual-apn
  { default | no } diameter encode-supported-features
  end

Notes:

• virtual-apn: This keyword enables configuration of Gx-based Virtual APN Selection feature. By default, this feature is disabled.
• This keyword is license dependent. For more information, contact your Cisco account representative.

Performance Indicator Changes

IMSA Schema

The following new bulk statistic variable is added to the IMSA schema to track the number of times the PCRF sends the new Diameter Experimental Result Code (5999) when a new virtual APN is selected.

• dpca-expres-gx-apn-change

System Schema

The following new disconnect reason is added to the System schema to track the number of times a P-GW/GGSN/SAEGW session was disconnected due to validation failure of virtual APN received from PCRF.

• gx-vapn-selection-failed (618)

show ims-authorization policy-control statistics

The following field has been added to the output of this show command to track the number of times the PCRF sends the new Diameter Experimental Result Code (5999) when a new virtual APN is selected.

• Gx APN Change

show ims-authorization sessions full all

The "Negotiated Supported Features" field in this show command output displays whether or not the Gx based Virtual APN Selection feature is configured as part of the Supported-Features AVP.
This supported feature is displayed only when the feature license is configured.

**show session disconnect-reasons**

The following new disconnect reason is added to track the number of times a P-GW/GGSN/SAEGW session was disconnected due to validation failure of virtual APN received from PCRF.

- gx-vapn-selection-failed

**show license information**

If the license to enable the Gx based VAPN Selection feature is configured, then the `show license information` command displays the associated license information.

### New Custom Dictionaries for S6b and SWm Interfaces

CSCut97277 - Create new customer specific diameter dictionaries for S6b and SWm

**Applicable Products:** ePDG, P-GW, SaMOG

**Feature Changes**

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This behavior change is applicable to 18.4.3 and later releases.</td>
</tr>
</tbody>
</table>

**Previous Behavior:** The existing AAA authentication standard dictionaries for S6b/STa/SWm interfaces encode Auth-Session-State AVP as part of client initiated requests.

That is, the Auth-Session-State AVP is present in the S6b/STa/SWm messages if the standard dictionaries for S6b/STa/SWm are configured.

**New Behavior:** Auth-Session-State AVP is excluded in the S6b/STa/SWm messages if the dictionaries "aaa-custom21" (for S6b), "aaa-custom22" (for SWm) and "aaa-custom23" (for STa) are configured. This change is implemented to be compliant with 3GPP TS 29.273.

### Support for AAA Failure Indication

CSCuu32592 - AAA-Failure-Indication AVP support

**Applicable Products:** ePDG, P-GW, SaMOG

**Feature Changes**

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This enhancement is applicable to 18.4.3 and later releases.</td>
</tr>
</tbody>
</table>

ePDG, P-GW and SaMOG connects with the AAA server over SWm, S6b and STa Diameter interfaces respectively. When a subscriber PDN connects, the PDN is authenticated over these authentication interfaces.
P-GW sends AAR whereas ePDG/SaMOG sends DER to authorize the subscriber. ePDG/P-GW/SaMOG has the capability to select one of the available AAA servers based on priority or round robin method. ePDG/P-GW/SaMOG sends DER/AAR to the selected AAA server. If the HSS indicates that the subscriber is currently being served by a different AAA server, it sends the DIAMETER_REDIRECT_INDICATION Result-Code (3006) over SWm/S6b/STa interfaces requesting ePDG/P-GW/SaMOG to redirect the AAR/DER request to the already bound AAA server.

If the redirection of DER/AAR fails for some reason (Diameter TCP connection being down or Diameter Response-Timeout), the ePDG/P-GW/SaMOG redirects this message to any other available AAA server with the AAA-Failure-Indication AVP set to 1. AAA server forwards the AAA-Failure-Indication AVP to HSS, which will reset the initial binding of the PDN with the failed AAA and bind the PDN with the AAA server that forwarded the AAA-Failure-Indication AVP.

On successful authentication at ePDG/P-GW/SaMOG, the ePDG/P-GW/SaMOG disconnects any other previously connected PDN for the same subscriber. This is done so that the PDNs are reestablished and are bound to the new AAA server.

In order to support a geo-redundant architecture for VoWiFi service, ePDG/P-GW/SaMOG supports the AAA-Failure-Indication AVP as described in 3GPP TS 29.273 specification. This AVP value is set to 1 to indicate that a previously assigned AAA Server is unavailable.

In support of this feature, a new bulk statistics field is added to the output of `show diameter aaa-statistics` command to track the number of times the AAA-Failure-Indication AVP is sent over these authentication interfaces.

**Limitations and Dependencies**

This section identifies the known limitations and dependencies for this feature.

- It is assumed that the Redirect-Host AVP contains a valid known host. If the host is invalid, ePDG/P-GW/SaMOG will terminate the connecting PDN.

- When the AAA server sends redirection indication, it is expected that the Result-Code is 3006 (DIAMETER_REDIRECT_INDICATION) and it should also send the Redirect-Host-Usage AVP with its value as 1 (ALL_SESSION) and set the Redirect-Max-Cache-Time AVP to the validity time for the Redirect-Route to exist. By default, the Redirect-Host-Usage is DON'T-CACHE (0) and in this scenario, only the redirected message will be forwarded to Redirect-Host. Any further messages belonging to the same Diameter session will undergo a fresh route-lookup and might contact a different AAA server.

- AAA-Failure-Indication AVP is included only in these Diameter dictionaries:
  - `aaa-custom21` for S6b
  - `aaa-custom22` for SWm
  - `aaa-custom23` for STa

**Performance Indicator Changes**

**Diameter Authentication Schema**

The following new bulk statistic variable is added to this schema to track the number of times AAA-Failure-Indication AVP is sent to AAA server over Diameter Authentication interfaces.
• aaa-failure-indication

show diameter aaa-statistics

The following field is added to the output of this show command to track the number of times
AAA-Failure-Indication AVP is sent over Diameter Authentication interfaces.

• AAA-Failure-Indication

Support for ACCESS_NETWORK_INFO_REPORT Event Trigger in dpca-custom11 Dictionary

CSCux12821 - Support for ACCESS_NETWORK_INFO_REPORT in dpca-custom11
Applicable Products: P-GW

Feature Changes
To support Network Provided Location Information (NPLI) feature, the ACCESS_NETWORK_INFO_REPORT
event trigger is supported and the Required-Access-Info AVP is included in dpca-custom11 dictionary.

Support for MPS-Priority AVP

CSCuv04515 - Diameter support needed for MPS-Priority AVP
Applicable Products: MME
Related CDETS ID = CSCuv04515

Feature Changes
A new Diameter AVP "MPS-Priority" is added to the grouped AVP "Subscription-Data" and included in the
s6a-standard dictionary as indicated in the 3GPP 29.272 specification. This AVP is required for Circuit
Switched (CS) fallback (CSFB) high priority paging support in MME.

Support for New RADIUS Accounting Algorithm

CSCuw31408 - Change PGW Radius Server State behavior after Failure recovery
Applicable Products: GGSN, P-GW, S-GW

Feature Changes
A new RADIUS accounting server selection algorithm "first-server fallback" is introduced. This algorithm
is an extension of the existing "first-server" algorithm.
This new algorithm behaves similar to "first-server" algorithm, i.e. the accounting data is sent to the highest
priority RADIUS/mediation server at any point of time.
If the highest priority server is not reachable, accounting data is sent to the next highest priority server. The difference between "first-server" and "first-server fallback" is that, with the new algorithm, if a higher priority server recovers, all new RADIUS requests of existing sessions and new accounting sessions are sent to the newly available higher priority server. In the case of "first-server" algorithm, the accounting requests of existing sessions continued to be sent to the same server to which the previous accounting requests of those sessions were sent.

**Limitations**

The following are the two scenarios during which the requests might be sent to lower priority servers even though a higher priority server is available:

- When `radius max-outstanding` command or `max-rate` is configured, there are chances that the generated requests might be queued and waiting to be sent when bandwidth is available. If a higher priority server recovers, the queued requests will not be switched to the newly available higher priority server.
- When a higher priority server becomes reachable, all existing requests, which are being retried to a lower priority server, will not be switched to the newly available higher priority RADIUS server.

**Command Changes**

`radius accounting algorithm`

A new keyword `fallback` is added to this command under Context Configuration mode to support a new RADIUS accounting algorithm. This algorithm will send accounting data to the highest priority available RADIUS/mediation server at any point of time.

```plaintext
configure
  context context_name
    radius accounting algorithm first-server fallback
  end

Notes:

  - `fallback`: Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. When the server is unreachable, accounting data is sent to the server with the next highest configured priority. If a higher priority server recovers back, the accounting requests of existing sessions and new sessions are sent to the newly recovered server.
```

`radius accounting algorithm`

A new keyword `fallback` is added to this command in the AAA Group Configuration mode to support a new RADIUS accounting algorithm. This algorithm will send accounting data to the highest priority available RADIUS/mediation server at any point of time.

```plaintext
configure
  context context_name
  aaa group group_name
    radius accounting algorithm first-server fallback
  end

Notes:

  - `fallback`: Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. When the server is unreachable, accounting data is sent to the server with the next highest configured priority. If a higher priority server recovers back, the accounting requests of existing sessions and new sessions are sent to the newly recovered server.
```
highest configured priority. If a higher priority server recovers back, the accounting requests of existing sessions and new sessions are sent to the newly recovered server.

Performance Indicator Changes

show aaa group all

The existing field "Algorithm" displays the configured RADIUS accounting algorithm in the output of this show command.

If this new algorithm is configured, then "First-server-fallback" is displayed as the configured value.

Support for SGSN-Address AVP and SGSN_CHANGE Event Trigger

CSCuv94938 - SGSN-address and SGSN_Change event trigger for pgw/ggsn

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

A new customer-specific Diameter dictionary "dpca-custom30" has been defined based on r8-gx-standard dictionary to meet customer's requirements. When this dictionary is configured under Policy Control Configuration mode, P-GW/SAEGW sends the SGSN-Address AVP and SGSN_CHANGE event trigger irrespective of the UE access type (LTE, ePDG, SAMOG, etc). This feature works efficiently with S5/S8, S2a and S2b interfaces.

Important

This feature is customer-specific. Contact your Cisco account representative for more information.

During the handoff, SGSN_CHANGE event trigger is sent instead of AN_GW_CHANGE event trigger and 3GPP-SGSN-Address AVP is sent in CCR-U instead of AN-GW-Address AVP.

Limitations:

• This feature is applicable only for SGSN IPv4 address. For SGSN IPv6 address, the 3GPP-SGSN-IPv6-Address AVP is not sent.

• This feature is applicable only to GGSN/WLAN/P-GW calls and not applicable to eHRPD.

AAA Enhancements for 19.1

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the AAA Interface Administration and Reference for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.
Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Configuration Control for Stripping Leading Digit of User-Name AVP

CSCu63006 - Adding cli for feature of removing leading digit in user name avp

Applicable Products: ePDG, HSGW, P-GW

Feature Changes

Important: This feature was initially supported as lab quality in 19.0 and released as deploy quality in 19.1.

As part of 2015 4G network upgrade release, no leading digit is included in the User-Name AVP of non-authentication procedures like AAR and STR. For backward compatibility, the 3GPP AAA server accepts User-Name with and without the leading digit.

To control the stripping of leading digit in the User-Name AVP, a new CLI command diameter authentication strip-leading-digit user-name is introduced at AAA Server Group level. This feature is applicable to all authentication and authorization interfaces like S6b, STa and SWm and not for accounting interfaces. This CLI command is applicable only for AAR and STR messages.

If the User-Name AVP is received in RAR (for SWm and STa), the same User-Name is included in the RAA message irrespective of the CLI option. For example, if the User-Name AVP is prefixed with 0 in RAR and the CLI option for stripping is enabled, then the User-Name AVP is sent in RAA with the leading "0".

Command Changes

diameter authentication strip-leading-digit

A new keyword strip-leading-digit is added to this CLI command to enable or disable stripping of leading digit from User-Name AVP of non-authentication procedures like AAR and STR.

configure

c context context_name

  aaa group group_name

  [ no ] diameter authentication strip-leading-digit { user-name }

end

Notes:

- strip-leading-digit: Strips off leading digit from User-Name AVP of non-authentication procedures. By default, this feature is disabled.
- This CLI command will not take effect for aaa-custom17 and aaa-custom19 dictionaries.
- This CLI is not applicable for response messages (RAA/ASA) sent by chassis.
Performance Indicator Changes

show aaa group name

The following field is added to the output of this show command to indicate the configuration status of this feature.

- Strip-leading-digit user-name

AAA Enhancements for 19.0

This section identifies all of the AAA (including Diameter and RADIUS) enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *AAA Interface Administration and Reference* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

Bulk Statistics for Rule Installation Failure

CSCup51941 - IMSA changes for pegging stats for Rule Installation failure

**Applicable Products:** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

**Related ID** = CSCuc60371

**Feature Changes**

New bulk statistics variables and counters were introduced to track the various reasons for dynamic PCC rule installation failures.

**Performance Indicator Changes**

**IMSA Schema**

The following new bulk statistics variables are added to the IMSA schema to track the reasons for rule installation failure at IMSA level.

- d pca-imsa-rule-install-failure-unknown-bid
- d pca-imsa-rule-install-failure-invalid-qci
- d pca-imsa-rule-install-failure-resource-limit
show ims-authorization policy-control statistics

The following fields are added to the output of this show command to track the rule installation failure reasons.

- Rule Installation Failure
  - Resource Limitation
  - Unknown Bearer ID
  - Invalid QCI
  - Invalid ARP
  - Bearer-Id in QoS

Compliance Requirements to Customer Specification

CSCuu87955 - Compliancy to Customer spec

Applicable Products: eHRPD

Feature Changes

This feature provides support to encode 3GPP-SGSN-MCC-MNC, 3GPP-Selection-Mode and Multiple-Services-Indicator AVPs in CCR messages for eHRPD calls.

Important

This is a customer-specific implementation to meet the spec compliance requirements.
Concatenation of Rulebase Names for 3G Subscribers

CSCut84538 - Concatenated rulebase name for 3G

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

Currently, the Wireless Mobile Private Network (MPN) configures a dedicated rulebase per service. The Enterprise that utilizes this service has the rulebase per subscriber in 3G or signaled from AAA server with SN1-Rulebase attribute. In the case of a prepaid service, the rulebase name will be the customer-specific prepaid policy attribute received from the AAA server.

When both the RADIUS attributes are received, the last received attribute is considered and applied to the subscriber session. In this release, for a 3G CDMA call, the AAA server merges prepaid attribute and SN1-Rulebase as a new rulebase and then applies the new rulebase to the session on the gateway.

Important

Rulebase Concatenation is a customer-specific feature. A valid feature license must be installed prior to configuring this feature. For more information, contact your Cisco account representative.

Previous Behavior: Rulebase was a single attribute value as obtained in the RADIUS Access-Accept response message. That is, only one rulebase can be applied with either SN1-Rulebase AVP or customer-specific prepaid policy AVP, whichever comes last.

New Behavior: When both the attributes are received, the rulebase name will be a concatenation of the attributes as received in the Access-Accept response message. If only one of the attributes is received, the current behavior is applicable i.e. the last received attribute will be selected as the rulebase and it will be applied to the session.

If the concatenated rulesbase is not matching with the rulebase configured on the gateway, and/or if both the attributes are present more than once, then the session is rejected.

New CLI configurations are added in APN and subscriber configuration modes to support rulebase concatenation. The new CLI is controlled through a customer-specific license.

Customer Impact: This feature implementation helps the MPN to customize the rulebase and combine prepaid service with additional services like Service Based Access (SBA).

Command Changes

radius rulebase-format

This new CLI command is configured at APN level to enable/disable the Rulebase Concatenation feature. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase. If the Rulebase Concatenation feature is not enabled, the last received rulebase is applied to the session.

configure
context context_name
apn apn_name
radius rulebase-format { custom1 | standard }
default radius rulebase-format standard
end

Notes:

• **custom1**: Identifies the rulebase as a custom value derived from multiple attributes in the RADIUS Access-Accept response message.

• **standard**: Identifies the rulebase as a single attribute value as obtained in RADIUS Access-Accept response message. The default setting is **standard**.

**radius rulebase-format**

This new CLI is configured at the subscriber level to enable/disable the Rulebase Concatenation feature. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase. If the Rulebase Concatenation feature is not enabled, the last received rulebase will be applied to the session.

```bash
configure
ccontext context_name
  subscriber { default | name subscriber_name }
  radius rulebase-format { custom1 | standard }
  default radius rulebase-format standard
end
```

Notes:

• **custom1**: Rulebase is a custom value derived from multiple attributes in the RADIUS Access-Accept response message.

• **standard**: Rulebase is a single attribute value as obtained in RADIUS Access-Accept response message. The default setting is **standard**.

**Performance Indicator Changes**

**RADIUS Schema**

The following bulk statistic variable has been added in this schema to track session rejection scenario in RADIUS server level.

• malformed-rulebase-authrsp – Total number of authentication responses received with multiple rulebase attributes

**RADIUS Group Schema**

The following bulk statistic variable has been added in this schema to track session rejection scenario in RADIUS server group level.

• malformed-rulebase-authrsp – Total number of authentication responses received with multiple rulebase attributes
show radius counters all

The following field has been added to the output of this show command to track the failure scenarios of multiple rulebase attributes' presence in the RADIUS server level.

• Access-accept Malformed Rulebase Received

show session subsystem facility aaamgr instance

The following field has been added to the output of this show command to track the failure scenarios of multiple rulebase attributes' presence in the AAA manager level.

• Total radius malformed auth responses

Configuration Control for Stripping Leading Digit of User-Name AVP

CSCuv63006 - Adding cli for feature of removing leading digit in user name avp

Applicable Products: ePDG, HSGW, P-GW

Feature Changes

Important

This feature is currently supported as lab quality only.

As part of 2015 4G network upgrade release, no leading digit is included in the User-Name AVP of non-authentication procedures like AAR and STR. For backward compatibility, the 3GPP AAA server accepts User-Name with and without the leading digit.

To control the stripping of leading digit in the User-Name AVP, a new CLI command diameter authentication strip-leading-digit user-name is introduced at AAA Server Group level. This feature is applicable to all authentication and authorization interfaces like S6b, STa and SWm and not for accounting interfaces. This CLI command is applicable only for AAR and STR messages.

If the User-Name AVP is received in RAR (for SWm and STa), the same User-Name is included in the RAA message irrespective of the CLI option. For example, if the User-Name AVP is prefixed with 0 in RAR and the CLI option for stripping is enabled, then the User-Name AVP is sent in RAA with the leading "0".

Command Changes

diameter authentication strip-leading-digit

A new keyword strip-leading-digit is added to this CLI command to enable or disable stripping of leading digit from User-Name AVP of non-authentication procedures like AAR and STR.

configure
  context context_name
    aaa group group_name
[ no ] diameter authentication strip-leading-digit { user-name }
end

Notes:

- **strip-leading-digit**: Strips off leading digit from User-Name AVP of non-authentication procedures. By default, this feature is disabled.
- This CLI command will not take effect for aaa-custom17 and aaa-custom19 dictionaries.
- This CLI is not applicable for response messages (RAA/ASA) sent by chassis.

**Performance Indicator Changes**

`show aaa group name`

The following field is added to the output of this show command to indicate the configuration status of this feature.

- Strip-leading-digit user-name

**Default Setting for Failure Handling Action for aaa-custom2 Dictionary**

CSCuv74175 - Restore default CCFH behavior of 5xxx result codes in SWm interface

**Applicable Products**: ePDG, HSGW

**Feature Changes**

**Previous Behavior**: Diameter messages in SWm interface were retried when 5xxx result code is received and no Credit Contol Failure Handling (CCFH) action is configured. That is, the default FH action was "retry-and-terminate" for 5xxx result codes in aaa-custom2 dictionary.

**New Behavior**: In the case of aaa-custom2 dictionary, the default CCFH action is configured as "terminate" for 5xxx result codes.

**Diameter Overload Control on P-GW and ePDG**

CSCut42292 - Support for vendor specific cause code to handle Network Overload

**Applicable Products**: ePDG, P-GW

Related CDETS ID: CSCut88698

**Feature Changes**

This feature is implemented to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. Whenever there is an overload condition at the Diameter Servers or DRA and request times out, the clients (ePDG/P-GW) are typically unaware of the overload condition and attempt to send the message on an alternate connection with the Diameter server causing some more traffic in the network. In order to handle this overload condition effectively, a new vendor-specific
Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is defined. When the overloaded PCRF/DRA receives a message, it includes the result-code 5198 in the response message. On receiving the experimental result-code, call is terminated based on the failure-handling configuration. If failure-handling is configured as local-policy, then the call is continued with local-policy without retrying the secondary server.

**Previous Behavior:** No indication was available to P-GW and ePDG when the Diameter Server or the DRA is overloaded. When a message sent to the primary link on Diameter is dropped or unanswered, P-GW/ePDG tried the same message on the secondary peer and resulted in the overloading of Diameter Server.

**New Behavior:** To support Overload Control on Gx interface, the following changes are implemented:

- A new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is added to indicate the overload state of PCRF.

- When the failure handling template is not configured and if the Experimental Result-Code (5198) is received in CCR-U, then the current call is terminated.

- If the Assume Positive feature is configured, the call is continued without retrying the secondary server.

- The default action for Experimental Result-Code error (5198) is retry and terminate. Retry and terminate will be the failure handing action irrespective of the configured value.

- New statistics are added to the output of `show ims-authorization policy-control statistics` command to display the number of times the Experimental Result-Code 5198 has been received. Separate statistics are also introduced to display the message level information.

To support Overload Control on S6b and SWm interfaces, the following changes are implemented:

- A new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is added to indicate the overload state of Diameter agent.

- Failure handling template is introduced for S6b and SWm interfaces, and associated to AAA group authentication.

- The default action for Experimental Result-Code (5198) is retry and terminate. For Diabase error, the failure-handling action will be retry and terminate irrespective of the configured value.

- When the Experimental Result-Code (5198) is received and the `failure-handling` command is configured as `continue`, then call is continued without retrying the secondary server. The `continue` action is applicable only to aaa-custom15 dictionary.

- When the Result-Code (5198) is received in DEA/AAA request, the call is terminated without the Session Terminate Request (STR) for S6b and SWm interfaces.

- New statistics are added to the output of `show diameter aaa-statistics` to indicate the number of times the specific failure handling actions are applied through the failure-handling template.

- When GGSN/P-GW receives the experimental result code 5198, the GTP cause code is mapped to NO_RESOURCES_AVAILABLE.
Command Changes

diameter authentication

A new keyword failure-handling-template is added to the diameter authentication command to associate the failure-handling with authentication under AAA group for authorization interface.

```configure
context context_name
    aaa group group_name
        diameter authentication failure-handling-template template_name
end
```

Notes:

- **failure-handling-template**: Associates the failure handling template to the authentication interface. By default, the template is not associated in the AAA Group.
- When the failure-handling-template is configured and the failure-handling CLI is also enabled in the AAA Group configuration, the template is given the higher preference.

msg-type

A new keyword without-retry is added to the msg-type command in the failure handling template configuration to fallback to local-policy without retrying the secondary server.

```configure
failure-handling-template template_name
    msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | result-code [ to end-result-code ] } | diameter exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action { continue | local-fallback | without-retry | retry-server-on-event | send-cert-on-call-termination | without-retry | retry-and-terminate | max-transmissions | without-term-req | terminate | without-term-req }
end
```

Notes:

- **without-retry**: This keyword specifies to continue the session without retrying the secondary PCRF server, when in Assume Positive mode. By default, the Diameter message is retried to secondary PCRF before falling back to local-policy.

Performance Indicator Changes

Diameter Authentication Schema

In support of the Diameter Overload Control feature, the following new bulk statistic variables are added to this schema.

- overload-ctrl-aaa
- overload-ctrl-dea
• fh-continue-retry
• fh-continue-wo-retry
• fh-retry-and-term
• fh-retry-and-term-wo-str
• fh-terminate
• fh-terminate-wo-str

**IMSA Schema**

In support of the Diameter Overload Control feature, the following bulk statistic variables are added to this schema.

• dpca-expres-overload-ctrl-ccai
• dpca-expres-overload-ctrl-ccau
• dpca-expres-overload-ctrl-ccat
• dpca-ccfh-continue-lp-wo-retry

**show diameter aaa-statistics**

The following fields are added to the output of this show command to track the number of times the Experimental Result-Code (5198) is received from PCRF.

• FH Behavior – Indicates the number of times the specific failure handling action is applied through the failure-handling-template.
  * Continue
    * With Retry
    * Without Retry
  * Retry and Terminate
    * Retry and Terminate
    * Retry Term without STR
  * Termination
    * Terminate
    * Terminate without STR

• Diameter Overload Control Stats – Indicates the number of times the Result-Code 5198 is received in a message.
  * AAA
  * DEA
show ims-authorization policy-control statistics
The following fields are added to the output of this show command to track the number of times the Experimental Result-Code (5198) is received from PCRF.
• Diameter Overload Control – Added under DPCA Experimental Result Code Stats
• Diameter Overload Control Stats
  • CCA-Initial
  • CCA-Update
  • CCA-Terminate
• Fallback – Added under FB Behavior statistics
• Fallback Without Retry – Added under FB Behavior statistics

Dynamic Dictionary for S6a and S6d Interfaces
CSCuq67272 - Dynamic dictionary support for s6a, s6d interfaces
Applicable Products: MME, SGSN

Feature Changes
In this release, the Dynamic dictionary support is extended to S6a and S6d interfaces. When the dynamic dictionary is configured under HSS Peer Service Configuration mode, the standard behavior is inherited from static dictionary and the customer-specific behavior is applied to the dynamic dictionary.

Encoding of AN-GW-Address AVP in dpca-custom28 Dictionary
CSCuv37727 - [PDSN-Gx]AN-GW-Address AVP not being sent in CCR-U
Applicable Products: HSGW

Feature Changes
Previous Behavior: For dpca-custom28 dictionary, when AN_GW_CHANGE was enabled and the PCF_CHANGE was not configured, then AN_GW_CHANGE event-trigger was sent but the AN-GW-Address AVP was not included in the CCR message.
New Behavior: The implementation is modified to send the AN-GW-Address AVP while triggering AN_GW_CHANGE event-trigger.

Encoding of User-Equipment-Info AVP for HRPD RAT Type
CSCuu88050 - MEID value in User-equipment-info for HRPD RAT type
Applicable Products: eHRPD
Feature Changes

This feature provides support to encode the MEID AVP and include it in the User-Equipment-Info grouped AVP for eHRPD calls in all Gy CCR messages.

Full Checkpointing of Diameter Peer Information During Session Recovery

CSCuu05894 - Add Diameter Peer to Micro checkpoint for all diameter interfaces

Applicable Products: ePDG, GGSN, P-GW

Feature Changes

Diameter applications like Gx and Gy does not checkpoint the Diameter peer information completely when the ICSR or Session Recovery occurs. This resulted in the subscribers contacting a different set of peers when the Diameter application level configuration is changed.

This feature is implemented to support the checkpoint and recovery of destination realm, bound peer, primary peer and secondary peer (from application-specific configuration). The subscriber session will continue to use the same peers even when the configuration changes on the standby chassis.

Previous Behavior: Diameter peer information for all session supported Diameter applications were not completely checkpointed when the ICSR and/or Session Recovery occurs.

New Behavior: The primary and secondary peer information for Gx and Gy applications are checkpointed and recovered during the failover scenario. If a session is using Gx and Gy applications, then the Diameter peers for each of these services are micro checkpointed. After the switchover, the Diameter messages applicable to the session are routed to the correct peers without being rejected.

New Diameter Attributes for Detecting Stale Message Requests

CSCuu11329, CSCus94250 - Diameter Support for Maintaining Session Uniqueness

Applicable Products: ePDG, eHRPD, GGSN, P-GW, SAE-GW

Related ID: CSCus87417, CSCut99086, CSCut88330, CSCuu01902

Feature Changes

When the ePDG/MME is reselected by the UE or when the ePDG/MME reselects a different P-GW during timeout scenarios, it is possible that the old PDN connection request is still being processed in the network and the session created by the new PDN connection request is overwritten by the stale procedure. VoLTE calls fail when such race conditions occur. Also, other stale information existing in the network elements might cause some unexpected issues.

In order to solve this problem, the implementation of ePDG/MME is modified to populate and send the Timestamp and Maximum Wait Time (MWT) private extensions in Create Session Request towards P-GW to be able to support session uniqueness.
Maintaining Session Uniqueness is a customer-specific feature. For more information, contact your Cisco account representative.

When this feature is enabled, these new Diameter attributes are included and sent to the AAA server through the initial AAR (S6b), CCR-I (Gx and Gy), and/or DER (SWm) message to maintain session uniqueness and avoid stale message processing. For more information on configuring this feature, see the **HSGW Enhancements for 19.0** or **P-GW Enhancements for 19.0** section in this guide.

- **Origination-TimeStamp** – This indicates the time (NTP synced) when the request message is sent to AAA Server from ePDG/MME. It is an 8 byte value that is encoded as the number of milliseconds elapsed since NTP time.

- **Max-Wait-Time** – This indicates the validity of the request message. It is a 4 byte value that is encoded as milliseconds and is an offset from the Origin Timestamp. If the current time at the AAA Server is greater than the Origin Timestamp + Max Wait Time, then the AAA server interprets that the ePDG/MME has timed out on the message. The Max-Wait-Time is taken as the minimum of response/request timeout in case MWT is not received from UE (applicable for Gx/Gy/S6b/SWm).

Session recovery is not supported for these attributes as this feature is applicable for initial messages.

These attributes are non-mandatory and are sent only when the customer-specific dictionary is configured. These attributes are used to identify if a message is valid and if it should be processed. AAA/PCRF/OCS server compares the Time Stamp and its own synced (NTP) time and identifies the latest session. When the message is retried to the same or different AAA server, then the origin timestamp is updated to reflect the current time.

In the case of Gx application, the Origination-TimeStamp and Max-Wait-Time AVPs are encoded in CCR-I message and applicable only for default bearer. Note that these AVPs are not applicable for dedicated bearers.

In support of this feature, a new Diameter Experimental-Result-Code "DIAMETER_NEWER_SESSION_DETECTED (5199)" is introduced. When the response message is received with 5199 result code, the Diameter application does not retry to a secondary AAA server. If the Experimental Result-Code 5199 is received in Assume Positive mode, then the current call is terminated.

DIAMETER_NEW_SESSION_DETECTED is available only as part of Experimental-Result-Code AVP. This is not supported under command level or MSCC level Result-Code AVP.

Currently, the experimental result code support is not available in result code behavior triggers for Assume Positive. So, Assume Positive is not triggered on receiving the Experimental-Result-Code (5199).

Delayed Gy occurs when CSResp has been sent to the network and upon receiving data / first packet the Gy session towards OCS is established. For this scenario, the origination timestamp will have the locally generated timestamp. This is applicable for default bearer.

Upon session termination for CCR-Initial, the cause code is sent as "EGTP_CAUSE_MULTI_PDN_CONNECTION_FOR_APN_NOT_ALLOWED (0x74)" and the disconnect reason is displayed as "newer-session-detected".
Command Changes

msg-type

The failure handling template configuration is enhanced to additionally accept the Diameter Experimental-Result-Code "DIAMETER_NEWER_SESSION_DETECTED (5199)" as the value for the diameter exp-result-code keyword.

configure

failure-handling-template template_name


end

Notes:

- diameter exp-result-code { any-error | result-code [ to end-result-code ] }: This keyword additionally accepts a new Diameter Experimental-Result-Code "DIAMETER_NEWER_SESSION_DETECTED (5199)". The current call terminates on receiving this result code if the failure handling action is configured as "terminate".

Performance Indicator Changes

DCCA Group Schema

The following new bulk statistic variable is added to this schema to indicate the number of times the Experimental Result-Code (5199) is received in the CCA-I message for Gy.

- cca-init-exp-5199-rc

Diameter Authentication Schema

The following new bulk statistic variable is added to this schema to indicate the number of times the Experimental Result-Code (5199) is received in the AAR message.

- diameter-auth-msg-exp-result-5199

IMSA Schema

The following new bulk statistic variable is added to this schema to indicate the number of times the Experimental Result-Code (5199) is received in the CCA-I message for Gx.

- dpca-imsa-exp-newer-session-detected
System Schema

The following new bulk statistic variable is added to this schema to indicate the number of times the Experimental Result-Code (5199) is received in the CCA-I message.

- cca-init-exp-5199-rc

**show active-charging credit-control statistics**

The following fields are added to the output of this show command to indicate the number of times the Experimental-Result-Code (5199) is received in the Credit Control response message.

- CCA Initial Experimental Result Code Stats
  - Exp Result Code 5199

**show diameter aaa-statistics**

The following fields are added to the output of this show command to indicate the number of times the Experimental-Result-Code (5199) is received in the authentication response message.

- Experimental Result Code Stats
  - Exp Result Code 5199

**show session disconnect-reasons verbose**

The following session disconnect reason is newly added to the output of this show command to detect the stale message requests.

- newer-session-detected(614)

---

**New Diameter AVPs for Rf Accounting Cumulative Usage Tracking**

CSCut74421 - Rf Accounting cumulative data AVPs

**Applicable Products:** GGSN, HSGW, P-GW, S-GW

**Related ID** = CSCut69338

**Feature Changes**

Two new Diameter AVPs are introduced to track the cumulative data usage for a subscriber session on a per Rating Group (RG) basis.

- Cumulative-Acct-Input-Octets: Represents the cumulative number of input octets.
- Cumulative-Acct-Output-Octets: Represents the cumulative number of output octets.
These new AVPs are added to the Service-Data-Container AVP and sent only in ACR-Interim and ACR-Stop messages for policy accounting with SDF configured or a combination of both SDF and QCI configured.

**Important**

This feature is customer-specific. For more information, contact your Cisco Account representative.

**Previous Behavior:** Service-Data-Container AVP in the Rf Accounting Request included the Accounting-Input-Packets and Accounting-Output-Packets AVPs when aaa-custom4 dictionary was used.

**New Behavior:** Service-Data-Container AVP does not contain Accounting-Input-Packets and Accounting-Output-Packets AVPs when the aaa-custom4 dictionary is used. Also, the Cumulative-Acct-Input-Octets and Cumulative-Acct-Output-Octets AVPs are newly added to the Service-Data-Container AVP to track the cumulative data usage per RG.

### Parsing of Terminal-Information AVP on SWm Interface

CSCu05734 - [ePDG] Terminal Information AVP support on SWm interface

**Applicable Products:** ePDG

**Feature Changes**

As part of this feature, ePDG is enhanced to encode and send the UE IMEI and Software Version as Terminal-Information AVP to the AAA Server through SWm interface. This AVP is sent in the DER message only when the "aaa-custom2" dictionary is used.

This attribute is required to enable the Equipment Identity Register (EIR) support on WiFi.

### RADIUS Enhancements to Support IPv6 Configuration

CSCuq34442 - IPv6 for Radius server configuration support

**Applicable Products:** GGSN, HA, PDSN, P-GW

**Feature Changes**

This feature is implemented to support IPv6 addresses in the transport layer so that the RADIUS authentication and accounting packets are sent to remote server. IPv6 address is configured for NAS-IP and RADIUS Authentication, Accounting and Mediation server addresses.

**Previous Behavior:** NAS-IP-Address attribute with type 4 was sent in the RADIUS packets.

**New Behavior:** If the IPv6 address is configured, NAS-IPv6-Address attribute with type 95 is encoded.

**Limitations:**

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In this release, a combination of IPv4 and IPv6 addresses is not supported.

- When a RADIUS server is configured in non-default AAA group without nas-ip, the NAS IP is taken from the default group. In this scenario, the IP address should be of the same transport type.
• This feature is supported for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and the same AAA group is shared, then the IPv6 address should not be configured.

• It is recommended that the primary and secondary server IP addresses should be of the same transport type.

**Command Changes**

**radius accounting keepalive**

This command is enhanced to support IPv6 address configuration for RADIUS accounting keepalive server.

```
configure
context context_name
    aaa group group_name
        radius accounting keepalive framed-ip-address ip_address
end
```

Notes:

• *ip_address*: This keyword accepts IPv4 or IPv6 address formats.

**radius accounting server**

This command is enhanced to support IPv6 address configuration for RADIUS accounting server.

```
configure
context context_name
    aaa group group_name
        radius accounting server ip_address [ encrypted ] key value | acct-on { disable | enable } ] [ acct-off { disable | enable } ] [ admin-status { disable | enable } ] [ max max_messages | max-rate max_value ] [ oldports ] [ port port_number ] [ priority priority ] [ type mediation-device | standard ] [ -noconfirm ]
end
```

Notes:

• *ip_address*: This keyword accepts IPv4 or IPv6 address formats.

**radius attribute**

This command is enhanced to support IPv6 configuration for NAS IP address.

```
configure
context context_name
    aaa group group_name
        radius attribute nas-ip-address address primary_address [ backup secondary_address ] [ nexthop-forwarding-address nexthop_address ] [ mpls-label input in_label_value | output out_label_value | output out_label_value1 | output out_label_value2 ] [ vlan vlan_id ]
end
```

Notes:

• *nas-ip-address address primary_address*: This keyword accepts IPv4 or IPv6 address formats.
• **backup secondary_address**: This keyword accepts IPv4 or IPv6 address formats.

• **nexthop-forwarding-address nexthop_address**: This keyword accepts IPv4 or IPv6 address formats.

**radius charging accounting server**

This command is enhanced to support IPv6 address configuration for RADIUS charging server.

```
configure
  context context_name
  aaa group group_name
    radius charging accounting server ip_address [ encrypted ] [ key value ] [ admin-status { disable | enable } ] [ max max_messages ] [ max-rate max_value ] [ oldports ] [ port port_number ] [ priority priority ] [ -noconfirm ]
end
```

Notes:

• **ip_address**: This keyword accepts IPv4 or IPv6 address formats.

**radius server**

This command is enhanced to support IPv6 address configuration for RADIUS server.

```
configure
  context context_name
  aaa group group_name
    radius server ip_address [ encrypted ] [ key value ] [ admin-status { disable | enable } ] [ max max_messages ] [ max-rate max_value ] [ oldports ] [ port port_number ] [ priority priority ] [ type { mediation-device | standard } ] [ -noconfirm ]
end
```

Notes:

• **ip_address**: This keyword accepts IPv4 or IPv6 address formats.
Performance Indicator Changes

**RADIUS Schema**

The following bulk statistic variables in this schema are enhanced to support IPv6 address.

- nasipaddr
- ipaddr

**RADIUS Group Schema**

The following bulk statistic variables in this schema are enhanced to support IPv6 address.

- nasipaddr
- ipaddr

**show radius accounting servers**

The output of this show command has been modified to display both IPv4 and IPv6 configurations for RADIUS accounting server.

**show radius authentication servers**

The output of this show command has been modified to display both IPv4 and IPv6 configurations for RADIUS authentication server.

**show radius charging servers**

The output of this show command has been modified to display both IPv4 and IPv6 configurations for RADIUS charging server.

**show radius client status**

The output of this show command has been modified to display both IPv4 and IPv6 configurations for NAS-IP-Address.

**show radius counters all**

The output of this show command has been modified to display both IPv4 and IPv6 configurations.

**show radius counters server**

The output of this show command has been modified to display both IPv4 and IPv6 configurations.
RTT Records for PMIP P-GW Calls

CSCut82619 - RTT support to be expanded to include PMIPv6 (S2a) diameter

**Applicable Products:** eHRPD

### Feature Changes

In Release 18, Real Time Tool (RTT) feature was introduced to enable P-GW to generate event records containing a series of fields or IEs at the completion of specific Diameter and GTPv2 procedures. This feature was supported only for LTE/WLAN call types. Now, this support is extended to eHRPD PMIPv6 (S2a) calls.

**Important**
This feature is customer-specific. Contact your Cisco account representative for more information.

The event records are made available to customers in CSV file format through their RTT system. This feature allows for near real time monitoring of the LTE network.

**Previous Behavior:** When the RTT feature was enabled under APN, RTT records were generated only for GTP P-GW calls.

**New Behavior:** On enabling this feature, RTT records are generated for both GTP and PMIP P-GW calls.

**Customer Impact:** The record count might increase when this feature is enabled.

## Saving Failed CCR-Ts in HDD for Assume Positive Sessions

CSCut84032 - Gy write file on PGW HD during assume positive

**Applicable Products:** HA, P-GW

### Feature Changes

In the existing implementation with Assume Positive feature, there are high chances of losing the usage data reported through the CCR-T when the session is being terminated while in Assume Positive mode. This problem is addressed by allowing the DCCA module to write the CCR-T messages in the Hard Disk Drive (HDD) of the chassis.

In cases where the Assume-Positive interim-quota is allocated, and CCR-T is not reported/answered, the CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.

**Important**
This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

This feature is controlled through a new CLI command "**diameter hdd**" introduced in the Credit Control Group configuration mode. When the CLI configuration is enabled, the Gy application sends the failed CCR-T messages to the CDR module for storing in the HDD.
This feature is applicable only when Assume Positive feature is enabled.

Limitations:

- When an ICSR event occurs unexpectedly before the CCR-T is written, the CCR-T will not be written to
  the HDD and hence the usage will be lost.
- It is expected that the customers requiring this feature should monitor the HDD periodically pull
  and delete the files so that the subsequent records can be buffered.

Previous Behavior: The usage counts that are reported on Gy are dropped if the CCR-T does not successfully
reach OCS.

New Behavior: When an Assume Positive session terminates, the usage counts that are not reported to OCS
are written to a local file.

Command Changes

diameter-event

This is a new command in the Diameter HDD Module Configuration mode to configure the HDD specific
parameters.

configure context context_name
diameter-hdd-module
diameter-event { purge { storage-limit storage_limit | time-limit time_limit } | max-files
max_records_to_purge } | push-interval push_interval | push-trigger space-usage-percent trigger_percentage
| remove-file-after-transfer | transfer-mode { pull [ module-only ] | push primary { encrypted-url
encrypted_url | url url } | max-files max_records | max-tasks task_num | module-only | secondary { encrypted-secondary-url encrypted_secondary_url | secondary-url secondary_url } | via local-context
| + | use-harddisk }

default diameter-event | purge | push-interval | push-trigger space-usage-percent |
remove-file-after-transfer | transfer-mode | module-only | push via | use-harddisk ] +
no diameter-event | purge | remove-file-after-transfer | use-harddisk ] +
end

Notes:

- **purge**: Specifies to purge/delete the Diameter records based on "time" or "volume" limit.
- **push-interval**: Specifies the transfer interval (in seconds) to push Diameter files to an external server.
- **push-trigger**: Specifies the record disk space utilization percentage, upon reaching which an automatic
  push is triggered and files are transferred to the configured external server.
- **remove-file-after-transfer**: Specifies that the system must delete Diameter files after they are transferred
to the external server. Default: Disabled
• **transfer-mode**: Specifies the file transfer mode—how the Diameter files are transferred to the external server.

• **use-harddisk**: Specifies that the hard disk be used to store Diameter files.

### **diameter hdd**

This new CLI command is used to enable/disable the HDD to store the failed CCR-T messages for the corresponding credit control group.

```plaintext
configure
  require active-charging-service
  active-charging-service service_name
  credit-control group ccgroup_name
  [ no ] diameter hdd
end
```

**Notes:**

- **diameter hdd**: This CLI enables/disables the HDD to store the failed CCR-T messages. When enabled, the Gy application sends the failed CCR-T messages to the CDR module for storing in the HDD. By default, this feature is disabled.

- **no diameter hdd**: Removes the HDD configuration for DCCA.

### **diameter-hdd-module**

This new CLI command is used to configure the HDD module for saving the failed CCR-T messages. This command enters the Diameter HDD Module Configuration mode.

```plaintext
configure
  context context_name
  diameter-hdd-module
end
```

### **file**

This is a new command in the Diameter HDD Module Configuration mode to configure the file creation properties for Diameter records.

```plaintext
configure
  context context_name
  diameter-hdd-module
```
show diameter-hdd-module

This new CLI is used to display the HDD module configuration information.

**Important** This command is license dependent. For more information, contact your Cisco account representative.

show diameter-hdd-module { file-space-usage | statistics }

Notes:

- **file-space-usage**: Displays the hard-disk space utilization for the HDD module.
- **statistics**: Displays statistics for the credit-control-event module.
Performance Indicator Changes

DCCA Group Schema

The following bulk statistic variable has been added in this schema to track the total number of CCR-T messages saved in the HDD.

• cc-msg-ccrt-hdd

show active-charging service all

The following field has been added to the output of this show command to indicate whether or not the corresponding credit-control group has been configured to write the failed CCR-Ts in HDD.

• HDD

show active-charging credit-control statistics

The following fields have been added to the output of this show command to display the number of records written to HDD per credit-control group.

• HDD Stats
  • CCR-T

show cdr statistics

The following fields have been added to the output of this show command.

• Diameter-hdd-module Record Specific Statistics
  • Diameter-hdd-module files rotated
  • Diameter-hdd-module files rotated due to volume limit
  • Diameter-hdd-module files rotated due to time limit
  • Diameter-hdd-module files rotated due to tariff-time
  • Diameter-hdd-module files rotated due to records limit
  • Diameter-hdd-module file rotation failures
  • Diameter-hdd-module files deleted
  • Diameter-hdd-module records deleted
  • Diameter-hdd-module records received
  • Current open Diameter-hdd-module files
  • Time of last Diameter-hdd-module file deletion
show diameter-hdd-module file-space-usage

The following fields have been added to the output of this show command.

- CDRMOD Instance Id
- Diameter-hdd-module File Storage LIMIT
- Diameter-hdd-module File Storage USAGE
- Percentage of Diameter-hdd-module file store usage

show diameter-hdd-module statistics

The following fields have been added to the output of this show command.

- Diameter-hdd-Module file Statistics:
  - CDRMOD Instance Id
  - Diameter-hdd-module files rotated
  - Diameter-hdd-module files rotated due to volume limit
  - Diameter-hdd-module files rotated due to time limit
  - Diameter-hdd-module files rotated due to tariff-time
  - Diameter-hdd-module files rotated due to records limit
  - Diameter-hdd-module file rotation failures
  - Diameter-hdd-module files deleted
  - Diameter-hdd-module records deleted
  - Diameter-hdd-module records received
  - Current open Diameter-hdd-module files
  - Time of last Diameter-hdd-module file deletion

- Diameter-hdd-module PUSH Statistics:
  - Successful File Transfers
  - Failed File Transfers
  - Num of times PUSH initiated
  - Num of times PUSH Failed
  - Num of times PUSH cancelled due to HD failure
  - Num of periodic PUSH
  - Num of manual PUSH
  - Current status of PUSH
  - Last completed PUSH time

Release Change Reference, StarOS Release 19
Securing Integrity of SDCs on Rf Interface

CSCut44560 - SDC integrity check on Rf - Checksum Algorithm

**Applicable Products:** P-GW

**Feature Changes**

P-GW generates the charging data and creates a new ACR with individual Service Data Containers (SDCs) based on Rating Groups, and then sends the ACR message directly to Charging Collection Function (CCF). When an intermediate node is inserted between P-GW and CCF, the node can append more SDCs in the charging record sent by P-GW through the Rf interface.

To protect the integrity of SDCs, P-GW counts the number of SDCs, runs a checksum algorithm against the bytes within the SDCs, and then adds a new Diameter AVP "SDC-Integrity-Grouping" with these two values in the ACR message. This new grouped AVP is optional and defined in "aaa-custom4" dictionary only. This vendor-specific AVP can be enabled only when the peer supports the vendor id. This feature helps CCF to distinguish the SDCs included by the intermediate node.
This feature is customer-specific. For more information, contact your Cisco Account representative.

This feature can be enabled by configuring the `diameter accounting sdc-integrity` CLI command in the AAA Server Group Configuration mode. When this command is configured, P-GW computes 1 byte XOR checksum for Service-Data-Container AVP present in ACR messages and includes it in the SDC-Integrity-Grouping AVP.

For this feature to work, the CLI control must be enabled and "aaa-custom4" dictionary containing the grouped AVP should be used and associated with the appropriate AAA group.

**Customer Impact:** When this feature is enabled, there might be minimal performance impact on P-GW specifically on AAA Manager tasks due to checksum calculation.

### Command Changes

**diameter accounting sdc-integrity**

A new keyword `sdc-integrity` is added to the `diameter accounting` CLI command to enable the SDC Integrity feature.

```plaintext
configure context context_name
    aaa group group_name
        [no ] diameter accounting sdc-integrity
end
```

**Notes:**

- When enabled, SDC-Integrity-Grouping AVP is included in the ACR message. This AVP contains the number of SDCs included by P-GW and the checksum as calculated by the previously defined algorithm. The checksum calculation is done only if the AVP is included. By default, this feature is disabled i.e. the grouped AVP is not included in the ACR message even if present in the dictionary. The CLI command will have no effect if the dictionary does not contain the SDC-Integrity-Grouping AVP.

### Performance Indicator Changes

**show aaa group name default**

The following field has been added to the output of this show command to indicate the current configuration state of the feature.

- SDC-Integrity

### S-GW Failure Reporting to PCRF

CSCut82014 - AN_GW_FAILED Reporting to PCRF

**Applicable Products:** P-GW

**Related CDETS ID =** CSCut97242
Feature Changes

The current implementation of P-GW is not compliant with 3GPP defined behavior during S-GW Restoration. P-GW does not indicate the S-GW failure to PCRF and for any PCRF initiated messages while the S-GW restoration is pending, P-GW returns a transient error code "5012 - Unable to Comply with 3GPP".

P-GW rejects the Gx procedures (rule installation, modification) when initiated by PCRF without receiving a S-GW failure notification. This results in unnecessary signaling of Gx messages. To avoid this scenario, the implementation is modified to align with the 3GPP defined behavior. This feature provides support for new AN_GW_FAILED cause code on Gx interface and also a message rejection to the PCRF due to S-GW failure. This feature also provides support for a new Experimental-Result-Code "DIAMETER_AN_GW_FAILED (4143) and notification of the S-GW Restoration for subscriber sessions, which were previously notification to PCRF as AN_GW_FAILED due to S-GW failure. The ability to inform the failure of S-GW is negotiated with PCRF via the Supported-Features AVP sent in CCR-I request.

P-GW is configured to support S-GW Restoration feature. P-GW sends S-GW Restoration feature in Supported-Features AVP through the CCR-I message during session creation. If P-GW receives S-GW Restoration feature in Supported-Features AVP in CCA-I message, then P-GW enables S-GW Restoration feature.

If P-GW and PCRF support S-GW Restoration feature, then the P-GW accepts CCA and RAR during S-GW restoration. Only Rule removal or RAR with session release cause is processed. Any rule with install or modify procedure is dropped. P-GW triggers CCR-U with PCC rule failure report and AN_GW_STATUS AVP to inform PCRF that S-GW is down. After receiving the SGW_Restoration indication, PCRF does not initiate any rule install or modification towards the P-GW. The P-GW informs the PCRF when the S-GW has recovered using the Event-Trigger AVP set to AN_GW_CHANGE and including the AN-GW-Address AVP related to the restored or new S-GW. If S-GW restoration is reported to PCRF, then the P-GW sends CCR-U with AN_GW_CHANGE trigger.

The AN_GW_CHANGE event is sent only for dpca-custom8 dictionary irrespective of whether or not the event trigger is installed by PCRF. For all other dictionaries, the event trigger must be explicitly installed to receive this event.

If S-GW Restoration feature is not negotiated, then P-GW falls back to the old behavior as follows:

- Drops all internal updates towards PCRF
- Rejects CCA and RAR during S-GW Restoration
- Does not include AN_GW_STATUS as AN_GW_FAILED (0) AVP in CCR-U
- Sends an RAA command with the Experimental-Result-Code set to UNABLE_TO_COMPLY (5012) upon receiving RAR command

After configuring the S-GW Restoration feature on Gx interface, the failure is sent to PCRF with Rule-Failure-Code as AN_GW_FAILED in both failure and restoration scenarios.

Previous Behavior: All messages from PCRF were discarded during S-GW Restoration mode.

New Behavior: If rule removal requests are received during S-GW Restoration, it is processed only when the S-GW becomes active.
Command Changes

diameter encode-supported-features

A new keyword **sgw-restoration** is added to this CLI command to enable sending the S-GW Restoration feature in the Supported-Features AVP.

```configure
context context_name
  ims-auth-service imsa-service-name
    policy control
      diameter encode-supported-features sgw-restoration
      { default | no } diameter encode-supported-features
    end
end
```

Notes:
- **sgw-restoration**: This keyword enables configuration of S-GW Restoration feature.

Performance Indicator Changes

IMSA Schema

The following new bulk statistic variables are added to the IMSA schema in support of this feature.

- dpca-msg-sgw-restore-rar-accepted-rule-rem
- dpca-msg-sgw-restore-rar-accepted-sess-rel
- dpca-msg-sgw-restore-raa-sent
- dpca-msg-sgw-restore-ccr-update-sent
- dpca-msg-sgw-restore-ccau-dropped
- dpca-msg-sgw-restore-ccau-accepted-rule-rem
- dpca-msg-sgw-restore-ccau-accepted-sess-rel

show active-charging session full all

The following field has been added to the output of this show command to indicate if the rule removal processing is enabled.

- Rule Removal buffered

show ims-authorization policy-control statistics

The following fields have been added to the output of this show command.

- RAR Accepted
  - Rule Removals
• Session Release
  • CCA-U Dropped
  • CCA-U Accepted
    • Rule Removals
    • Session Release
  • SGW Restoration Reported
    • RAA Sent
    • CCR-U Sent

**show ims-authorization service name**

The "Supported Features" field in this show command output displays whether or not the SGW Restoration feature is configured as part of the Supported-Features.

**show ims-authorization sessions full all**

The "Negotiated Supported Features" field in this show command output displays whether or not the SGW Restoration feature is configured as part of the Supported-Features.

**Time Zone Information in RAA**

CSCut90968 - Message storm prevention caused by DST and Time Zone Information in RAA

**Applicable Products:** P-GW

**Feature Changes**

When MS-Time-Zone event has been enabled through PCRF and when the time zone change occurs, the event trigger UE_TIME_ZONE_CHANGE (25) is generated and CCR-U is sent. During Day Light Savings Time (DST) change, it was identified that the Gx traffic increases significantly in a short period of time and this can overload the PCRF. To avoid this scenario, the event trigger should be disabled. As per the current implementation if the event trigger is disabled, the customer will not able to receive the current UE Time Zone information. To continue receiving this information, the current implementation is modified so that the last known or currently available time zone information is always sent in the RAA messages for dpca-custom8 dictionary even if the UE_TIME_ZONE_CHANGE (25) trigger is disabled.

**Previous Behavior:** Earlier, the 3GPP-Time-Zone AVP was not included in the RAA message unless the UE_TIME_ZONE_CHANGE (25) trigger was enabled.

**New Behavior:** The encoding of 3GPP-MS-TimeZone AVP in RAA message is automatically enabled when dpca-custom8 dictionary is configured under Policy Control configuration mode. That is, the 3GPP-MS-TimeZone AVP is included in all the RAA messages irrespective of whether or not the UE_TIME_ZONE_CHANGE(25) trigger is enabled for P-GW calls.

**Customer Impact:** This behavioral change is applicable only to dpca-custom8 dictionary.
ADC Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from ADC in StarOS 19 software releases.

- ADC Enhancements for 19.2, page 55

ADC Enhancements for 19.2

This section identifies all of the ADC enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the ADC Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

SNI Detection Support

CSCu71291 - Develop rule matching capability for ssl sni feature

Related IDs: CSCu67445, CSCu71216, CSCu71264, CSCu71316, CSCu37026, CSCu64469, CSCu65109, CSCu76197, CSCu88857

Applicable Products: GGSN, IPSG, PDSN, P-GW

Feature Changes

Server Name Indication (SNI) is an extension of the Transport Layer Security (TLS) protocol that allows multiple secure (HTTPS) websites (or any other service over TLS) to be served from the same IP address without requiring all those sites to use the same certificate. SNI provides a mechanism for the client to tell the server which hostname it is trying to connect to.
ADC detects encrypted traffic using the SNI field (signatures) of TLS/SSL (Secure Sockets Layer) traffic. These signatures are added along with other detection mechanisms and delivered as a plugin. If there are new SNI fields either in the already detected applications or new applications, then these new fields are added to the plugin and a new version of the plugin is released. This results in frequent releases of plugin versions causing delay in upgrading the new plugin in the network and leading to revenue leak to the operator. Due to increased number of applications moving towards TLS/SSL, an option is provided to configure the SNI in ruledef and classify traffic based on the configured SNI with this release.

The SNI Detection feature requires a valid Application Detection and Control license. Contact your Cisco account representative for more information.

**Important**

**Previous Behavior:** There was no provision to configure a custom defined protocol (CDP) in previous releases. Only protocols as part of the ADC plugin were populated as part of bulk statistics in P2P schema.

**New Behavior:** An option to configure the SNI and the corresponding custom defined protocol (CDP) name in a ruledef is added. CDP names defined in TLS ruledef will be populated as part of the P2P schema.

### Command Changes

**tls**

The new `tls` CLI command is added in the ACS Ruledef Configuration mode to configure TLS/SSL Server Name Indication (SNI) and the corresponding custom defined protocol (CDP).

```
configure active-charging service service_name
   ruledef ruledef_name
       [ no ] tls { set-app-proto cdp_name_string | sni operator server_name_string }
end
```

**Notes:**

- **set-app-proto cdp_name_string**: Specifies the name of the custom defined protocol for TLS/SSL flows matching the ruledef.

  `cdp_name_string` must be an alphanumeric string of 1 through 19 characters.

- **sni operator server_name_string**: Specifies the TLS/SSL Server Name Indication (SNI) field value in the SSL Client Hello packet.

  **operator**: Specifies how to match and must be one of the following:

  - `!=`: Does not equal
    
    The `!=` operator in the TLS SNI rule results in non-optimized rule.
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

  `server_name_string`: Specifies the server name and must be an alphanumeric string of 1 through 127 characters.
The following commands must be configured for SNI rules to work:

- Enable SSL protocol in the Active Charging Service configuration:
  ```
  [local]P2P_SSL(config-acs)# p2p-detection protocol ssl
  ```
  If the `p2p-detection protocol all` CLI command is enabled in the Active Charging Service configuration, then the `ssl` keyword need not be enabled again as it will be already enabled with the `all` keyword.

  The `ssl` protocol is available only in Plugin releases 1.142.526 and later.

- Enable P2P in the ACS Rulebase configuration:
  ```
  [local]P2P_SSL(config-rule-base)# p2p dynamic-flow-detection
  ```

- The action priority for SNI ruledef must be configured in the rulebase similar to other ruledefs.

### clear active-charging analyzer statistics name

In this release, `cdp` is a new keyword added to this command to clear statistics for CDP flows.

```
clear active-charging analyzer statistics name cdp [ application app_name | instance instance_number ] [ | { grep grep_options | more } ]
```

### show active-charging analyzer statistics name

In this release, `cdp` is a new keyword added to this command to display analyzer statistics for flows matching the SNI ruledefs.

```show active-charging analyzer statistics name cdp [ application app_name | instance instance_number | summary | verbose | wide ] [ | { grep grep_options | more } ]
```

Notes:

- `application app_name`: The CDP name specified in the TLS rules.
- `instance instance_number`: Displays Session Manager information for specific instance.
- `summary`: Summary of SNI application statistics.
- `verbose`: Displays detailed statistics configured in a service.
- `wide`: Displays all available CDP statistics in a single wide line.

### show active-charging flows

In this release, `cdp` is a new keyword added to this command to display flow-level statistics for flows matching the SNI ruledefs.

```show active-charging flows type cdp [ application app_name | instance instance_number | summary | verbose | wide ] [ | { grep grep_options | more } ]
```
Performance Indicator Changes

P2P Schema
In support of the SNI detection feature, the "p2p-protocol" bulk statistic variable in the P2P schema will display the application protocol configured in the "set app-proto" string of TLS ruledef.

show active-charging analyzer statistics name cdp
The following new fields are added to the output of this new command:

- CDP Summary:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts

show active-charging flows type cdp
The following new fields are added to the output of this new command:

- Session ID
- Flow-ID
- Application Protocol
- Transport Protocol
- Tethered Flow
- Bytes-Up
- Bytes-Down
- Pkts-Up
- Pkts-Down

show active-charging ruledef name
In support of the SNI detection feature, this command displays the fields for TLS/SSL SNI and CDP as configured in the TLS ruledef.

SNI Rule Variable Support in EDR

CSCu10146 - Server Name Indication (SNI) name field support EDR for SSL flows

Applicable Products: GGSN, IPSG, PDSN, P-GW
Important

This enhancement is applicable to 19.2.3 and later releases.

Feature Changes

With this enhancement, the Server Name Indication (SNI) rule variable is added as an optional field in EDRs for detection of TLS/SSL flows. The SNI field in the TLS/SSL handshake is used to determine the type of TLS/SSL flow being setup. The `tls sni` keyword is added to the `rule-variable` CLI command in the EDR Format Configuration mode. When this rule variable is configured and a valid SNI name is detected in the flow, the SNI field is populated in the EDR.

**Previous Behavior:** The SNI rule variable was not supported in EDR.

**New Behavior:** A new EDR rule variable "tls sni" is added to configure SNI for TLS/SSL flows.

Command Changes

`rule-variable`

The `tls` keyword is added to this command to configure the SNI rule variable for TLS/SSL flows in EDR.

```plaintext
configure
  active-charging service service_name
  edr-format format_name
  rule-variable tls sni priority priority
  end
```

Notes:

- **tls sni:** Specifies the TLS/SSL SNI field.
- **priority priority:** Specifies the CSV position of the field (protocol rule) in the EDR. `priority` must be an integer from 1 through 65535.

Performance Indicator Changes

`show active-charging edr-format all`

This command will display the new EDR rule variable if configured.

`show configuration`

This command will display the new EDR rule variable if configured.
CHAPTER 3

ECS Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from ECS in StarOS 19 software releases.

- ECS Enhancements for 19.4, page 61
- ECS Enhancements for 19.3, page 62
- ECS Enhancements for 19.2, page 65
- ECS Enhancements for 19.0, page 69

ECS Enhancements for 19.4

This section identifies all of the ECS enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the ECS Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Tethering Database Load on Session Managers

CSCuy82624 - Tethering DBs not loaded when tethering is disabled after reload

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

**Previous Behavior:** If tethering database load was in progress, tethering detection was disabled immediately using the no tethering-database CLI command.
New Behavior: If tethering database load is in progress, the `no tethering-database` CLI command to disable tethering-detection will not be allowed to execute, and needs to rerun after the database load process is completed.

Customer Impact: Delayed disabling of the tethering detection feature is observed.

**UA Database File Entry Limit**

CSCuv73599 - [MARS-DPC2]-Tethering DB's fails to load after boot

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

Previous Behavior: The file entry limit for UA database was 4K bytes.

New Behavior: The new file entry limit is 127 bytes which is equal to the bytes used when UA-based tethering detection is done. The remaining bytes are mostly unused by ECS. The "All" database format check is also made stricter.

Customer Impact: The entries of UA DB file are truncated to fit a maximum of upto 127 characters in each line.

**ECS Enhancements for 19.3**

This section identifies all of the ECS enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *ECS Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

**Activation/Removal of GoR through Charging-Rule-Name AVP**

CSCuw20700 - Support for activation of GoR through Charging-Rule-Name AVP

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

PCRF can activate and remove a PCC rule with group-of-ruledefs (GoR) for a subscriber session over Gx using the Charging-Rule-Install and Charging-Rule-Name AVPs in CCA and RAR messages.

Previous Behavior: ASR5K allowed activation and deactivation of group-of-ruledefs only through the "Charging-Rule-Install" AVP grouped under "Charging-Rule-Install" and "Charging-Rule-Remove" AVPs. The `policy-control charging-rule-base-name active-charging-group-of-ruledefs` configuration is required to interpret the Charging-Rule-Base-Name AVP as group-of-ruledefs.
New Behavior: In this release, group-of-ruledefs can also be activated/removed through Charging-Rule-Name AVP grouped under "Charging-Rule-Install" and "Charging-Rule-Remove" AVPs. PCRF sends group-of-ruledef name through Charging-Rule-Name AVP included in the Charging-Rule-Install grouped AVP similar to predefined rule. On receiving the Charging-Rule-Install AVP, ASR5K searches the group name in the list of configured group-of-ruledefs. If the group name exists, ASR5K activates the group. This behavior is independent of the policy-control charging-rule-base-name active-charging-group-of-ruledefs configuration.

Similar to the activation, PCRF sends group-of-ruledef name in Charging-Rule-Name AVP under Charging-Rule-Remove AVP. ASR5K checks the list of activated group-of-ruledefs, and deactivates the group if a matching group name exists.

ADC Rule Support over Gx for ECS rules

CSCuw21320 - ADC over Gx support for Non P2P Rules

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

In this release, the ADC Rule functionality is extended to support all ECS protocols in addition to existing P2P protocols. This also supports detection of application flows for Group of Ruledefs.

ADC Rules are certain extensions to dynamic and predefined PCC Rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Important

ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

Previous Behavior: In previous releases, the ADC Rule activation over Gx is supported only for ADC based rules as described in Release-11 of 3GPP standard.

New behavior: In this release, the functionality is extended for non-ADC based rules in addition to the following support for both ADC and non-ADC rules:

- ADC rules will support combination of P2P and non-P2P rule lines in the same ruledef.
- Detection of application flows based on group of ruledefs.
- Application START/STOP event reporting at instance level, that is, per flow basis. This was supported per Application ID basis in previous releases.
- Support of dynamic routes to analyzers for installed ADC rules. Dynamic routes will be supported only for the following protocols:
  - HTTP
  - HTTPS
  - FTP
  - RTP
  - RTCP

Release Change Reference, StarOS Release 19
• SIP

• Support multi-line AND logic for rulelines when configuring ADC ruledefs.

• Removal of all PCC rules will result in termination of Application Detection for that application. In previous releases, if more than one PCC rule with same Application ID is installed, then removal of any of the PCC rules will terminate Application Detection for that application.

When a subscriber attaches to the network, PCRF will install ADC rule/Group of Ruledefs towards PCEF to detect Application flow. The Install ADC rules will additionally enable default routes to HTTP, HTTPS, FTP, RTSP, RTCP or SIP analyzer based on the rule-definition. The default routes use the standard ports associated with the respective protocol. When a new flow comes, the route matching happens for dynamic routes first, then static routes and finally default routes. When a flow matches that ADC rule, an APP-START notification is sent to PCRF with Application ID, Instance ID and flow information. Instance ID is a unique identifier for a particular ADC flow. PCRF then takes necessary action for the detected application. When ADC flow terminates, an APP-STOP notification is sent to PCRF with Application ID and Instance ID.

ADC Rule Support based on TOS/DSCP Bearer Mapping

CSCux24001 - DSCP based ADC Rule support

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

With this release, the ADC functionality is extended to identify applications and distinguish bearer traffic based on TOS/DSCP. DSCP/TOS based ADC dynamic rules over Gx will be supported for default and dedicated bearers. Bearer mapping and rule matching will be done based on DSCP/TOS value.

When a subscriber attaches to the network, PCRF will install PCC rule with TOS/DSCP filter towards PCEF. PCEF will create a dedicated bearer and send the packet filters to UE as well. When a new flow comes with first packet as Uplink, UE does bearer matching based on the TOS/DSCP value, and sends flow on the correct dedicated bearer. For downlink packet, ECS does bearer lookup and assigns correct bearer to the flow based on the TOS/DSCP value.

ADC Event reporting will contain flow template with outer IP 3 tuples (Source IP, Destination IP, Port). L4-L7 rule match will now work for PIMP service.

The TOS based PCC rules that were earlier supported are qualified in this release for LTE/eHRPD/PMIP services primarily for MAG-LMA based PMIP service.

Previous Behavior: Filters were not created for PCC rules based on TOS Traffic Class AVP.

New Behavior: In this release, filters can be created for PCC rules based on TOS Traffic Class AVP under flow information.

Rule match for Dynamic ADC Rules

CSCux20387 - Issues with dynamic rule match logic with filters and ADC

Applicable Products: GGSN, PDSN, P-GW
Feature Changes

**Previous Behavior:** If ADC dynamic rule is installed with filters, the rule matching logic does not consider the associated filters and skips these filters. Only the associated Application ID rule lines are considered for rule match in this case.

**New Behavior:** If ADC dynamic rule is installed with filters, the rule match logic will consider both the associated filters and related Application ID rule lines for rule matching.

**Customer Impact:** Change in the rule match logic will result in new dynamic rule match or no rule match if ADC dynamic rules are installed with filters.

ECS Enhancements for 19.2

This section identifies all of the ECS enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *ECS Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

HTTP URL Percent Encoding

CSCuv43653 - percent encode compliance of all reserved characters as per RFC 3986

**Related CDETS ID:** CSCuw10676, CSCuw10681

**Applicable Products:** GGSN, P-GW

Feature Changes

Percent-encoding functionality is used whenever URL redirection happens for an HTTP Request packet and the requested URL (original URL) is embedded in redirected response. The reserved characters present in the requested URL are replaced by % followed by ASCII hexadecimal value. As defined in RFC 3986, a capability is added in the ECS to percent-encode reserved characters when modifying HTTP URLs. As the percent (%) character serves as the indicator for percent-encoded octets, it must be percent-encoded as "%25" for that octet to be used as data within a URL.

HTTP URL redirection can happen via Charging Action or DCCA. For redirection via DCCA, percent encoding is needed only when original URL is appended. URL append is supported only for dcca-custom1 and dcca-custom24 dictionaries.

**Previous Behavior:** In case of HTTP URL redirection, when original URL is embedded in the redirected URL string:

1. All reserved characters in the original URL (per RFC 3986) were not percent-encoded in case redirection was triggered via charging-action.
2 All reserved characters in the original URL (per RFC 3986) were not percent-encoded in case redirection was triggered via DCCA.

3 The % character, if present in the original URL was not percent-encoded.

4 In case the original URL was concatenated with other information, then no reserved character was percent-encoded if redirection was triggered via charging-action.

**New Behavior:** In case of HTTP URL redirection, when original URL is embedded in the redirected URL string:

1 All reserved characters in the original URL (per RFC 3986) are percent-encoded in case redirection is triggered via charging-action.

2 All reserved characters in the original URL (per RFC 3986) are percent-encoded in case redirection is triggered via DCCA.

3 The % character, if present in the original URL is percent-encoded to %25.

4 In case the original URL was concatenated with other information, then all reserved characters and % character are percent-encoded if redirection is triggered via charging-action.

**Customer Impact:** When original URL is embedded in the redirected URL string for HTTP URL redirection, all reserved characters in the original URL are now percent-encoded when redirection is triggered via charging action or DCCA.

For detailed information on this feature, refer to the *HTTP URL Percent Encoding* chapter of the *ECS Administration Guide*.

---

### Support for Splash Pages

CSCuv54231 - splash page for MFL:3615

**Applicable Products:** GGSN, P-GW, S-GW

---

### Feature Changes

The Splash Page support feature helps to distinguish HTTP traffic coming from mobile browsers and redirect the very first flow to a splash page whenever a subscriber attaches to the network. Splash page is the page of a website that the user sees first before being given the option to continue to the main content of the site.

When a subscriber attaches to the network, PCRF installs predefined rule/group of ruledefs towards PCEF to match mobile browser specific flows. On the first match of this rule/group of ruledef, redirect packet containing information of the welcome page where the flow needs to be redirected, is sent to UE and the first request gets terminated. Subsequently the predefined rule/group of ruledef from the list is removed and sends CCR-U with Charging Rule Report (CRR) AVP to PCRF for rule status. The existing `deactivate-predefined-rule` CLI command in the ACS Charging Action configuration mode is used to remove the matched predefined rule/group of ruledef.

In 17.2 and later releases, the redirection functionality was supported in the case when 80% threshold usage is reached for the subscriber and the same rule gets deactivated to ensure one time redirection for the subscriber. In this release, the functionality is extended to redirect the first mobile browser flow to the splash page whenever subscriber attaches to the network. This feature now supports predefined group of ruledefs in addition to previously supported predefined rules. CLI and Statistics are enhanced to support HTTP-based rule matching in HTTP header.
Command Changes

http accept

The new `accept` keyword is added to the `http` command to define rule expressions to match content types that are acceptable for the response.

```configure
active-charging service service_name
  ruledef ruledef_name
    [ no ] http accept [ case-sensitive ] operator accept_field
  end
```

Notes:

- `operator`: Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!present`: Not present
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `present`: Present
  - `starts-with`: Starts with

- `accept_field` specifies the ACCEPT field present in the HTTP header to be matched. This must be an alphanumeric string of 1 through 127 characters.

http

New keyword options `!present` and `present` are added to enhance rule matching for flow detection on the basis of absence/presence of ACCEPT, REFERER, X-HEADER, USER_AGENT, COOKIES and VERSION fields in HTTP header request.

```configure
active-charging service service_name
  ruledef ruledef_name
    [ no ] http accept [ case-sensitive ] { !present | present } accept_field
    [ no ] http cookie [ case-sensitive ] { !present | present } cookie_string
    [ no ] http referer [ case-sensitive ] { !present | present } referer_name
    [ no ] http user-agent [ case-sensitive ] { !present | present } user_agent
    [ no ] http version [ case-sensitive ] { !present | present } http_version
    [ no ] http x-header field_name [ case-sensitive ] { !present | present } string
  end
```

Release Change Reference, StarOS Release 19
rule-variable

The new `accept` keyword option is added to the `http` keyword in the event data record for HTTP to match content types that are acceptable for the response.

```
configure
  active-charging service service_name
  edr-format format_name
  rule-variable http accept priority priority
  no rule-variable http accept [ priority priority ]
end
```

deactivate-predefined-rule

This command is enhanced to support predefined group of ruledefs in this release. This command allows to remove or deactivate the matched predefined rule/Group of ruledefs that selected this action to ensure one time redirection for the subscriber. Static rules are not deactivated by this command.

```
configure
  active-charging service service_name
  charging-action charging_action_name
  [ default | no ] deactivate-predefined-rule
end
```

Performance Indicator Changes

ECS Schema

The following new bulk statistic is added to provide the total number of matches for one time hit PCC rules.

- `total-one-time-hit-pcc-rule-matched`

show active-charging charging-action all

The existing field in the output of this command is enhanced to check the status of Predefined rule/Group of ruledefs.

- Predefined Rule Deactivation

show active-charging charging-action statistics name

The following field in the output of this command is enhanced to check the number of times Predefined rule/Group of ruledefs is deactivated through charging action.

- Predef-Rules Deactivated

show active-charging flows full all

The following field is displayed in the output of this command only when the HTTP transaction contains the Accept header field.
show active-charging rulebase statistics name

The following field in the output of this command displays the number of matches for one time hit PCC rules.

- One Time Hit PCC Rule Matched

ECS Enhancements for 19.0

This section identifies all of the ECS enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *ECS Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

Bulk Statistics for Rule Installation Failures

CSCuc60371 - Enhancements to IMSA stats to include rule-install failures

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

Whenever ECS receives a request for dynamic rule installation, modification or removal from PCRF over Gx interface, it performs a set of validations on received requests for correctness. If these validations fail, the gateway rejects the rule or generates "Charging-Rule-Report" with a "Rule-Failure-Code". In most of the cases, the "Rule-Failure-Code" is very generic and difficult to identify the actual failure reason. Some failure statistics are maintained but available until the call is active.

Detailed statistics about successful installations/modifications/removals and for the failures are required for debugging purpose. Granular statistics and bulk statistics variables are now maintained at rulebase level to track the number of successful installation, modification and deletion of dynamic rules.

**Limitations:**

The statistics support is not available at ECS for the following conditions:

- Rating Group = 0
- QCI value missing
- QCI value = 0
- Priority Level (PL) in ARP
- Protocol in Flow Information
• Blank Charging Rule Name or missing Charging Rule Name

Note that the statistics for these failure conditions are supported through the show ims-authorization policy-control statistics CLI output.

Performance Indicator Changes

ECS Schema

The following new bulk statistics variables are added to this schema to track the reasons for rule installation failure at instance level.

• dyn_rule_install_received
• dyn_rule_install_succeeded
• dyn_rule_install_failed
• dyn_rule_install_fail_unknown_rule_name
• dyn_rule_install_fail_rating_group_error
• dyn_rule_install_fail_service_id_error
• dyn_rule_install_fail_trigger_policy_failure
• dyn_rule_install_fail_resources_limitation
• dyn_rule_install_fail_max_no_of_bearer_reached
• dyn_rule_install_fail_missing_flow_info
• dyn_rule_install_fail_resource_allocation_failure
• dyn_rule_install_fail_unsuccessful_qos_validation
• dyn_rule_install_fail_incorrect_flow_info
• dyn_rule_install_fail_redirect_server_add_missing
• dyn_rule_install_fail_tdf_app_id_error
• dyn_rule_modify_received
• dyn_rule_modify_succeeded
• dyn_rule_modify_failed
• dyn_rule_modify_fail_rating_group_error
• dyn_rule_modify_fail_service_id_error
• dyn_rule_modify_fail_trigger_policy_failure
• dyn_rule_modify_fail_resources_limitation
• dyn_rule_modify_fail_max_no_of_bearer_reached
• dyn_rule_modify_fail_resource_allocation_failure
• dyn_rule_modify_fail_unsuccessful_qos_validation
• dyn_rule_modify_fail_incorrect_flow_info
• dyn_rule_modify_fail_redirect_server_add_missing
• dyn_rule_modify_fail_tdf_app_id_error
• dyn_rule_common_rule_received
• dyn_rule_common_fail
• dyn_rule_common_fail_unknown_bearer_id
• dyn_rule_common_fail_resource_allocation_fail
• dyn_rule_intended_fail
• dyn_rule_intended_fail_ps_to_cs_handover
• dyn_rule_intended_fail_resource_allocation_failure
• dyn_rule_remove_received
• dyn_rule_remove_succeeded
• dyn_rule_remove_failed
• dyn_rule_remove_fail_unknown_rule_name
• dyn_rule_remove_fail_bcm_mode_mismatch

**show active-charging rulebase statistics name**

The following fields are added to the output of this show command to track the number of successful installation, modification and deletion of dynamic rules.

• Dynamic Rule Statistics:
  • Rule Installation Statistics:
    • Total number of Installation Received
    • Total number of Installation Succeeded
    • Total number of Installation Failed
  • Rule Installation Failure Statistics:
    • Unknown Rule Name Error
    • Rating Group Error
    • Service ID Error
    • Trigger Policy Failure
    • Resources Limitation
    • Maximum Number Of Bearer Reached
    • Flow Information Missing
    • Resource Allocation Failure
- QOS Validation Error
- Incorrect Flow Information
- Adc Rule - Redirect Server Address Missing
- Adc Rule - TDF App ID Error

* Rule Modification Statistics:
  - Total number of Modification Received
  - Total number of Modification Succeeded
  - Total number of Modification Failed

* Rule Modification Failure Statistics:
  - Rating Group Error
  - Service ID Error
  - Trigger Policy Failure
  - Resources Limitation
  - Maximum Number Of Bearer Reached
  - Resource Allocation Failure
  - QOS Validation Error
  - Incorrect Flow Information
  - Adc Rule - Redirect Server Address Missing
  - Adc Rule - TDF App ID Error

* Common Rule Statistics:
  - Total Number Of Common Rules Received
  - Total Number Of Common Failures
  - Unknown Bearer ID Error
  - Resource Allocation Failure

* Already Installed Rule removal:
  - Total Number Of Intended Removals
  - PS to CS Handover
  - Resource Allocation Failure

* Rule Removal Statistics:
  - Total Number Of Removal Received
Call Drop due to Checkpoint Mismatch

CSCuv02285 - Call should be dropped if OC chkpt not received during internal audit

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

During internal audit of ICSR recovery, if sub map node checkpoints are received and Override Control (OC) checkpoint fails, call will be dropped.

**Previous Behavior:** If OC checkpoint corresponding to a sub map checkpoint entry is lost, the entry is deleted during internal audit. As a result, Override Control was not applied for this entry after recovery.

**New Behavior:** If OC corresponding to a sub map checkpoint is not found in internal audit, the call is dropped.

Change in Display Output for sn-volume-dropped-amt Attribute

CSCus98119 - direction not being displayed for attribute sn-volume-dropped-amt

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

The "sn-volume-dropped-amt" attribute in the EDR Format configuration reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets dropped by Stateful Firewall during a flow. However, the uplink and downlink direction are not reported through the `show active-charging edr-format all` CLI output.

**Previous Behavior:** The `show active-charging edr-format all` CLI output does not display the direction for "sn-volume-dropped-amt" attribute.

**New Behavior:** Both uplink and downlink direction are indicated for the "sn-volume-dropped-amt" attribute through the show CLI output.

Group-of-Ruledefs Support for Override Control

CSCus07043 - Need to support group-of-ruledef for inheritance and override control

**Applicable Products:** GGSN, PDSN, P-GW
**Feature Changes**

The Override Control in Release 17 provided the functionality to override pre-configured rules but there was no support to override Group-Of-Ruledefs. Individual ruledefs inside group-of-ruledef had to be overridden separately. With this enhancement, override sent for a group-of-ruledefs will apply to all the ruledefs defined in a group. The same **Override-Rule-Name** AVP is used to send Ruledef or Group-of-Ruledef interchangeably.

This feature supports two AVPs — **Override-Rule-Name** and **Override-Charging-Action-Exclude-Rule**. These AVPs support either a Ruledef name or a Group-of-Ruledefs name.

**Handling of Predefined Rules in Pending List**

CSCuv39288 - Incorrect Rule failure CCR-U after LTE to GnGp HO

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

**Previous Behavior:** If a predefined rule is in the Create Bearer Response or Update Bearer Response pending list and a new CCA-U/RAR is received with a request for installation of the same rule, the P-GW sends rule installation failure for the latest request in CCR-U to PCRF. On receiving Create Bearer Response/Update Bearer Response, it installs the predefined rule. This causes the P-GW and PCRF to be out of sync.

**New Behavior:** If a predefined rule is in the pending list and a new CCA-U/RAR is received with an installation request for the same rule, the P-GW ignores the latest installation request.

**Handling of Simultaneous Delete Bearer and Create Bearer Requests**

CSCut23703 - Support of Simultaneous Delete Bearer Request and Create Bearer Request

**Applicable Products:** GGSN, PDSN, P-GW

**Feature Changes**

**Previous Behavior:** When Delete Bearer Request (DB-Req) and a Create Bearer Request (CB-Req) are received back-to-back for the same bearer, the CB-Req received before receiving the Delete Bearer Response (DB-Resp) for the DB-Req was rejected resulting in call drop.

**New Behavior:** ECS buffers the Create and Update Bearer Requests for a bearer when response for the DB-Req for the same bearer is pending. ECS processes the buffered Create and Update Bearer Requests only after bearer-release indication is received for the bearer-deletion request.

**Customer Impact:** This change in the rule buffering logic leads to a better user experience.

**New TRM Statistic Support**

CSCuu25969 - PGWCDR: flow should be moved out of A-ECS after service idleout expiry

**Applicable Products:** GGN, PDSN, P-GW
Feature Changes

**Previous Behavior:** In previous releases, the G-CDR bucket was not inserted for next idle timeout until flow comes out of A-ECS.

**New Behavior:** In this release, all the flows related to eG-CDR bucket are moved out of A-ECS after service idle timeout expiry so that the bucket can be inserted again for next service idle timeout expiry. Hence, TRM is disengaged in this scenario and a new TRM statistic is added to the output of the show active-charging rulebase statistics CLI command to display the total number of times TRM was cleared from a flow or transaction due to service idle timeout expiry of eG-CDR bucket.

Performance Indicator Changes

show active-charging rulebase statistics

The following field is added to the output of this command in this release.

- Cleared, egcdr bucket idle time out

Reporting of Usage Data During APN-AMBR Change

CSCuq30554 - SDC not sent in interim RF record after APN-AMBR change for Only SDF

**Applicable Products:** GGSN, P-GW

Feature Changes

Interim Rf record is generated without including Service-Data-Container (SDC) for data on default bearer when SDF is configured in Policy Accounting and APN-AMBR of the attached session is changed.

**Previous Behavior:** When the APN-AMBR is changed, buckets associated with only dynamic and predefined rules were reported if rules corresponding to trigger QCI ARP matched the charging action/bucket.

**New Behavior:** For a change in the APN-AMBR, all buckets associated with dynamic, predefined and static rules are released irrespective of the bearers they belong to.

**Customer Impact:** More number of buckets can be seen in the Rf record for APN-AMBR change event in SDF accounting.
 CHAPTER 4

ePDG Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from ePDG in StarOS 19 software releases.

• ePDG Enhancements for 19.4, page 77
• ePDG Enhancements for 19.2, page 78
• ePDG Enhancements for 19.0, page 80

ePDG Enhancements for 19.4

This section identifies all of the ePDG enhancements included in this release:

 Feature Changes - new or modified features or behavior changes. For details, refer to the ePDG Administration Guide for this release.

 Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

 Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.

 Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your ePDG.

• AAA Enhancements
• CF Enhancements
• ECS Enhancements
• Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
Send DSReq if new PGW is Selected during Re-attach

CSCuy28077 - ePDG not sending DSReq during re-attach if new PGW is selected.

Feature Changes

With this release ePDG will send the delete session request during reattach if another PGW is selected for current session. If the same PGW is selected for current session during reattach, ePDG will not send the delete session request to PGW and will do local purge.

In case of session creation failure during reattach, ePDG will always trigger delete session request to PGW.

This feature can be enabled by configuring "newcall duplicate-session notify-delete" in ePDG Configuration Mode.

Command Changes

newcall

With this release a new command [ no | default ] newcall duplicate-session notify-delete is introduced in ePDG Service configuration mode.

configure
context var_name
epdg service service_name
[ no | default ] newcall duplicate-session notify-delete
end

ePDG Enhancements for 19.2

This section identifies all of the ePDG enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the ePDG Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your ePDG.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

**SCTP support for SWM interface**

CSCuv52506 SCTP support for SWM interface

**ePDG Service Level Threshold Parameters Monitoring Support**

CSCuv41418 - ePDG service level threshold parameters monitoring support.

**Command Changes**

`threshold`

Below command `threshold` is added as part of this release:

```
configure
context context_name
no threshold { epdg-ikev2-authentication-failures | epdg-ikev2-setup-attempts | epdg-ikev2-setup-failure | epdg-ikev2-setup-failure-rate | epdg-ikev2-setup-success }
end
```
epdg-ikev2-authentication-failures

New command `epdg-ikev2-authentication-failures` is introduced in this release:

```
configure
  [ default ] threshold poll epdg-ikev2-authentication-failures interval interval
end
```

epdg-ikev2-setup-attempts

New command `epdg-ikev2-setup-attempts` is introduced in this release:

```
configure
  [ default ] threshold poll epdg-ikev2-setup-attempts interval interval
end
```

epdg-ikev2-setup-failure

New command `epdg-ikev2-setup-failure` is introduced in this release:

```
configure
  [ default ] threshold poll epdg-ikev2-setup-failure interval interval
end
```

epdg-ikev2-setup-failure-rate

New command `epdg-ikev2-setup-failure-rate` is introduced in this release:

```
configure
  [ default ] threshold poll epdg-ikev2-setup-failure-rate interval interval
end
```

epdg-ikev2-setup-success

New command `epdg-ikev2-setup-success` is introduced in this release:

```
configure
  [ default ] threshold poll epdg-ikev2-setup-success interval interval
end
```

ePDG Enhancements for 19.0

This section identifies all of the ePDG enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the ePDG Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your ePDG.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

### Multiple AAA-Groups Support

CSCus54922 [ePDG] support multiple aaa-groups in diff contexts for SWm interface

#### Feature Changes

With this feature, ePDG has the ability to support call-control-profile for AAA context/group selection.

- This is useful for context separation (SWm, SWu and S2b interface configuration can be configured with different contexts)
- UICC, Non-UICC users can goto different AAA groups if required (based on AAA capabilities)

### PGW FQDN Per APN Configuration Support

CSCus66047 - Configurable PGW FQDN support per APN

#### Feature Changes

Flexibility added to configure Primary/Secondary PGW IP/FQDN under apn-profile.

**Previous Behavior:** Weight based selection supporting.

**New Behavior:** Flexibility to configure primary/secondary PGW IP/FQDN under apn-profile or weight based selection support.

**Customer Impact:** Yes
Command Changes

pgw-address

Below key words are added to `pgw-address` command as part of this release:

```
configure
context context_name
pgw-address { IP-ADDRESS ip_address { primary | secondary | [fqdn fqdn_var primary | secondary ] } }
end
```

GTP-C Load and Overload Control on ePDG

CSCus68120 - 3GPP based GTP-C Load and Overload Control on ePDG

Feature Changes

Load/Overload control

**Previous Behavior:** Load/overload support for ePDG was not available.

**New Behavior:** Load/overload support for ePDG provided, It will throttle various messages depending on the load/overload on peer nodes.

**Customer Impact:** Provides customer an option to load balance the different nodes by enabling the CLI.

Command Changes

message-prioritization

New command `message-prioritization` is introduced in this release:

```
configure
context context_name
| no | message-prioritization group1 percentage group2 percentage
| default | message-prioritization
end
```

Maintain Session Uniqueness and Avoid Stale Session Processing

CSCus87417 - PGW: Maintain Session Uniqueness

Feature Changes

Added a mechanism for the sender/message originator to add a time stamp of when the message is originated and the maximum time that the originator is going to wait before giving up on the message response and the procedure. The receiving node should utilize the same time stamp and maximum wait time to identify if it is
still a valid message and if it should process it. If the message is processed, the intermediate nodes should replicate the time stamp and maximum wait time in messages generated by the node towards other peers. Each network element should compare the Time Stamp and its own synced (NTP) time to ensure stale messages are not processed.

If any session related information is created and before the network element responds, the maximum wait time has passed, the network element should ensure any stale session information is cleared and released.

**AVP Support on SWm Interface**

CSCut05734 - [ePDG] Terminal Information AVP support on SWm interface

**Feature Changes**

New AVP in DER message for SWm interface

**Previous Behavior:** Terminal-Information does not have IMEI and Software-Version AVP encoded in DER message.

**New Behavior:** IMEI and Software-Version is encoded under Terminal-Information AVP.

**Customer Impact:** AAA server now supports Terminal-Information.

**IKE SA Establishment Failure Bulkstats Support**

CSCut26317 - [ePDG] IKEv2 bulkstats addition

**Feature Changes**

When IKE SA establishment fails, following counters are incremented. However there is absence of corresponding bulkstats support in the system schema, which is added as part of this change.

- ikev2-auth-invalidnai — send as Idi NAI in IKE_AUTH_REQ
- ikev2-xchg-dropunexppld — scenario notify error payload is received in IKE_SA_INIT message

**Previous Behavior:** Bulkstats supporting IKE SA establishment failure unavailable.

**New Behavior:** New bulkstat variables "ikev2-auth-invalidnai" and "ikev2-xchg-dropunexppld" added as part System Schema.

**New Statistics Introduced to the ePDG Schema**

CSCut26325 - [ePDG] -Per QCI attempts/failure/success stats

**Feature Changes**

Currently ePDG does have the Bulk Statistics for the Active/Setup/Released bearers. From Release 19.0 of VoWIFI, ePDG supports and maintains per QCI Active/Setup/Released. Also **show epdg-service statistics apn-name** which is existing Stat for success is directly mapped.
Previous Behavior: ePDG displayed only Active/Setup/Released Stats Per QCI only.

New Behavior: Now ePDG displays Attempt/Failure Stats Per QCI along with existing stats.

Customer Impact: Better understanding of Quality of Service Attempt/Success/Failure.

Performance Indicator Changes

ePDG Schema

Below stats are introduced as part of this release:

- num-qci1_bearer_attempt
- num-qci1_bearer_failure
- num-qci2_bearer_attempt
- num-qci2_bearer_failure
- num-qci3_bearer_attempt
- num-qci3_bearer_failure
- num-qci4_bearer_attempt
- num-qci4_bearer_failure
- num-qci5_bearer_attempt
- num-qci5_bearer_failure
- num-qci6_bearer_attempt
- num-qci6_bearer_failure
- num-qci7_bearer_attempt
- num-qci7_bearer_failure
- num-qci8_bearer_attempt
- num-qci8_bearer_failure
- num-qci9_bearer_attempt
- num-qci9_bearer_failure

Diameter Interface Overload Control

CSCut42292 - Support for vendor specific cause code to support 3GPP DOCME

Feature Changes

Following is the behavior when the experimental result code is received by ePDG:

For Diameter Initial Requests:
ePDG will reject the procedure towards the Downstream Network Elements and should not retry the secondary Connection.

2. ePDG will reject the UE messages with IKE Error Code 24 - AUTHENTICATION_FAILED.

For Diameter Update requests:

1. ePDG will reject the procedure towards the Downstream Network Elements and should not retry the secondary Connection.
2. ePDG sends IKE informational Deletemessage to UE for clearing the SA.

For Diameter Termination Requests:

1. If the Request Times out, Client will try the Secondary Server as per existing behavior and clean up the session information if the secondary connection times out as well.

APN Level Statistics for VoWiFi HO

CSCut90771 - [ePDG]-APN level stats for VoWifi HO

Feature Changes

The LTE to WiFi stats are present as "Total Handoff" and WiFi to LTE is present as disconnect stats in epdg-service stats.

Previous Behavior: Session disconnect stats at APN level is not maintained.

New Behavior: Maintaining session disconnect stats at APN level is added.

Customer Impact: Better system operation.

GTP Overload Control Support

CSCut94997 - [ePDG] - GTP overload control support

Feature Changes

Previous Behavior: APNS cannot be identified as emergency APN.

New Behavior: We can identify the apn as emergency apn. via the apn-profile associated for that apn. In the apn-profile configure new apn-type, so that we can identify as APN as emergency APN. So we handle things differently for emergency APN.

The gtpc-overload-profile can be associated to epdg-service. Based on the message prioritization we can throttle the messages on s2b interface if overload info is available.

Customer Impact: Better system operation.
Command Changes

associate

Key word `gtpc-overload-control-profile` is added to `associate` command to control GTPC overload.

configure
  context `context_name`
  epdg-service `epdg_service_name`
  associate `gtpc-overload-control-profile` variable
end

GTP Load Control Support With Peer Load Value

CSCuu18054 - [ePDG] - GTP load control support

Feature Changes

Load distribution between PGWs using PGW weight in addition to peer load value.

**Previous Behavior:** Not considering peer load value in load distribution between PGWs using PGW weight.

**New Behavior:** Load distribution between PGWs using PGW weight along with peer load value.

**Customer Impact:** Yes

associate

Key word `gtpc-load-control-profile` is added to `associate` command to control GTPC load.

configure
  context `context_name`
  epdg-service `epdg_service_name`
  associate `gtpc-load-control-profile` variable
end

RLF Overload Control

CSCuv11028 - RLF support on ePDG

Feature Changes

Rate limiting of the Diameter messages towards AAA server on SWm interface would be done as per the existing StarOS RLF framework.
GGSN Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from GGSN in StarOS 19 software releases.

- GGSN Enhancements for 19.6.1, page 87
- GGSN Enhancements for 19.6, page 90
- GGSN Enhancements for 19.4.4, page 91
- GGSN Enhancements for 19.4, page 93
- GGSN Enhancements for 19.2, page 105
- GGSN Enhancements for 19.0, page 116

GGSN Enhancements for 19.6.1

This section identifies all of the GGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *GGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your GGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
Handling IMEI or IMSI Mismatch During Handover

CSCvc21444 - Option to reject the MBReq/UPC when IMEI in MBreq/UPC different than the session present in PGW

**Applicable Products:** GGSN, P-GW

**Feature Changes**

During certain network scenarios, when a subscriber's session using a control tunnel endpoint ID (TEID) with P-GW/GGSN is disconnected, the session might be cleared locally (P-GW/GGSN) while it remains active on the peer node. When another subscriber connects to P-GW/GGSN from a home network, there is a probability that P-GW/GGSN might assign the same TEID value that was allotted during the earlier session to this subscriber. When S-GW/SGSN forwards the MBReq/UPC message to P-GW/GGSN with the TEID from the stale session, the session is considered as a handover for the earlier subscriber and P-GW CDRs are generated for that subscriber. The earlier subscriber is thus charged incorrectly.

**Previous Behavior:** Handover of MBReq/UPC was accepted even when IMEI/IMSI in MBreq/UPC was different than the session present in P-GW/GGSN.

**New Behavior:** With this release, handover of MBReq/UPC is rejected when IMEI/IMSI in MBreq/UPC is different than the session present in P-GW/GGSN. This change in behavior is controlled by newly introduced keywords in `egtp modify-bearer-rsp` and `gtpc` CLI commands.

**Command Changes**

`egtp`

The `reject imei-mismatch` keywords are added to the `egtp modify-bearer-rsp` CLI command under the P-GW Service Configuration Mode for configuring the P-GW to reject IMEI in the MBReq message during handover, when the IMEI is different than the one present in P-GW.

`configure`

`context context_name pgw-service service_name`

`| default | no | egtp modify-bearer-rsp reject imei-mismatch`

**Notes:**

- `default`: Resets the command to the default setting.
- `no`: Disables the configuration statement.
• **reject**: Modify Bearer Response reject options.

• **imei-mismatch**: Rejects Modify Bearer Request (MBReq) with CONTEXT_NOT_FOUND (CC 64) cause if IMEI/IMEISV received in MBReq does not match with the IMEI/IMEISV of an existing session.

• By default, the MBReq will be accepted even if IMEI/IMEISV received in MBReq does not match with the IMEI/IMEISV of an existing session.

**gtpc**

The `update-pdp-resp reject imsi-mismatch` keywords are added to the `gtpc` CLI command under the GGSN Service Configuration Mode for configuring the GGSN to reject IMSI in the MBReq message during handover, when the IMSI is different than the one present in GGSN.

configure

```plaintext
context context_name
  ggsn-service service_name
    [default | no ] gtpc update-pdp-resp reject imsi-mismatch
end
```

**Notes:**

• **default**: Resets the command to the default setting.

• **no**: Enables the configuration statement.

• **update-pdp-resp**: Updates PDP Response options.

• **reject**: Updates PDP Response reject options.

• **imsi-mismatch**: Rejects Update PDP Request with NON_EXISTENT (CC 192) cause if IMSI received in Update PDP Request does not match with the IMSI of an existing session.

• By default, the Update PDP Request will be accepted even if IMSI received in Update PDP Request does not match with the IMSI of an existing session.

### Performance Indicator Changes

**show pgw-service name <service_name>**

This command is enhanced to display the current status of **reject imei-mismatch** option. The following sample display is only a portion of the output:

```
EGTP Bit Rate in Rounded Down Kbps : Disabled
EGTP Suppress Update Bearer Request (no bitrate change) : Disabled
EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch : Enabled/Disabled
```

**show ggsn-service name <service_name>**

This command is enhanced to display the current status of the **reject imsi-mismatch** option. The following sample display is only a portion of the output:

```
GTPC Prioritized Rel99 ARP(s) :
GTPC Update PDP Response with Non Existent cause if IMSI mismatch : Enabled/Disabled
3GPP Qos to DSCP Mapping (for G-PDUs):
```
GGSN Enhancements for 19.6

This section identifies all of the GGSN enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the *GGSN Administration Guide* for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your GGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

MS to Change QoS Parameters

CSCvc21496 - MS should able to change the QoS parameters if NoTFT cases [BCM Mixed scenario]

Applicable Products: GGSN

Feature Changes

Previous Behavior: The MS was not allowed to change the QCI in UPC Request for gn-gp GGSN in Mixed Mode BCM.

New Behavior: The existing gtpc CLI command has been modified to allow the MS to change the QCI, if traffic class is not upgraded, in UPC Request for gn-gp GGSN in Mixed Mode BCM.

This is a customer-specific implementation to meet the 3GPP TS 23.060 (Rel 11) Section 9.2 compliance requirements.
Command Changes

gtpc

New keywords are added to gtpc CLI command under GGSN Service Configuration Mode.

configure
    context context_name
    ggsn-service service_name
        [default | no] gtpc support-access-side traffic-class downgrade
    end

Notes:

• default: Restores the default setting. That is, for gn-gp GGSN, the MS will not be allowed to change the QCI when BCM is set as mixed.
• no: Disables the configuration.
• support-access-side: Allows the MS to change the QoS for gn-gp GGSN when BCM is set as mixed. This functionality is disabled by default.
• traffic-class: Allows Traffic Class to be changed by the MS for gn-gp GGSN when BCM is set as mixed. This functionality is disabled by default.
• downgrade: Allows Traffic Class to be downgraded by the MS for gn-gp GGSN when BCM is set as mixed. This functionality is disabled by default.

Performance Indicator Changes

show ggsn-service all

The following field is added to the output of this show command to indicate the configuration status of this feature.

• Support MS QoS Change

GGSN Enhancements for 19.4.4

This section identifies all of the GGSN enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the GGSN Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your GGSN.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

### Handling of DHCPv6 Unicast Messages

CSCvd10605 - DHCP relay from UE to external DHCP server - in R17 PGW forwards the message, in R19 PGW inter

**Applicable Products:** GGSN, P-GW, SAEGW

### Feature Changes

Handling of DHCPv6 unicast messages has been modified with this release.

**Previous Behavior:** All the DHCPv6 messages originating from UE (access side) with destination port number as 547 were consumed by the DHCPv6 server running on the boxer. These messages included DHCPv6 messages sent to unicast, multicast, or both unicast and multicast destination address with destination port number = 547. Other DHCPv6 messages with destination port number != 547 were sent to Gi interface as is, that is without any processing.

**New Behavior:** Following is the behavior when the `dhcpv6-client-unicast` CLI command under DHCP Client Profile Configuration Mode is:

- Disabled (default behavior) – The P-GW only consumes DHCPv6 message received from UE which has destination address as multicast address (FF02::1:2) and port number as 547. This behavior is compliant as per RFC 3315. All other messages are forwarded to Gi interface as it is, without any processing. To proxy the unicast messages, operators should configure `dhcp-client-profile` with `enable dhcpv6-client-unicast` CLI command.

- Enabled – The P-GW consumes DHCPv6 messages received from UE which has any destination address (unicast, multicast, or both unicast and multicast) and port number as 547. These messages are proxied to the external DHCPv6 server with the configured unicast address in DHCPv6-Service. The messages which does not satisfy this condition are forwarded as it is, without any processing, to Gi interface.

**Customer Impact:** Changes in DHCPv6 signaling for unicast packets.
GGSN Enhancements for 19.4

This section identifies all of the GGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *GGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your GGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**IPv6 Prefix Delegation from the RADIUS Server and the Local Pool**

**Feature Description**

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into the following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
IPv6 Prefix Delegation from the RADIUS Server

Important: This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the delegated prefix from the RADIUS server to the UE or the CPE.

To enable the prefix delegation from the RADIUS server, first configure the APN on the P-GW. See Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96

How It Works

This section describes functionality of the prefix delegation from the RADIUS server.

During initial authentication process, RADIUS AAA can authorize Framed-IPv6-Address and Delegated-IPv6-Prefix AVP. Prior to the introduction of this feature Cisco P-GW was able to process only Framed-IPv6-Address AVP. This AVP was treated as Default-Prefix for the attaching UE. P-GW used to allocate 64-bit Interface-ID and the combined 128-bit address. The 64-bit default-prefix, derived from Framed-IPv6-Address AVP, and locally generated 64-bit Interface-ID was sent to the UE during this initial attachment. This 64-bit default-prefix was then associated with the default bearer/PDN for the UE and is considered as the UE’s IPv6 address.

With the introduction of this feature, P-GW is able to process Delegated-IPv6-Prefix AVP along with Framed-IPv6-Address. Delegated-IPv6-Prefix AVP is used to designate the Delegated Prefix of prefix length 48/52/56 bits. This AVP is treated differently than Framed-IPv6-Address. P-GW communicates this delegated prefix to the UE only using DHCPv6 message handshake SOLICIT/ADVERTIZE/REQUEST/RESPONSE. Delegated-IPv6-Prefix is not associated with the default bearer and it is not considered as the UE IPv6 address.

1 Configure the APN on the P-GW, to enable the prefix delegation from the RADIUS server. For the configuration steps, see Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96.

2 Configure APN on the P-GW for the prefix delegation. RADIUS server may send delegated prefix in the Access-Accept message independent of the APN configuration on the P-GW. Based on the APN configuration and presence of delegate prefix in the Access-Accept message, the following combinations are possible. The PDN setup is rejected if:

- The RADIUS server has not sent Delegated Prefix in the Access-Accept message
- The `pd-alloc-method` in the APN configuration is `no-dynamic`

The following table lists all possible combination of the APN configuration and presence of delegated prefix in the Access-Accept message:
### Table 1: Mapping of APN Configuration and RADIUS Message

<table>
<thead>
<tr>
<th>pd-alloc-method in APN Configuration</th>
<th>Delegated-IPv6-Prefix in Access-Accept RADIUS Message</th>
<th>PDN State</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-dynamic</td>
<td>Yes</td>
<td>PDN is set up if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The delegated prefix is successfully allocated after level1 and level2 validations are done</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Validation with the static pool, as mentioned in step 3, is successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If validation fails, PDN is not set up.</td>
</tr>
<tr>
<td>no-dynamic</td>
<td>No</td>
<td>PDN is not set up.</td>
</tr>
<tr>
<td>local/dhcpv6-proxy</td>
<td>Yes</td>
<td>Delegated-IPv6-Prefix in Access-Accept RADIUS message is discarded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDN is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delegate prefix is allocated to the UE, on receiving SOLICIT message, based on the configured <code>pd-alloc-method</code> in the APN.</td>
</tr>
<tr>
<td>local/dhcpv6-proxy</td>
<td>No</td>
<td>PDN is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delegated prefix is allocated to the UE, on receiving SOLICIT message, based on the configured <code>pd-alloc-method</code> in the APN.</td>
</tr>
</tbody>
</table>

3 The P-GW then performs the following two level validation for the prefix length received in Access-Accept RADIUS message:

**Level 1:** Prefix length must be only one of the supported values, such as, 48 / 52 / 56. For any other length, delegate prefix is rejected and PDN is not set up.

**Level 2:** If level 1 validation is passed, the prefix length is compared with the `prefix-delegation-len` configured in the APN using the CLI command, `ipv6 address prefix-delegation-len`.

If there is a mismatch, delegate prefix is rejected and PDN is not set up.

**Important** Level 2 validation is not done if `prefix-delegation-len` is not configured in the APN.

4 Only if the above two level validation is successful, the received delegate prefix is validated against the **static** ipv6 prefix pool configured in the destination context. If validation with the static pool is successful, then the delegate prefix is stored on the P-GW. If validation with the static pool fails, the delegate prefix is rejected and PDN is not set up.
5 After the PDN is set up, the UE or the CPE sends a delegated prefix request by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix, which it had stored earlier, in the DHCPv6 ADVERTISE message to the UE.

6 Next, the UE sends the DHCPv6 REQUEST message to the P-GW and the P-GW sends the DHCPv6 REPLY message to the UE, which completes the DHCPv6 handshake.

1 When the DHCPv6 RELEASE message is received from the UE, P-GW blocks data from any sources IP address from the delegated prefix pool. The delegated prefix is not released to the static ipv6 prefix pool from which it was allocated. If the DHCPv6 SOLICIT message is received again from the UE, the same delegate prefix is sent to the UE. The P-GW starts passing the data from the source address part of the said delegated prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests delegated prefix release by sending DHCPv6 RELEASE REQUEST message to the P-GW.

The DHCPv6 RELEASE REPLY message is not sent to the UE and no message is sent to the RADIUS server if:

• The delegated prefix is released when validity time configured in the DHCPv6 service expires
• When the PDN is cleared

Release triggered reason can be checked from the DHCPv6 statistics(output of the CLI command show dhcpv6 statistics, which are as follows:

<table>
<thead>
<tr>
<th>Session Release Reasons: (dhcp-prefix-delegation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDNs Released: 3</td>
</tr>
<tr>
<td>UE Initiated Release: 1</td>
</tr>
</tbody>
</table>

7 When the PDN is cleared, the delegate prefix is released to the static ipv6 prefix pool from which it was allocated.

Configuring APN to Enable Prefix Delegation From RADIUS Server

Use the following syntax to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the RADIUS Server.

```
cfg
  context context_name
  apn apn_name
    ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic | allow-prefix-delegation
    pd-alloc-method no-dynamic
      ipv6 address prefix-delegation-len [48 | 52 | 56]
    end
  end
```

Notes:

• **dhcpv6-proxy**: Configures the IPv6 address from DHCP server for the APN.
• **dhcpv6-proxy**: Configures the IPv6 address from DHCP server for the APN.
• **local**: Configures the IPv6 address from the local pool configured.
• **no-dynamic**: Configures the IPv6 address as indicated by the authentication server.
• **allow-prefix-delegation**: Configures the APN to allow DHCPv6 prefix-delegation.
• **ipv6 address prefix-delegation-len**: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.
Verifying Prefix Delegation from the RADIUS Server

To verify the Prefix Delegation from the RADIUS Server, use the following show commands.

```
show dhcpv6 statistics
```

When APN is configured to receive Delegated Prefix from Radius Server, the sessions statistics is visible under CLI command output of `show dhcpv6 statistics` and displays the following output:

```
DHCPv6 Session Stats:
  Total Current: 0
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 0
  Local PD: 0
  Total Setup: 5
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 1
  Local PD: 4
  Total Released: 5
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 1
  Local PD: 4
```

**Notes:**

- The total current counter is incremented while sending request reply message to the UE.
- The total current counter is decremented while sending release reply message to the UE (in case of UE initiated release) in the following two cases:
  - on valid life timer expiry
  - when PDN is cleared
- The total current counter may be incremented/decremented multiple times during a PDN connection.
- The total setup counter is incremented multiple times during the PDN connection lifetime. For example, every-time when the SOLICIT message is processed, the PD is successfully allocated to the UE.
- The total release counter is incremented multiple times during a PDN connection lifetime. For example, every-time when the PD is released when DHCPv6 RELEASE message is processed from the UE and/or PD is released due to VALID lifetime timer expiry event. Along with this Session Release Reasons: (dhcp-prefix-delegation) counters are also incremented to the corresponding release reasons.
- Hence in case of delegate prefix allocation from the RADIUS server, Total Setup is equal to Total Current + Total Released.

```
show ggsn-only full all
```

This command displays the following output:

```
IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

show sub pgw-only full all
IPv6 Prefix Delegation from the Local Pool

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request the delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the prefix delegation from the local pool to the UE or the CPE.

To enable the prefix delegation from the local pool, first configure the APN on the P-GW. See Configuring APN for Private Pool Name, on page 99 and Configuring Prefix Delegation on Destination Context, on page 100.

How It Works

This section describes the functionality of the prefix delegation from the local pool.

1 Configure APN on the GGSN/P-GW/SAE-GW to enable the prefix delegation from the local pool. For configuration steps, see Configuring APN for Private Pool Name, on page 99

2 Once the APN is configured, configure the pool on destination context. See Configuring Prefix Delegation on Destination Context, on page 100.

3 The PDN is first set up with default ipv6 prefix of length 64.

4 Once the PDN is set up, User Equipment (UE) or a Customer Premises Equipment (CPE) can request delegated prefix by sending DHCPv6 SOLICIT message to P-GW.

5 The P-GW then performs the following two level validation for the prefix length:

**Level 1:** The prefix length requested in DHCPv6 SOLICIT message must be only one of the supported values, 48 / 52 / 56. For any other length, the SOLICIT is silently dropped at P-GW.

**Level 2:** If level 1 validation is successful, then the following validation is done. If `prefix-delegation-len` is configured in the APN, then delegate prefix allocation of this length is attempted from the local private pool. If `prefix-delegation-len` is not configured in the APN, then delegate prefix allocation of length requested in SOLICIT message is attempted from the local private pool.
The requested length for the delegate prefix must match with the prefix-length configured for the private pool. The requested prefix length is as configured in the APN as ipv6 address prefix-delegation-len 52. If it is not configured in the APN, it may also be from the SOLICIT message. Configure the prefix length for the private pool by using the CLI command, `ipv6 pool ipv6-private prefix 5001::1/48 prefix-length 52 private 0`. Only when these lengths match, delegated prefix allocation from the local pool is successful.

6 The UE or a CPE can request the delegated prefix by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix allocated from the local pool, in the DHCPv6 ADVERTISE message to the UE.

7 Next, the UE sends the DHCPv6 REQUEST message to the P-GW. The P-GW sends the DHCPv6 REPLY message to the UE, which completed the DHCPv6 handshake.

If the delegated prefix allocation from the local pool fails, the DHCPv6 SOLICIT message is silently dropped at the P-GW.

8 When the UE sends the DHCPv6 RELEASE message, the delegated prefix is released to the ipv6 prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests prefix delegation released by sending DHCPv6 RELEASE REQUEST message to the P-GW.

DHCPv6 RELEASE REPLY message is not sent to UE if:

- The prefix delegation is released when validity time configured in the DHCPv6 service expires
- The PDN is cleared

If DHCPv6 SOLICIT message is received again from the UE, a new delegated prefix is allocated from the local pool and sent to the UE.

**Configuring APN to Enable Prefix Delegation From Local Pool**

Configuration Overview

To enable prefix delegation from a local pool, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure the private pool name in the APN configuration mode, to be used for delegate prefix allocation.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the APN to enable or disable IPv6 prefix delegation or default prefix delegation from the local pool.</td>
</tr>
</tbody>
</table>

Configuring APN for Private Pool Name

Use the following steps to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the local pool:

```
config
context context_name
apn apn_name
ipv6 address delegate-prefix-pool pool_name
```
no ipv6 address delegate-prefix-pool
end

config
context context_name
  apn apn_name
    ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic | allow-prefix-delegation
  pd.alloc-method local
    ipv6 address delegate-prefix-pool pool_name
    ipv6 address prefix-delegation-len [48 | 52 | 56]
end

Notes:

• delegate-prefix-pool: Configures a pool of IPv6 address delegated prefix.
  pool_name: Name of the pool with IPv6 address delegated prefix.
• no: Disables the pool of IPv6 address delegated prefix.
• dhcpv6-proxy: Configures the IPv6 address from the DHCP server for the APN.
• local: Configures the IPv6 address from the local pool configured.
• allow-prefix-delegation: Configures the APN to allow DHCPv6 prefix-delegation.
• ipv6 address prefix-delegation-len: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Configuring Prefix Delegation on Destination Context
Use the following configuration to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the Local Pool:

config
context context_name
  ipv6 pool ipv6-private prefix 5001::1/48 prefix-length [48 | 52 | 56] private 0
end

Notes:

• ipv6 pool: Modifies the current context's IP address pools by adding, updating, or deleting a pool. This command also resizes an existing IP pool.

---

Important
The ipv6 prefix pool must be of the type private.

Verifying Prefix Delegation from the Local Pool
To verify the Prefix Delegation from the local pool, use the following show commands.

show dhcpv6 statistics

When APN is configured to receive Delegated Prefix from the local pool, the sessions statistics is visible under CLI command output of show dhcpv6 statistics and displays the following output:

DHCPv6 Session Stats:
  Total Current: 0
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 0
Local PD: 0
Total Setup: 5
DHCP Proxy: 0
DHCP Server: 0
DHCP PD: 0
Radius PD: 1
Local PD: 4

Total Released: 5
DHCP Proxy: 0
DHCP Server: 0
DHCP PD: 0
Radius PD: 1
Local PD: 4

Notes: In case of delegate prefix allocation from local pool, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

show sub pgw-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

show sub saegw-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

IPv6 Interface ID from the RADIUS Server
This feature allows the RADIUS/AAA Server to send an Interface-ID to the GGSN/P-GW/SAEGW service, in the Access-Accept message. This interface-id is used by these services and is communicated to the UE or the CPE. In this case, the GGSN/P-GW/SAEGW do not allocate a local interface-id. If the RADIUS/AAA server do not send an interface-id, then GGSN/P-GW/SAEGW allocate an interface-id locally and send it to the UE.

show apn statistics
Following CLI command can be used to see the total current active counter for Interface-ID allocation.

IP address allocation statistics:
Total IPv6 Interface IDs allocated:
  AAA provided: 1
  Locally Generated: 2
Limitations

Following are the limitations of the IPv6 Prefix Delegation feature:

- RADIUS ACCOUNTING messages do not support delegated prefix.
- Zero PL in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- NULL PD prefix in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- For PDN type v4v6, the dhcpv6-proxy method of allocation for the default prefix is not supported.
- The UE-requested Delegated Prefix in SOLICIT message is not supported. If the UE sends SOLICIT message requesting Delegated Prefix, it is rejected.
- One PD prefix per PDN is supported; multiple PD-prefixes per PDN are not supported.
- P-GW and GGSN do not support local-based and RADIUS-based allocation of both DHCPv6 prefix delegation and framed prefix delegation from the same pool. Hence the allocation is done from separate pools. Framed prefix received in the access-accept message is not part of the delegated prefix range.

GGSN Support for PDP Type PPP

Feature Changes

This feature describes support for PDP type Point to Point Protocol (PPP) in GGSN. PPP sessions originated from MS/UE terminates on the GGSN. User traffic is encapsulated into PPP frames between the UE-GGSN. These PPP packets (data/control) are tunneled inside GTPU tunnels between the SGSN/GGSN.

Limitations:

This feature has the following limitations:
- Secondary PDP context creation for GGSN PDP type PPP session is not supported.
- PDP type PPP for GnGp GGSN is not supported.
- Routing Behind Mobile Station functionality for GGSN PDP-type PPP is not supported.
- Inter-Chassis session recovery of GGSN PDP-type PPP sessions is not supported.
- Multi-PDN with PDP-type PPP is not supported.
- Inter-RAT handovers with PDP-type PPP is not supported.
- L2TP with PDP-type PPP is not supported in this release.
- Lawful Interception with PDP-type PPP is not supported.
- Static IP address allocation with PDP-type PPP is not supported.
- IPv6 address allocation with PDP-type PPP is not supported.
ECS Rules Written for IP Protocol

CSCuy14480 - ECS rules written for IP protocol 132 are not hit

**Applicable Products:** GGSN, P-GW, SAE-GW

**Feature Changes**

**Previous Behavior:** Earlier, SCTP downlink traffic passed through the default bearer instead of dedicated bearer, when the received packet was matched with the packet filter, which was configured in either of the following ways:

- Only source port or destination port was configured
- IP Address and port was configured

However, when the packet filter was configured for source and destination IP address, and the packet filter matched with the received packet, traffic passed through the dedicated bearer.

**New Behavior:** Now, SCTP downlink traffic pass through the dedicated when the received packet is matched with the packet filter, which was configured in either of the following ways:

- Source and destination IP address
- Only source port or destination port was configured
- IP Address and port was configured

SPGW Incorrectly Sending UDPv6 Packets

CSCuy78988- SPGW incorrectly sending UDPv6 packets with 0x0 checksum against RFC2460

**Applicable Products:** GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

**Previous Behavior:** Earlier, if the result of the UDPv6 checksum calculation is zero, GW used to send the same, which effectively disables checksum for that packet. This was not compliant with the RFC2460, which suggests the checksum value to be set to 0xFFFF if derived calculation is zero.

**New Behavior:** After the fix, the checksum value is set to 0xFFFF if the result checksum calculation is ZERO and the compliance is met.

**Impact on customer:** Packet drops might be seen at peer, which does not support of handling packet with 0xFFFF checksum as suggested by the RFC.

DHCPv6 Related GTPU Packets

CSCuz27274 - DHCPv6 related GTPU packets counted as data packets at sessmgr

**Applicable Products:** GGSN
Feature Changes

**Old Behavior:** DHCPv6 uplink control packets were getting counted for charging.

**New Behavior:** This edet retains the packet counting behavior. However, the charging of DHCPv6 packets in the up-link direction for GGSN has been stopped.

**Impact on Customer:** GGSN Uplink DHCPv6 control packets are not charged.

### DSCP Marking in a PPP Call

CSCuz45804 - Issue in DSCP Marking in PPP Call

**Applicable Products:** GGSN

**Feature Changes**

**Previous Behavior:** A PPP call was established after doing the following configuration:
- QCI-QoS mapping table was configured in an APN
- DSCP values were configured in the GGSN service

The DSCP marking for the downlink encapsulation packets was not as expected. The downlink packets must have selected values from the QCI-QoS mapping table, as it did in an IPv4 call. However, instead of picking values from the QCI-QoS mapping table, it selected values from the GGSN-service configuration.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>For an IPv4 call, the DSCP marking for the downlink encapsulation was as configured in the QCI-QoS mapping table.</td>
</tr>
</tbody>
</table>

**New Behavior:** A PPP call or an IPv4 call is established after doing the following configuration:
- QCI-QoS mapping table is configured in an APN
- DSCP values are configured in the GGSN service

The DSCP downlink encapsulation packets are marked with values from the QCI-QoS mapping table for both PPP call and an IPv4 call.

### Bulk Stats Schema for GGSN PPP Call

CSCuz49627 - PPP bulkstat schemas not getting updated for ggsn-PPP call

**Applicable Products:** GGSN

**Feature Changes**

**Old Behavior:** Earlier, PPP bulk stats schemas were not updated for a PPP call on GGSN.

**New Behavior:** Now, PPP bulk stats schemas are updated for a GGSN-PPP call on GGSN.
**Impact on Customer:** It is possible to view/peg PPP bulk stats for a PPP call on GGSN.

## GGSN Enhancements for 19.2

This section identifies all of the GGSN enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *GGSN Administration Guide* for this release.
- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.
- Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your GGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

## DHCPv6 Unicast Address Support

CSCu792596 - DHCPv6 Unicast address support in message exchange.

**Applicable Products**: GGSN, P-GW, and SAEGW

### Feature Changes

**Important**

Use of DHCPv6 Unicast Address Support requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.
The IPv6 prefix delegation for requested UE is either allocated locally or from an external DHCPv6 server by P-GW or GGSN based on configuration at P-GW or GGSN. Currently, these DHCPv6 messages are sent to the external DHCPv6 server using multicast address as destination address. This feature adds Unicast address support which enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCPv6 service. The operator need to configure a CLI to support for client unicast operation to the DHCPv6 Server. By default client-unicast is disabled.

**Previous Behavior:** Earlier there was no support to send DHCPv6 messages to the server on a unicast address. Message exchange used to happen on a multicast address.

**New Behavior:** Now with this feature, support for sending all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in DHCPv6 service has been added.

**Customer Impact:** Operators will now be able to send DHCPv6 messages on a unicast address by using the config CLI mentioned below.

### Command Changes

**dhcpv6-client-unicast**

A new command `dhcpv6-client-unicast` has been added to the existing command `dhcp-client-profile`. This CLI command enables support for client unicast operation to the DHCPv6 Server. By default client-unicast is disabled.

```conf
configure
c
context context_name
dhcp-client-profile
    [ enable | disable ] dhcpv6-client-unicast
end
```

**Notes:**

- `dhcpv6-client-unicast`: enables client to send messages on unicast address towards server.

### Performance Indicator Changes

**show configuration**

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

```
  dhcp-client-profile clientprof
  disable dhcpv6-client-unicast
  request dhcp-option dns-address
  request dhcp-option sip-server-address
```

**show configuration**

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

```
  dhcp-client-profile clientprof
  disable dhcpv6-client-unicast
  dhcp-client-profile dhcp-client-profile
  request dhcpv6-client-unicast
  request dhcp-option sip-server-address
```
show configuration verbose

When client unicast is enabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

dhcp-client-profile clientprof
enable dhcpv6-client-unicast
dhcp-client-profile dhcp-client-profile
disable dhcpv6-client-unicast

show dhcpv6-client-profile all

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

Client Profile name: clientprof
Context: egress
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
NetBios_address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: enabled
Client identifier: IMSI
User Class Option: NONE
Client Profile name: dhcp-client-profile
Context: egress
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
NetBios_address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: disabled
Client identifier: IMSI
User Class Option: NONE

Traffic Shaping at the APN-AMBR Data Rate Level

CSCuv23766 - Traffic Shaping; CSCuw33511 - Reduce Policing bucket interval from 100 ms to 10 ms.

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

| Important | In StarOS release 19.2, this feature is supported as lab quality only. With StarOS release 19.2.1, this feature is fully qualified as Deploy Quality. |
| Important | Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information. |

Traffic Shaping is a rate limiting method similar to Traffic Policing, but provides a buffer facility for packets exceeding the configured limit. Once packets exceed the data-rate, the packet is queued inside the buffer to be delivered at a later time.
The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data, the system can be configured to either drop the packets or retain it for the next scheduled traffic session.

Traffic will be shaped to the configured APN-AMBR value. Previously, data carried on non-GBR bearers was policed at the configured APN-AMBR rate. APN-AMBR policing dropped the data that did not match the configured APN-AMBR. With APN-AMBR traffic shaping, non-GBR data that does not match the configured APN-AMBR rate will be buffered. When enough memory tokens are available, the data will be transmitted. In addition, operators still have the option to allow operators to drop the data when the buffer limit is reached.

**Command Changes**

**apn-ambr**

The `shape` and `transmit-when-buffer-full` keywords are now available in *APN Configuration Mode* for traffic shaping on the GGSN, P-GW and SAEGW.

```plaintext
configure context context_name
  apn apn_name
    apn-ambr rate-limit direction { downlink | uplink } |
    violate-action { shape [transmit-when-buffer-full ] }
    [ default | no ] apn-ambr rate-limit direction { downlink | uplink }
end
```

Notes:

- `shape [transmit-when-buffer-full ]`: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.

**apn-ambr**

The `token-replenishment-interval` keyword has been added to the `apn-ambr` command in *APN Configuration Mode*. This token replenishment interval is used for both APN AMBR traffic policing and traffic shaping. Operators have the option of using the default interval (100ms) or configuring a lower token replenishment interval of 10ms. Reducing the interval to 10ms helps reduce the queuing time required by the 100ms interval for a given packet size.

```plaintext
configure context context_name
  apn apn_name
    apn-ambr rate-limit token-replenishment-interval duration_msecs
end
```

Notes:

- Where `token-replenishment-interval` is the time duration, in milliseconds, to be used for APN AMBR-based traffic policing and shaping.
- Valid entries are 10 or 100 milliseconds. The default is 100 milliseconds.
The **milliseconds** variable has been added to the **auto-readjust duration** keyword for the **apn-ambr** command in **APN Configuration Mode**. This variable allows operators to configure the **auto-readjust duration** in increments of 100 milliseconds.

```
configure
  context context_name
    apn apn_name
      apn-ambr rate-limit direction { downlink | uplink } | burst-size { auto-readjust duration milliseconds integer 100...900 } [ default | no ] apn-ambr rate-limit direction { downlink | uplink }
  end
```

**Notes:**

- Where **milliseconds** is the time duration, in milliseconds, to be used for the **auto-readjust duration** function in APN AMBR-based traffic policing and shaping.
- Valid entries are from 100 to 900 milliseconds, in increments of 100 milliseconds. For example, 100, 200, 300 and so on.

The new **traffic shape** command has been added to **Global Configuration Mode**. This command enables operators to configure the maximum limit for data buffering during APN AMBR traffic shaping.

```
configure
  traffic shape max-buffer-size sessmgr MBs subscriber MBs
  end
```

**Notes:**

- **sessmgr MBs**: Specifies the amount of memory allocated towards buffering session manager instances during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The **sessmgr MBs** setting should be larger than the **subscriber MBs** setting.
- **subscriber MBs**: Specifies the amount of memory allocated towards buffering subscriber traffic during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The **subscriber MB** setting should be less than the **sessmgr MB** setting.

**Caution**

Standard size buffers (500, 2k, and 10k bytes) are used for buffering packets to avoid memory fragmentation. As a result, there may be additional memory overhead in the memory used for buffering. The buffer limit in the above configuration refers to actual effective bytes used to store packets. Use caution to use appropriate buffer limits, so that the system does not significantly affect the overall Session Manager memory requirement for sessions.
Performance Indicator Changes

show configuration verbose

The output of this command has been enhanced to provide APN AMBR traffic shaping parameters for the GGSN, P-GW, and SAEGW, if configured.

- `apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape (if configured without the `transmit-when-buffer-full` option).
- `apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape transmit-when-buffer-full (if configured with the `transmit-when-buffer-full` option).

The output of this command has also been enhanced to show the `token-replenishment-interval` for APN AMBR traffic shaping and policing, if configured.

- `apn-ambr rate-limit token-replenishment-interval <milliseconds>`

The output of this command has also been enhanced to provide the maximum buffer size allocated for traffic shaping for both subscribers and the session manager.

- `traffic shape max-buffer-size sessmgr <no. of MB> subscriber <no. of MB>`

show subscriber pgw-only/ggsn-only/saegw-only full all

Command output for each of these commands has been enhanced to show APN AMBR traffic shaping configuration parameters and statistics.

- APN AMBR shaping:
- Token replenishment interval(ms):
- Downlink traffic-shaping: <Enabled or Disabled>
- APN-AMBR(bps):
- Buffer full action: <drop or transmit>
- Burst Size:
- Auto Readjust: <Enabled or Disabled>
- Auto Readjust Duration(ms):
- Peak Burst size (bytes):
- Guaranteed burst size (bytes):
- Queued data (packets):
- Queued data (bytes):
- Drop count (packets):
- Drop count (bytes):
- Buffer Full Packets Fwd:
• Buffer Full Bytes Fwd:
• Packets Forwarded:
• Bytes Forwarded:
• Uplink traffic shaping: <Enabled or Disabled>
• APN-AMBR(bps):
• Buffer full action: <drop or transmit>
• Burst Size:
• Auto Readjust: <Enabled or Disabled>
• Auto Readjust Duration(ms):
• Peak Burst Size:
• Guaranteed burst size (ms):
• Queued data (packets):
• Queued data (bytes):
• Drop count (packets):
• Drop count (bytes):
• Buffer Full Packets Fwd:
• Buffer Full Bytes Fwd:
• Packets Forwarded:
• Bytes Forwarded:

If APN AMBR traffic shaping is disabled, the following output appears:
• APN AMBR Shaping:
• Downlink traffic-shaping: Disabled
• Uplink traffic-shaping: Disabled

**Virtual APN Selection Based On PDP-Type**

CSCuo61924 - Virtual APN based on PDP type.

**Applicable Products:** GGSN, P-GW, and SAEGW

**Feature Changes**

The current implementation of selection of virtual APN is based on various criteria and a call received on a selected APN can be forwarded to another APN based on the configured criteria. This feature enables the operator to select the Virtual APN on the basis of PDP-type and PDP-type for roamers. For this, PDP-type rules for PDP-types IPv4, IPv6, and IPv4v6 have been added to the existing Virtual APN rules. Also, roaming
**mode-roaming** has been implemented as a secondary option to PDP type enable the operator to select the Virtual APN on the basis on PDP-type for roamers.

**Previous Behavior:** Earlier, Virtual APN was selected on the basis on various factors such as IMSI and MSISDN. PDP-type and PDP-type for roamers were not the basis for selection.

**New Behavior:** Now, an existing CLI **virtual-apn preference** has been modified to enable the Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

**Command Changes**

**virtual-apn preference**

New keyword **pdp-type** has been added to the command **virtual-apn preference** to support Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

```bash
configure
  context  context_name
  apn  apn_name
  virtual-apn preference  priority  apn  apn_name
    [access-gw-address { ip_address | ip_address/mask } |
     bearer-access-service  service_name
     | cc-profile  cc_profile_index
     | pre-rel-9.1-cc-behavior  cc_behavior_value
     | ]
    [rat-type { eutran | gan | geran | hspa | utran | wlan } ]
    | [cc-behavior  cc_behavior_value ]
    [rat-type { eutran | gan | geran | hspa | utran | wlan } ]
    | [domain  domain_name
     | IPv4 | IPv6
     | mcc  mcc_number
     | mnc  mnc_number ]
    | [cc-profile  cc_profile_index
     | pre-rel-9.1-cc-behavior  cc_behavior_value ]
    | [msin-range from  msin_range_from
to  msin_range_to ]
    | [rat-type { eutran | gan | geran | hspa | utran | wlan } ]
    | [msisdn-range from  msisdn_start_range
to  msisdn_to_range ]
    | [rat-type { eutran | gan | geran | hspa | utran | wlan } ]
    | [pdp-type { ipv4 | ipv6 | ipv4v6 } ]
    | [roaming-mode { roaming } ]
    | [rat-type { eutran | gan | geran | hspa | utran | wlan } ]
    | [roaming-mode { home | roaming | visiting } ]

{no}
  virtual-apn preference  priority
end
```

**Notes:**

- **pdp-type** Configures pdp-type rule.
- **ipv4** Configures Virtual APN rule for ipv4 addresses.
- **ipv6** Configures Virtual APN rule for ipv6 addresses.
- **ipv4v6** Configures Virtual APN rule for ipv4v6 addresses.
- **roaming-mode** \{ home | roaming | visiting \} Supports separate PDP context or PDN connection processing for roaming subscribers.

**Performance Indicator Changes**

**show apn <apn_name>**

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

<table>
<thead>
<tr>
<th>Virtual APN Configuration:</th>
<th>Selected-APN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference Rule-Definition</td>
<td>PDP Type = ipv4 telenor.ipv4v6</td>
</tr>
<tr>
<td>1</td>
<td>PDP Type = ipv6 telenor.ipv6v6</td>
</tr>
<tr>
<td>2</td>
<td>PDP Type = ipv6 telenor.ipv6nat64</td>
</tr>
</tbody>
</table>
show pgw-service stats all

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

Virtual APN Configuration:
Preference Rule-Definition    Selected-APN
1  PDP Type = ipv4  telenor.ipv4v6
2  PDP Type = ipv6  telenor.ipv4v6
3  PDP Type = ipv4v6
Roaming mode = roaming  telenor.nat64

show saegw-service stats all function pgw

This command has been modified to include counters to indicate the number of PDNs setup and rejected for Virtual APNs selected on the basis of PDP-type at the service level. Modified output includes the following fields:

VAPNs Selected Based on Configured PDP-Type
IPv4: Setup: 8    Rejected: 5
IPv6: Setup: 8    Rejected: 5
IPv4v6: Setup: 8  Rejected: 5

Virtual APN Selection Based on CC-Behavior

CSCuu43329 - Virtual APN selection based on all 16 bits of charging characteristics.

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Virtual APN Selection feature enables an operator to select Virtual APN based on all 16 bits of Charging Characteristics for GGSN, P-GW, and SAEGW nodes. Earlier, virtual APN selection was possible only on the basis on 4 cc-profile bits. With this feature, now an operator can select a Virtual APN on the basis on 4 cc-profile bits and 12 cc-behavior bits or on the basis on complete 16 cc-behavior bits. This selection can be done with the help of a CLI.

Previous Behavior: Earlier, Virtual APN selection was possible on the basis of 4 cc-profile bits.

New Behavior: Now, Virtual APN selection can now be done on the basis of 4 cc-profile bits and 12 cc-behavior bits or complete 16 cc-behavior bits.

Customer Impact: Virtual APN can be selected based on all 16 bits of Charging Characteristics.
Command Changes

virtual-apn preference

New keywords `pre-rel-9.1-cc-behavior` and `cc-behavior` have been added to the command `virtual-apn preference` to support Virtual APN selection on the basis of all charging characteristics.

configure
context `context_name`
apn `apn_name`
virtual-apn preference `priority` `apn_name` { `access-gw-address` { `ip_address` | `ip_address/mask` } | bearer-access-service `service_name` | cc-profile `cc_profile_index` | `pre-rel-9.1-cc-behavior` `cc_behavior_value` || rat-type { `eutran` | `gan` | `geran` | `hspa` | `utran` | `wlan` } || `cc-behavior` `cc_behavior_value` || rat-type { `eutran` | `gan` | `geran` | `hspa` | `utran` | `wlan` } || domain `domain_name` | mcc `mcc_number` | mnc `mnc_number` || cc-profile `cc_profile_index` | `pre-rel-9.1-cc-behavior` `cc_behavior_value` || `cc-behavior` `cc_behavior_value` || rat-type { `eutran` | `gan` | `geran` | `hspa` | `utran` | `wlan` } || msisdn-range from `msisdn_start_range` to `msisdn_to_range` || rat-type { `eutran` | `gan` | `geran` | `hspa` | `utran` | `wlan` } || roaming-mode { `home` | `roaming` | `visiting` } }
{ no } virtual-apn preference `priority` end

Notes:

- `pre-rel-9.1-cc-behavior` `cc_behavior_value` Specifies the behavior charging characteristics bits in 12 bit format, post 3GPP release 9.1. For example, if `cc-behavior` is configured as 0x341, then 0x34 corresponds to B12-B5 [MSB] and 0x1 corresponds to B4-B1 [Least significant nibble] of CC behavior.`cc_behavior_value` must be a hex value in the range 0x0000 to 0xFFFF.

- `cc-behavior` `cc_behavior_value` Specifies the behavior charging characteristics bits in 16 bit format, post 3GPP release 9.1. For example, if `cc-behavior` is configured as 0x3412, then 0x34 corresponds to B15-B8 [MSB] and 0x12 corresponds to B7-B0 [LSB] of charging char)`cc_behavior_value` must be a hex value in the range 0x0000 to 0xFFFF.

Performance Indicator Changes

show apn `<apn_name>`

The following fields have been added to the output of this command.

Virtual APN Configuration:
<table>
<thead>
<tr>
<th>Preference</th>
<th>Rule-Definition</th>
<th>Selected-APN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CC Profile Index = 1</td>
<td>cisco.ipv4</td>
</tr>
<tr>
<td>2</td>
<td>RAT Type = gan</td>
<td>intershat2</td>
</tr>
<tr>
<td>3</td>
<td>CC Profile Index = 2</td>
<td></td>
</tr>
<tr>
<td>Pre Rel-9.1 CC Behavior Bits = 0x341</td>
<td>cisco.ipv4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CC Profile Index = 3</td>
<td></td>
</tr>
<tr>
<td>Pre Rel-9.1 CC Behavior Bits = 0x341</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAT Type = gan</td>
<td>intershat2</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CC Behavior Bits = 0x3412</td>
<td>cisco.ipv4</td>
</tr>
<tr>
<td>6</td>
<td>CC Behavior Bits = 0x1204</td>
<td></td>
</tr>
<tr>
<td>RAT Type = gan</td>
<td>cisco.ipv4</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>IMSI-MCC = 100, IMSI-MNC = 100</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>IMSI-MCC = 100, IMSI-MNC = 100</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CC Profile Index = 2</td>
<td></td>
</tr>
<tr>
<td>Pre Rel-9.1 CC Behavior Bits = 0x104</td>
<td>cisco.ipv4</td>
<td></td>
</tr>
</tbody>
</table>
The following fields have been added to the output of this command.

```
apn starent.ipv4
selection-mode sent-by-ms
accounting-mode gtp
ip context-name pgw-gi
virtual-apn preference 1 apn cisco.ipv4 cc-profile 1
virtual-apn preference 2 apn cisco.ipv4 cc-profile 1 rat-type eutran
virtual-apn preference 3 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104
virtual-apn preference 4 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104 rat-type gan
virtual-apn preference 5 apn star.com cc-behavior 0x1204
virtual-apn preference 6 apn star.com cc-behavior 0x1204 rat-type gan
virtual-apn preference 7 apn abc2.com mcc 100 mnc 100 cc-profile 1
virtual-apn preference 8 apn pqr2.com mcc 100 mnc 100 cc-profile 2 pre-rel-9.1-cc-behavior 0x104
virtual-apn preference 9 apn star2.com mcc 100 mnc 100 cc-behavior 0x1204
exit
```
show sub saegw-only full all

The following fields have been added to the output of this command.

charging id: 16777216
Charging chars (hex): 0x341 Charging chars: flat

GGSN Enhancements for 19.0

This section identifies all of the GGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *GGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your GGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

Change to the 'show gtpc' CLI Command

CSCuc83409 - 'show gtpc summary' not able to filter on imsi, ip-address, callid, username

**Feature Changes**

Unwanted filter command options have been removed from the CLI commands *show gtpc* and *show gtpc summary.*
**Previous Behavior:** The CLI commands `show gtpc` and `show gtpc summary` had many filter options.

**New Behavior:** The CLI commands `show gtpc` and `show gtpc summary` have been modified to remove the following keywords and their associated options:

- callid
- imsi
- user-address

**Performance Indicator Changes**

**show gtpc**

This command has been modified as follows:

Previous Command: `show gtpc { all | apn | callid | counters | full | ggsn-service | imsi | sgsn-address | smgr-instance | statistics | summary | user-address | username }

New Command: `show gtpc { all | apn | counters | full | ggsn-service | sgsn-address | smgr-instance | statistics | summary }`

**show gtpc summary**

This command has been modified as follows:

Previous Command: `show gtpc summary {all | apn | callid | ggsn-service | imsi | sgsn-address | smgr-instance | user-address | username}

New Command: `show gtpc summary { all | apn | ggsn-service | sgsn-address | smgr-instance }`

**MS-to-MS traffic for IPSec**

CSCum98092 - MS-to-MS traffic for Ipsec

**Feature Changes**

When ACL includes a destination "any" and IPSec is used in the communication, then all packets are sent to the remote IPSec peer through a tunnel, even when the subscriber is in the same IP pool. Some IPSec gateways cannot handle the returning packets from the tunnel. This enhancement allows the routing packets within the system.

Hence, with this enhancement, for any mobile to mobile communication the following options are possible:

- Local routing within the node is possible and there is no need to send traffic out of the node for re-routing back.
- Forced routing outside GGSN such as IPSec tunnel and next-hop is also possible.

Both options are configurable and available for all outside interface type such as nexthop, VLAN, MPLS, GRE tunnel, IPSec tunnel, GRE over IPSec, and so on.

**Previous Behavior:**
• Packets are forced into the tunnel.
• By default, ip guarantee framed route local switching has been enabled for VPN and VRF level.

**New Behavior:**

• Packets are routed to connected subnets internally or can be routed into the tunnel if the option is configured.
• By default, ip guarantee framed route local switching has been disabled at both VPN and VRF level. When you change the value at VPN level, all the VRF under that VPN will get affected unless they are explicitly configured with a value.

**Command Changes**

`framed-route local-switching`

The default configuration for ip guarantee framed route local switching has been changed. Now, by default, ip guarantee framed route local switching has been disabled at both VPN and VRF level. When you change the value at VPN level, all the VRF under that VPN will get affected unless they are explicitly configured with a value.

```plaintext
configure
c  ontex t  con text_ name
   |  default | no | ip guarantee framed-route local-switching  var iable
end
```

Notes:

• **no**: Disables local switching of framed route packets.
• **default**: At VPN level, disables local switching of framed route packets. At VRF level, falls back to configuration in base context.
• **framed-route local-switching**: Enables local switching of framed route packets. By default, this functionality is enabled.

**Change in the CLI Command Output**

CSCus36138 - CLI diff between config file and config after booting

**Feature Changes**

**Previous Behavior:** Earlier, the output of CLI command show configuration displayed the field source-port standard.

**New Behavior:** Now, the output of CLI command show configuration does not show the field source-port standard.
"Newcall policy reject" Enhancement for Releasing Existing Calls

CSCuu21036 - Newcall policy reject enhancement for releasing existing calls

**Applicable Products** = GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

If the newcall policy is set to `reject release-existing-session` and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

**Important**

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Command Changes**

`newcall policy`

The keyword `release-existing-session` has been added to this command to reject and release existing IMSI/IMEI session(s) when newcall arrives.

`newcall policy ggsn-service { apn name apn_name | all | name service_name } reject [ release-existing-session ]`

`no newcall policy ggsn-service { apn apn_name | all | name service_name }`

**Notes:**

- `reject release-existing-session`: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Disabled by default.

Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions.

**Performance Indicator Changes**

`show egtpc statistics verbose`

The following new field has been added to indicate such calls released:

- NewCall Reject Existing Sessions Released
Syslogging of Reject Events

CSCuu21047 - Inclusion of IMSI in EGTPC logs for reject events

Applicable Products = GGSN, P-GW, SAEGW, S-GW

Feature Changes

Syslogging of Reject Events

Previous Behavior: The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all eGTP-C system event logs of type error and critical.

New Behavior: The P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the eGTP-C event log details for the system event logs of type error and critical, if available. If the IMSI is not available, the P-GW/SAEGW/S-GW will make the best effort to obtain the IMEI.

Command Changes

logging

The include-ueid keyword has been added to the logging command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

configure

logging include-ueid
no logging include-ueid
end

Performance Indicator Changes

show configuration

The output of this command has been enhanced to indicate if the logging command is enabled with the include-ueid keyword.

- logging include-ueid
- no logging include-ueid

IMSI/IMEI Available in System Event Logs of Type Error and Critical

CSCuu51587, CSCut68271 - Inclusion of IMSI/IMEI in logs

Applicable Products = GGSN, P-GW, SAEGW, S-GW
Feature Changes

IMSI/IMEI Available in System Event Logs of Type Error and Critical

**Previous Behavior:** The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all system event logs of type error and critical.

**New Behavior:** The GGSN/P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available.

---

**Important** Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.

---

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format &quot;[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d&quot;</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s&quot;</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Ran out of session handles&quot;</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format &quot;[IMSI &lt;IMSI&gt;]%s&quot;</td>
</tr>
<tr>
<td><strong>Modified Events</strong></td>
<td></td>
</tr>
<tr>
<td>139001</td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td>191006</td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td>10034</td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR PGW REJECT BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s&quot;. For example &quot;[IMSI 112234454566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>12668</td>
<td>Represents <code>fsm_event_error</code> in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot;</td>
</tr>
<tr>
<td>12774</td>
<td>Represents <code>pgw_purge_invalid_ciderr</code> in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot;</td>
</tr>
<tr>
<td>12855</td>
<td>Represents <code>ncqos_nrspca_trig_err</code> in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td>12857</td>
<td>Represents <code>ncqos_nrupe_tft_err</code> in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>12858</td>
<td>Represents <code>ncqos_nrxx_trig_already</code> in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>12859</td>
<td>Represents <code>ncqos_nrxx_tft_check抗议err</code> in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%u&gt;: pf_id_bitmap 0x%x and tft_opcode: %d&quot;</td>
</tr>
<tr>
<td>12860</td>
<td>Represents <code>ncqos_sec_rej</code> in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12861</td>
<td>Represents <code>ncqos_upc_rej</code> in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12862</td>
<td>Represents <code>ggsn_subsession_invalid_state</code> in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state: &lt;%s&gt;.[event:&lt;%s&gt;]&quot;</td>
</tr>
<tr>
<td>11830</td>
<td>Represents <code>gnpg_handoff_rejected_for_pdh_ipv4v6</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
<tr>
<td>11832</td>
<td>Represents <code>gnpg_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents <code>gnpg_handoff_from_ggsn_rejected_no_ggsn_call</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0x%x&gt; not found.&quot;</td>
</tr>
<tr>
<td>12960</td>
<td>Represents <code>gtp_pdp_type_mismatch</code> in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN %s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>11282</td>
<td>Represents <code>pcc_intf_error_info</code> in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents <code>collision_error</code> in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d&quot;</td>
</tr>
</tbody>
</table>
### Event Log # | Description
---|---
11917 | Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr %d: Received invalid bearer binding request from ACS."
11978 | Represents saegw_uid_error in format "[IMSI <IMSI>] %s"
11994 | Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005 | Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <%s> in state <%s>"
140006 | Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <%s> in state <%s>"
140007 | Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <%s> in state <%s>"
10726 | Represents saegwdrv_generic_error "[IMSI <IMSI>] %s"

### Command Changes

**logging**

The `include-ueid` keyword has been added to the `logging` command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```plaintext
configure
logging include-ueid
no logging include-ueid
end
```

### Performance Indicator Changes

**show configuration**

The output of this command has been enhanced to indicate if the `logging` command is enabled with the `include-ueid` keyword.

- logging include-ueid
- no logging include-ueid
Pre-Release 8 QoS Mapping

CSCuv49840 - Non standard QCI modification fails when mapped to same pre-rel8 QCI

Feature Changes

Previous Behavior: When multiple non-standard QCIs were associated with the same pre-release 8 QoS value (such as the following example) and there was a change between those non-standard QCI, QCI was not updated.

```plaintext
configure
  qci-qos-mapping name
    operator-defined-qci 190 non-gbr pre-rel8-qos-mapping 7
    operator-defined-qci 254 non-gbr pre-rel8-qos-mapping 7
end
```

New Behavior: Now, when multiple non-standard QCIs are associated with the same pre-release 8 QoS value and there is a change between those non-standard QCIs, the non-standard QCIs will be updated and no UPC will be triggered towards the access side for the same.
GTPP Changes in Release 19

This chapter identifies GTPP management features and functionality added to, modified for, or deprecated from GTPP in StarOS 19 software releases.

- GTPP Enhancements for 19.2, page 125

GTPP Enhancements for 19.2

This section identifies all of the GTPP enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the GTPP Interface Administration and Reference for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Support for Low Access Priority Indicator in CDRs

CSCuw20972 - LAPI support for Custom39 dictionary

Applicable Products: GGSN, P-GW

Feature Changes

This release provides support for Low Access Priority Indicator (LAPI) attribute in eG-CDRs for custom39 and in PGW-CDRs for custom38 GTPP dictionaries. This attribute field indicates if the PDN connection has a low priority, i.e. for Machine Type Communication (MTC).

This attribute is included in eG-CDRs and PGW-CDRs only if the gtpp attribute lapi CLI command is configured in the GTPP Group Configuration mode.
Support for Low Access Priority Indicator in CDRs
CHAPTER 7

HA Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from HA in StarOS 19 software releases.

- HA Enhancements for 19.0, page 127

HA Enhancements for 19.0

This section identifies all of the HA enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the HA Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Subscriber Level Support for Periodical and Event Based Idle Microcheck Point

CSCuu12448 - Support periodical & event based idle microcheck point generation for HA

Feature Changes

Previous Behavior: Subscriber level support was not added for periodical/deemed idle timeout.

New Behavior: ICSR micro checkpoints can now be sent based on the configuration (deemed/periodical) at subscriber level. As part of this feature, the following new CLI commands are added in the subscriber template level.

1 Micro-checkpoint-deemed-idle: Configures micro-checkpoint duration when UE transitions from Idle to Active and vice versa. Micro-checkpoint-deemed-idle value should be less than idle timeout value.
2 Micro-checkpoint-periodicity: ICSR micro checkpoint periodicity for idlesecs is made configurable instead of using the default periodicity of 10 seconds. This way, the operators can configure a large value as per need to reduce the number of micro checkpoints on the SRP link.

Important On the fly change of configuring micro-checkpoint-deemed-idle to micro-checkpoint-periodicity, and vice-versa, is not supported.

Command Changes

timeout idle

Enables configuration of periodic idle seconds micro checkpoint timer on a per-subscriber basis.

configure
  context context_name
  subscriber subscriber_name
  timeout idle idle_dur \[ micro-checkpoint-deemed-idle \[ time_in_seconds \] \]
  micro-checkpoint-periodicity time_in_seconds \[ \{ default | no \} \]
end

Notes:

• micro-checkpoint-deemed-idle: Number of seconds, and must be an integer value in the range from 10 through 1000. Default is 180.

Important micro-checkpoint-deemed-idle value should be less than idle timeout value.

• micro-checkpoint-periodicity: Number of seconds, and must be an integer value in the range from 10 through 10000. Default is 10.

Important micro-checkpoint-periodicity value should be less than idle timeout value.

• default | no: Indicates the timeout specified to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

Performance Indicator Changes

show subscribers configuration username

The show subscribers configuration username user_name command has been modified to display "micro-checkpoint-deemed-idle" and "micro-checkpoint-periodicity" in the output.

For example:
idle seconds deemed
idle checkpoint periodicity : n/a
idle seconds micro
checkpoint periodicity : 30

**show configuration**

The **show configuration** command has been modified to display "micro-checkpoint-deemed-idle" and "micro-checkpoint-periodicity" in the output.

For example:
micro-checkpoint-periodicity 60

**show configuration verbose**

The **show configuration verbose** command has been modified to display "micro-checkpoint-deemed-idle" and "micro-checkpoint-periodicity" in the output.

For example:
micro-checkpoint-periodicity 10
Subscriber Level Support for Periodical and Event Based Idle Microcheck Point
CHAPTER

HeNBGW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 19 software releases.

- HeNBGW Enhancements for 19.2, page 131
- HeNBGW Enhancements for 19.0, page 135

HeNBGW Enhancements for 19.2

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 19 software releases.

This section identifies all of the HNBGW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HNBGW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HNBGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
SCTP stats based on henb or lenb association peerid are incorrect.

CSCuo19206 - HENBGW:SCTP stats based on henb or lenb association peerid are incorrect.

**Feature Changes**

SCTP stats display per peer_id has changed both for the accesss-service and network-service.

**Previous Behavior:** SCTP Stats were not captured as per the peer_id given in the "show" CLI. It was displaying overall SCTP Stats for an henbgw-access-service and henbgw-network-service.

**New Behavior:** SCTP Stats are collected per peer id and display is changed according to the SCTP Stats received per peer from the SCTP Stack.

**Customer Impact:** Customer will be able to see correct SCTP Stats for a particular peer.

Multiple HENBGW Access Services

CSCuu80088 - Multiple HeNBGW Access Services.

**Feature Changes**

CLI outputs and Statistics

**Previous Behavior:** Single HeNBGW access service supported.

**New Behavior:** Upto 16 multiple HeNBGW access services supported.

**Customer Impact:** Feature addition.

Obsoleting Existing DSCP Marking CLI

CSCuv07438 - Obsoleting existing DSCP marking CLI.

**Feature Changes**

CLI is obsoleted.

**Previous Behavior:** DSCP marking was configurable on HeNBGW. HeNBGW changes the IP / control packets DSCP marking based on the configuration.

**New Behavior:** DSCP marking will be in pass through mode.
Customer Impact: Existing DSCP configuration on HeNBGW will not work but there won’t be any failure if even the customer loads the build with old configuration.

CLI Configuration for QCI to DSCP Mapping Table

CSCuv26542 - CLI config for QCI to DSCP mapping table.

Command Changes

```plaintext
henbgw qci-dscp-mapping-table

Below new command `henbgw qci-dscp-mapping-table` is added as part of this release:

```
configure
lte-policy
[ no ] henbgw qci-dscp-mapping-table `table_name`
end
```

Important: This command on execution will open a new mode HeNBGW QCI DSCP Mapping Table mode.

```plaintext
dscp-marking-default

Below new command `dscp-marking-default` is added as part of this release:

```
configure
lte-policy

henbgw qci-dscp-mapping-table `table_name`
dscp-marking-default { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
end
```

```plaintext
qci

Below new command `qci` is added as part of this release:

```
configure
lte-policy

henbgw qci-dscp-mapping-table `table_name`
qci `qci_value` dscp-marking { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
end
```
```

Multiple Access service

CSCuv34994 - Multiple Access service.
Feature Changes

Deprecation of mme-id, mme-code and plmn id part of henbgw-access-service configuration

**Previous Behavior:** The mme-id sends GUMMEI in case of s1 setup response and plmn id validates against every s1 setup.

**New Behavior:** The S1 setup is validated against the TAI list db instead of PLMN id and the S1 Setup response consists the GUMMEI of the MME's serving the PLMN for which S1 setup request is received.

**Customer Impact:** Removal of configurations as part of henbgw-access-service.

"Enb Config Update Failure" msg is not handled in Henbgw

CSCuv47581 - "Enb Config Update Failure" msg is not handled in Henbgw.

Feature Changes

**Previous Behavior:** On recieving Enb configuration update fail from MME with TTW IE, enb configuration update will not be retried from henbgw-network.

**New Behavior:** On recieving Enb configuration update fail from MME with TTW IE, enb configuration update will be retried from henbgw-network for s1ap-max-retransmission count value. Default value is 4.

HeNBGW sends Reset Message to MME when access service goes down

CSCuv90876 - Henbgwmgr sends Reset Message to MME.

Feature Changes

**Previous Behavior:** S1AP Full Reset sent to MME(s) when access service goes down

**New Behavior:** No S1AP Full Reset procedure initiated towards MME(s) when access service goes down.

Multi Access SVC With QoS Support

CSCuw21614 - Multi Access SVC retaining QCI during X2 handover.

Feature Changes

HeNBGW retains QCI during X2HO between F2F without SGW Relocation.

**Previous Behavior:** No QCI information was retained during X2HO between F2F with SGW Relocation.

**New Behavior:** HeNBGW support retaining QCI during X2HO between F2F with or without SGW relocation. Following are the limitations:

- X2 handover will fail with overlapping MME UE S1AP IDs.
• No support for M2F X2 handover.

Customer Impact: M2F X2 handover is not supported.

### HeNBGW Enhancements for 19.0

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 19 software releases.

This section identifies all of the HNBGW enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *HNBGW Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HNBGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

### Increase in Number of LeNBs Towards MME

CSCuV75780 - US2334 HeNBGW: Num of LeNB needs to increased to 64 from 8

**Feature Changes**

- **Previous Behavior:** Only 8 LeNBs were supported towards MME.
- **New Behavior:** Now total 64 LeNBs will be supported towards MME.
Customer Impact: Customer can now support handovers to 64 LeNBs without using TAI based approach.

X2 Handover With S1u Support

CSCuv30623 - HeNBG expects E-RAB To Be Switched in Uplink List in Path Switch Ack

Feature Changes

X2 handover with S1u enabled.

Previous Behavior: No X2 handover support without SGW relocation.

New Behavior: HeNBGW starts supporting X2 handover with/without SGW relocation with S1u Enabled. Following are the limitations:

1. X2 handover will fail with overlapping MME UE S1AP IDs.
2. No support for M2F X2 handover.

No change in the behaviour of X2 handover with S1u disabled. It continues to behave the same as older versions.

Customer Impact: X2 handover with S1u Enabled in HeNBGW.
CHAPTER

HNBGW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from HNBGW in StarOS 19 software releases.

- HNBGW Enhancements for 19.4, page 137
- HNBGW Enhancements for 19.2, page 139
- HNBGW Enhancements for 19.0, page 140

HNBGW Enhancements for 19.4

This section identifies all of the HNBGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the HNBGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your HNBGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
Encode Calling Party Address in SCCP Message

CSCuy36163 - SCCP Connection Refused

Feature Changes

**Previous Behavior:** In earlier releases, when HNB-GW forwards an empty calling party address in the SCCP Connection Request message to third-party vendor's MSS, it results in SCCP Connection Refused messages.

**New Behavior:** With this release, a new CLI is introduced under the HNB-CS and HNB-PS Network Configuration Modes to enable or disable the inclusion of the calling party address in the outgoing SCCP Connection Request message.

Command Changes

**sccp (HNB-CS Network Configuration Mode)**

With this release, the `sccp calling-party-address` command is introduced under the HNB-CS Network Configuration Mode to enable HNB-GW to include the optional calling party address in the outgoing Signaling Connection Control Part (SCCP) Connection Request (CR) message on the circuit switched network.

```
configure
cs-network cs_instance
    | default | no | sccp calling-party-address
end
```

**Notes:**

- Use the `default` keyword to restore the configuration to its default setting.
- If previously enabled, use the `no` keyword to remove the configuration and restore to the default setting.
- By default, the calling party address is not included in the outgoing SCCP CR messages.

**sccp (HNB-PS Network Configuration Mode)**

With this release, the `sccp calling-party-address` command is introduced under the HNB-PS Network Configuration Mode to enable HNB-GW to include the optional calling party address in the outgoing Signaling Connection Control Part (SCCP) Connection Request (CR) message on the packet switched network.

```
configure
ps-network ps_instance
    | default | no | sccp calling-party-address
end
```

**Notes:**
• Use the `default` keyword to restore the configuration to its default setting.
• If previously enabled, use the `no` keyword to remove the configuration and restore to the default setting.
• By default, the calling party address is not included in the outgoing SCCP CR message.

Performance Indicator Changes

`show cs-network`

The "Include SCCP calling party address" field is added to the output of the `show cs-network all` and `show cs-network name cs_network_name` commands to indicate if the configuration to include the calling party address in the outgoing SCCP CR message is enabled or disabled.

`show ps-network`

The "Include SCCP calling party address" field is added to the output of the `show ps-network all` and `show ps-network name ps_network_name` command to indicate if the configuration to include the calling party address in the outgoing SCCP CR message is enabled or disabled.

`show configuration`

When the `sccp calling-party-address` command is enabled under the HNB-CS and/or HNB-PS Network Configuration Modes, the output of the `show configuration` and `show configuration verbose` commands will display the "sccp calling-party-address" configuration information under the HNB-CS and/or HNB-PS Network Configuration Mode sections.

HNBGW Enhancements for 19.2

This section identifies all of the HNBGW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HNBGW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HNBGW.

• AAA Enhancements
• CF Enhancements
• ECS Enhancements
• Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
• MVG Enhancements
• NAT Enhancements
• SNMP MIB Enhancements
• System and Platform Enhancements

Handin with FAP aggregator

CSCuv56186 - M2F-HANDIN-SN-CFG-CLI

Command Changes

hnbgw-aggregation

New option **handin-with-aggregator** is added to HNB-GW Service Configuration mode command **hnbgw-aggregation** as part of this release:

```
configure
  context context_name
  hnbgw-service service_name
[ no | default | hnbgw-aggregation handin-with-aggregator [ -noconfirm ]
end
```

HNBGW Enhancements for 19.0

This section identifies all of the HNBGW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HNBGW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HNBGW.

• AAA Enhancements
• CF Enhancements
VPC-DI support for HNBGW

CSCut97596 - HNBGW support for VPC DI

Feature Changes

Optimization to support HNBGW service on VPC-DI platform.

Previous Behavior: VPC DI supported.

New Behavior: Once session colocation is enabled, IU and HNB sessions will be on same session manager.

Command Changes

session-collocation

New command session-collocation is added to HNB-GW Service Configuration mode command as part of this release:

```
configure
  context context_name
    hnbgw-global service_name
    [ no | default ] session-collocation { both | iucs | iups }
end
```

Issues Setting or Resetting the Show Subscriber All Command

CSCuu68952 - [16.1.8] TIME-IDLE in "show sub all" not set/reset correctly

Feature Changes

Previous Behavior: TIME_IDLE field displayed in "show sub all" was not being reset in case of any activity by the session.

New Behavior: IDLE-TIME will be accurate now in case of any uplink activity for the session.
IPSEC Session Connection

CSCuv54482 - Multiple FAPs unable to connect due to duplicate address error

Feature Changes

IPSEC session is cleared if idle for long time.

Previous Behavior: IPSec session stays in boxertill external trigger happens.

New Behavior: New CLI is added to configure a timer, on expiry of the timer idle IPSec session will be cleared in sessmgr.

Command Changes

`ipsec connection-timeout`

Below command is added to HNB-GW Service Configuration mode as part of this release:

```
configure
  context context_name
    hnbgw-service service_name
    { default | no } ipsec connection-timeout ipsec_connection_timeout
end
```

Performance Indicator Changes

Show hnbgw-service

The output of this command has been enhanced to provide additional details on IPSEC Connection Timeout settings:

• IPSEC Connection Timeout
HSGW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from HSGW in StarOS 19 software releases.

- HSGW Enhancements for 19.1, page 143
- HSGW Enhancements for 19.0, page 144

HSGW Enhancements for 19.1

This section identifies all of the HSGW enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *HSGW Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HSGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
**Updated Value Sent for 3GPP2-BSID AVP after ULI-CHANGE Event**

CSCuv85413 - WxGW: Invalid 3GPP2-BSID is sent in STOP record after interhsgw handoff

**Feature Changes**

- **Important**
  - This is a customer-specific enhancement. For more information, contact your Cisco account representative.

  **Previous Behavior:** 3GPP2-BSID AVP value in INTERIM/STOP message for eHRPD call is same throughout the call even though ULI_CHANGE occurs in between.

  **New Behavior:** 3GPP2-BSID AVP value in INTERIM/STOP message for eHRPD call is sent with latest/updated value after ULI_CHANGE event.

**HSGW Enhancements for 19.0**

This section identifies all of the HSGW enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *HSGW Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

**Important**

- This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your HSGW.

  - **AAA Enhancements**
  - **CF Enhancements**
  - **ECS Enhancements**
  - **Firewall Enhancements**
  - **GTPP Enhancements**
  - **Lawful Intercept Enhancements**
  - **MVG Enhancements**
PMIP Part of Maintain Session Uniqueness

CSCut99086 - HSGW: PMIP part of Maintain Session Uniqueness

Feature Changes

When the HSGW reselects a PGW (or a different PGW) during timeout scenarios, the old PDN connection request might still be processed in the network, and the session created by the new PDN connection request is overwritten by the stale procedure. To resolve this issue, TimeStamp and MWT (MaxWaitTime) IE have been incorporated to be transmitted from the PGW on S6b, Gx and Gy interfaces.

A timestamp value is sent by the HSGW in a Proxy Binding Update message to the PGW which in turn forwards it to the Diameter interface. The maximum wait time is calculated by the PGW, and not forwarded by the HSGW.

Both timestamp and MWT are sent for the initial Diameter messages only.

Command Changes

message-timestamp-drift

This new command allows drift time configuration to take care of NTP drift issues.

```
configure
case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

case

casedebug

casedebug

casedebug
Performance Indicator Changes

LMA Schema

The following new counters have been added to show the total number of binding update deny messages due to newer sessions detected:

- bindupd-denynewsessaaa
- bindupd-denynewsesspcrf
- bindupd-denynewsesspcs

show lma-service statistics

The following new fields have been added to show the number of PBA failures due to newer sessions detected:

- Update Denied - Unspecified Reason
  - Newer Session detected by AAA
  - Newer Session detected by PCRF
  - Newer Session detected by PCS

RTT Support Expanded to Include PIMPv6 (S2a)

CSCut82602 - RTT support to be expanded to include PMIPv6 (S2a)

Feature Changes

Previous Behavior: For eHRPD, RTT messages were not generated even if configuration was enabled.

New Behavior: For eHRPD, RTT messages are generated if configuration is enabled.

Performance Indicator Changes

System Schema

The following counters have been added for RTT messages:

- sess-pgw-total-pmipv6-event-records
- sess-pgw-total-pba-event-records
- sess-pgw-total-bra-event-records
show event-record statistics pgw

The following new fields have been added for RTT messages:

- PMIPv6 Event Records
- PBU-PBA
- BRI-BRA/Timeouts

Static P-GW Selection for IMS APN on HSGW

CSCuu36494 - Static PGW Selection for IMS APN on HSGW

Feature Changes

With this feature, DNS resolution is triggered simultaneously for both the primary and secondary P-GW FQDN. Therefore, it is possible for both DNS resolutions to be successful. The focus is on the primary FQDN. However in the case of primary FQDN resolution failure, P-GW selection happens based on the secondary FQDN.

Important
Use of Static P-GW Selection for IMS APN on HSGW requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Command Changes

Important
This new CLI command requires a valid HSGW license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

pgw fqdn

A new command has been added to the HSGW CLI to configure both the primary and the secondary FQDN string in the configuration.

```plaintext
configure
  context  context_name
  apn  apn_name
    pgw fqdn primary  primary_fqdn_name secondary  secondary_fqdn_name
{ default | no } pgw fqdn
end
```

Notes:

- **pgw fqdn**: Configures the static FQDN string for the HSGW to select the P-GW.
- **primary**: Configures the primary static FQDN string for the HSGW to select the P-GW.
Secondary: Configures the secondary static FQDN string. The primary FQDN will be tried before trying the secondary FQDN.

default: Returns the command to default setting of pgw fqdn.

no: Disables the pgw fqdn command if it was previously enabled.

Important

If the above CLI command is not configured then the HSGW uses DNS to select the serving P-GW. The HSGW receives a list of all the P-GWs that serve the given APN. Then, the HSGW compares a list of P-GWs with the locally configured FQDN and selects the best matching P-GW.

Performance Indicator Changes

APN Schema

The following counters are newly added to the output of this show command to support static P-GW Selection for IMS APN on HSGW:

- primary-fqdn-dns-att
- secondary-fqdn-dns-att
- primary-fqdn-dns-fail
- secondary-fqdn-dns-fail
- primary-fqdn-dns-success
- secondary-fqdn-dns-success
- pbu-sent-to-primary-fqdn-timeout
- pbu-sent-to-secondary-fqdn-timeout

show apn statistics

New counters have been added to the output generated by this command:

HSGW Static FQDN Statistics:
Primary FQDN Select Attempt: 0 Primary FQDN DNS Success: 0
PBU sent to primary FQDN timeout: 0 Primary FQDN DNS Failure 0
Secondary FQDN Select Attempt: 0 Secondary FQDN DNS Success: 0
PBU sent to secondary FQDN timeout: 0 Secondary FQDN DNS Failure 0

show apn statistics all hsgw-only

The following fields have been added to the output of this command as part of this feature.
These new fields require a valid HSGW license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Important**

APNs without static PGW FQDN configuration will not be displayed under this output.

```
show apn statistics hsgw-only

The following fields are added to the output of this command as part of this feature.
```

**Important**

These new fields require a valid HSGW license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Important**

APNs without static PGW FQDN configuration will not be displayed under this output.
Static P-GW Selection for IMS APN on HSGW
CHAPTER 11

IPSec Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from IPSec in StarOS 19 software releases.

- IPSec Enhancements for 19.6, page 151

IPSec Enhancements for 19.6

This section identifies all of the IPSec enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the SaMOG Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SaMOG.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
• SNMP MIB Enhancements
• System and Platform Enhancements

Certificate and Private Key Storage

CSCvb38168 - [ePDG] save config and reload with large cert does not work

**Applicable Products:** All products that support IPSec

**Feature Changes**

**Old Behavior:** In earlier releases, when a configuration is saved, any configured certificate and private keys are saved as data. When the saved configuration is reloaded, the configuration might not load completely when private keys are larger than 8192 characters due to a CLI limitation. This results in the crypto template not loading completely due to incomplete certificate and private key.

**New Behavior:** With this release, certificates (configured using a URL) and private keys are stored as a file in a private directory locally to avoid the CLI limitation outlined above. The output of the `show config` command will display the local URL of the certificate (only if the bootup configuration is URL) and private key instead of the data. When the certificate is removed using the `no certificate certificate_name` command, the certificate and private key from the local private directory are removed.
IPSG Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from IPSG in StarOS 19 software releases.

- IPSG Enhancements for 19.2, page 153

IPSG Enhancements for 19.2

This section identifies all of the IPSG enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *IPSG Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your IPSG.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
**IPSG vPC-DI Qualification**

CSCuw10079 - IPSG Qualification on VPC-DI

**Feature Changes**

With this release, the IP Services Gateway has been fully qualified to run on Cisco's virtual Packet Core (vPC)-Distributed Instance (DI) platform. In vPC-DI, multiple virtual machines (VMs) act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management.
L-ESS Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from L-ESS in StarOS 19 software releases.

• L-ESS Enhancements for 19.0, page 155

L-ESS Enhancements for 19.0

This section identifies all of the L-ESS enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the ESS Reference Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Configuring L-ESS Application To Be Monitored Based On PSMON Process

CSCuv66725 - VCS configuration to avoid concurrency violation using MonitorProcess

Feature Changes

In this release, support and procedure is provided for VCS to be monitored based on PSMON process instead of PID files.

Refer to the ESS Administration and Reference Guide for information on system recommendations, environment setup, and installation procedures.

L-ESS Support in Virtual Environment

CSCuq08378 - LESS should run on Virtualized Environment (VMWare / KVM as hypervisors)
Feature Changes

In this release, support and procedure is provided for L-ESS deployment in a virtual environment using KVM or VMware as hypervisors. L-ESS can be deployed in stand-alone mode or in cluster mode on KVM or VMware.

Refer to the ESS Administration and Reference Guide for information on system recommendations, environment setup, and installation procedures.
MME Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from the MME in StarOS 19 software releases.

- MME Enhancements for 19.6, page 157
- MME Enhancements for 19.5, page 159
- MME Enhancements for 19.4, page 170
- MME Enhancements for 19.3, page 187
- MME Enhancements for 19.2, page 192
- MME Enhancements for 19.0, page 216

MME Enhancements for 19.6

This section identifies all of the MME enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your MME.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
Handling of LCS Message in Idle State of UE

CSCvb76399 - LCS CONNECTION ORIENTED INFORMATION TRANSFER message is not handled properly in IDLE state

Feature Changes

MME suspends Location Services (LCS) procedure and starts paging procedure if EPS Mobility Management (EMM) is not in CONNECTED/CONNECTING state instead of aborting it immediately.

**Previous Behavior:** MME aborts LCS procedure when CONNECTION ORIENTED INFORMATION TRANSFER is received from Evolved Serving Mobile Location Centre (eSMLC) if UE is in IDLE state.

**New Behavior:** MME pages UE to send LPPA message in downlink NAS when CONNECTION ORIENTED INFORMATION TRANSFER is received from eSMLC if UE is in IDLE state.

Modified LCS Procedure Handling

CSCvc43494 - LCS Procedure Not Resumed When Connection Oriented Info transfer Comes With LPPa (1)

Feature Changes

**Previous Behavior:** MME handles the LCS procedure with ESMLC partially. Consider the scenario where the UE is in connecting mode that is, IM-EXIT is in progress after successful paging. The "DOWNLINK UE ASSOCIATED LPPA TRANSPORT" sent by the MME gets dropped in the S1AP stack as this message cannot be sent when IM-EXIT is in progress. The stack drops the LCS PDU and does not proceed with the IM-EXIT procedure. On paging failure LCS procedure is not getting aborted immediately instead it is waiting till guard-timer expiry. Also, the LCS procedure is not getting suspended when "Connection Oriented Message" is received from ESMLC while IM-EXIT is in progress.

**New Behavior:** MME handling of the LCS procedure with ESMLC is modified after the UE moves to connected state. The MME now suspends the LCS procedure and resumes it after a successful IM-EXIT procedure and then initiates a "DOWNLINK UE ASSOCIATED LPPA TRANSPORT" towards the UE. In case of a paging failure, the LCS procedure gets aborted immediately and does not wait for the guard timeout to expire.
MME Enhancements for 19.5

This section identifies all of the MME enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your MME.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**Configurable Cause Codes Based on ODB Condition**

CSCuz71936 - Invalid reject cause in Attach Reject due to ESM PDN Connectivity Reject

**Feature Changes**

*Previous Behavior*: In releases prior to 17.5, the EMM cause code #19 (ESM failure) and ESM cause as #8 are sent in the Attach Reject when the subscriber does not have an LTE/EPS subscription.

In 17.5, 18.x, 19.x (19.0 to 19.4) and 20.x releases, the EMM cause code #15 (No suitable cells in tracking area) and ESM cause as #31 are sent in the Attach Reject when the subscriber does not have an LTE/EPS subscription. The significant change is the change of EMM cause code as the ESM cause can be anything as long as the EMM cause code is not #19.

*New Behavior*: In releases 19.5, 21.0 and beyond, the behavior of MME is modified to accustom to the needs of all customers. New configurable options `odb packet-services emm-cause-code` and `odb roamer-to-vplmn`
**Command Changes**

**local-cause-code-mapping**

Two new keywords `odb packet-services emm-cause-code` and `odb roamer-to-vplmn emm-cause-code` are introduced as part of `local-cause-code-mapping` CLI command in the Call Control Profile configuration mode. This keyword enables to include the configured EMM and ESM cause codes when ODB condition is hit.

```plaintext
call-control-profile profile_name
  local-cause-code-mapping odb packet-services emm-cause-code cc_value [ esm-cause-code cc_value ]
  local-cause-code-mapping odb roamer-to-vplmn emm-cause-code cc_value [ esm-cause-code cc_value ]
end
```

Notes:

- `odb packet-services emm-cause-code cc_value`: Specifies the EMM cause code for ODB all packet services. The EMM cause code value is an integer from 0 to 255.
- `odb roamer-to-vplmn emm-cause-code cc_value`: Specifies the EMM cause code for ODB roamer to visited PLMN. The EMM cause code value is an integer from 0 to 255.
- `esm-cause-code cc_value`: This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.
- Use the `remove local-cause-code-mapping odb packet-services` CLI command to remove the configured cause code mapping.

**local-cause-code-mapping**

Two new keywords `odb packet-services emm-cause-code` and `odb roamer-to-vplmn emm-cause-code` are introduced as part of `local-cause-code-mapping` CLI command in the MME Service configuration mode. This keyword enables to include the configured EMM and ESM cause codes when ODB condition is hit.

```plaintext
mme-service service_name
  local-cause-code-mapping odb packet-services emm-cause-code cc_value [ esm-cause-code cc_value ]
  local-cause-code-mapping odb roamer-to-vplmn emm-cause-code cc_value [ esm-cause-code cc_value ]
end
```

Notes:

- `odb packet-services emm-cause-code cc_value`: Specifies the EMM cause code for ODB all packet services. The EMM cause code value is an integer from 0 to 255.
By default, the MME sends the UE the EMM cause code #15 - NO_SUITABLE_CELL_IN_TRACKING_AREA for this condition.

- `odb roamer-to-vplmn emm-cause-code cc_value`: Specifies the EMM cause code for ODB roamer to visited PLMN. The EMM cause code value is an integer from 0 to 255.
- `esm-cause-code cc_value`: This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Enhancements to APN Remapping

CSCva45395 - Support for APN remapping of non-3gpp apn and other enhancement

**Feature Description**

MME sends remapped APN to the UE in the ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ messages when APN Remapping feature is enabled. In this release, this behavior is modified so that MME can control to send either the UE requested APN or remapped APN in these messages. This behavior is controlled through adding a new optional keyword `orig-apn` in the existing apn-remap CLI command in the APN Remap Table configuration mode.

Additional configuration control is provided at the MME service level to reject or accept UE sessions with APN containing non-3GPP standard characters. The following are considered as standard 3GPP characters:

- A - Z, a - z (alphabets)
- 0 – 9 (numeric)
- - (hyphen)
- * (asterisk)
- . (period)

All other characters are considered as non-3GPP standard.

New CLI configuration is also introduced in the APN Remap Table configuration mode to allow remapping of APNs with non-3GPP characters.

**Configuring APN Override**

Configuration for all of the functions of the APN Override feature is accomplished in the APN Remap Table configuration mode of the Operator Policy Feature. In order to enable apn-overflowing, an apn-remap-table must be configured and associated to the mme-service through the operator-policy.

**Enabling MME to Send UE Requested APN**

Use the following configuration commands to configure MME to send the UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message.

```
configure
apn-remap-table table_name
    apn-remap network-identifier company.com new-ni internet.com [ orig-apn ]
```
cc behavior 0xff profile 10 apn-remap network-identifier company.com new-ni internet.com [ orig-apn ]
apn-selection-default lowest-context-id [ orig-apn ]
apn-selection-default first-in-subscription [ orig-apn ]
apn-selection-default network-identifier require-dns-fail-wildcard [ orig-apn ]
end

Notes:

• **orig-apn**: This is an optional keyword newly added to the existing CLI commands to enable MME to send UE requested APN to the UE. If this optional keyword is not configured, then MME continues with its default behavior of sending the remapped APN to the UE.

• For more information on the existing CLI commands, see the *Command Line Interface Reference* guide.

### Rejecting UE Requested APN with Non-standard Characters

Use the following configuration commands to configure MME to reject UE sessions containing non 3GPP standard characters in the APN.

```plaintext
configure
  context context_name
  mme-service service_name
    [default] policy attach reject-non3gpp-char-apn
    [default] policy pdn-connect reject-non3gpp-char-apn
end
```

Notes:

• **policy attach reject-non3gpp-char-apn**: This command enables MME to immediately reject the attach procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The attach procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the Attach reject message.

• **policy pdn-connect reject-non3gpp-char-apn**: This command enables MME to immediately reject the PDN connect procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The PDN connect procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the PDN connect reject message.

• For more information on the existing CLI commands, see the *Command Line Interface Reference* guide.

### Remapping UE Requested APN with Non-standard Characters

Use the following configuration commands to configure MME to remap UE requested non 3GPP character APN to an operator defined APN.

```plaintext
configure
  apn-remap-table table_name
  apn-remap non3gpp-char-apn new-ni new-ni-name [ orig-apn ]
end
```

Notes:

• **apn-remap non3gpp-char-apn new-ni new-ni-name**: This command enables MME to remap all UE requested APNs containing non 3GPP characters to the configured new-ni APN. If the optional keyword "orig-apn" is configured, then MME sends the UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message. If this keyword is not configured, then remapped APN is sent back to UE.
• This CLI is applied only if the UE sessions are not rejected by the new configuration options policy attach reject-non3gpp-char-apn and policy pdn-connect reject-non3gpp-char-apn under the mme-service.

• If the UE requested APN contains non-3GPP characters and the apn-remap non3gpp-char-apn new-ni new-ni-name CLI command is configured, then this CLI takes precedence over any other matching criterion for APN remapping.

• For more information on the existing CLI commands, see the Command Line Interface Reference guide.

Monitoring and Troubleshooting the APN Override Feature

This section provides information regarding show commands and/or their outputs in support of this feature. The following operations should be performed for any failure related to this feature:

• Verify if the feature is enabled using show configuration and show mme-service all CLI commands. If not enabled, configure the CLI commands mentioned in the Enabling MME to Send UE Requested APN and Rejecting UE Requested APN with Non-standard Characters sections and check if it works.

• Collect the output of show mme-service statistics debug command and analyze the debug statistics "Rejected Attach due to non3gpp char APN" and "Rejected PDN Connect due to non3gpp char APN". For further analysis, contact your Cisco account representative.

show configuration

The output of this show command is enhanced to indicate whether MME sends back UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message.

The following is a sample output of this show command indicating that this feature is enabled.

[local]asr5000# show configuration
config
... ... ...
no session trace network-element saegw
apn-remap-table abc
  apn-remap non3gpp-char-apn new-ni mappedApn orig-apn
  apn-remap network-identifier origApn new-ni mappedApn orig-apn
  #exit
  port bits 24/4
  snmp trap link-status
  ... ... ...
  no heuristic-paging
  no isr-capability
  policy attach set-ue-time disable
  policy attach reject-non3gpp-char-apn
  policy pdn-connect reject-non3gpp-char-apn
  policy tau set-ue-time disable
  ... ... ...
end

show mme-service all

The output of this show command is enhanced to indicate whether MME rejects APNs with non-standard characters in Attach Request or PDN Connect Request message. The following fields are added in support of this feature.
• Reject attach with non-3GPP char APN
• Reject pdn connect with non-3GPP char APN

The following is a sample output of this show command with the new field included.

show mme-service all
Policy for Idle Mode Detach : Explicit
NAS Max Retransmissions Count : 4
Set UE Time (attach processing) : Disabled
Reject attach with non-3GPP char APN : Disabled
Reject pdn connect with non-3GPP char APN : Disabled
IMEI Query (attach processing) : None
EIR Query (attach processing) : Disabled

show mme-service session full { all | imsi | mme-service }

The output of this show command is enhanced to display the name of UE requested APN with non-standard character in hexadecimal format, and with all standard characters in normal string format. The following field is added in support of this feature.

• UE Requested APN

The following is a sample output of this show command with the new field included.

show mme-service session full all
PDN Information:
   APN Name: starent.com
   UE Requested APN: starent-ueside.com
   APN Restriction: 1
   PDN Type: IPv4

---

**Important**
The UE requested APN information will not be available for UE after the session recovery as it will not be checkpointed.

---

**Extended EMM cause IE - E-UTRAN not allowed**

CSCva14791 - MME - CR-1917 - #15 - Extended EMM cause IE "E-UTRAN not allowed"

**Old Behavior:** Earlier, MME did not include Extended EMM Cause IEI in both ATTACH and TAU procedure; they get rejected with EMM Cause #15 under the following scenarios:

• Whenever the HSS subscription has Operator-Determined-Barring enabled.
• Whenever the HSS subscription has Access-Restriction-Data enabled.
• Whenever the operator restricts the EPS attaches locally through the call-control-profile configuration (configuration based).

**New Behavior:** In release 19.5, MME includes Extended EMM Cause IEI (defined in 3GPP TS 24.301 V12.5.0, section 9.9.3.26A (defines the encoding/decoding of Extended EMM cause IEI)) for both Attach and TAU procedure when rejected with EMM Cause #15 under the following scenarios:

• Whenever the HSS subscription has Operator-Determined-Barring enabled.
• Whenever the HSS subscription has Access-Restriction-Data enabled.
Whenever the operator restricts the EPS attaches locally through the call-control-profile configuration (configuration based).

MME Re-try of HSS initiated QoS Modification Procedure

CSCva20423 - Failure in updating QCI after TAU, during 3G to 4G handover

Feature Changes

**Previous Behavior:** The MME does not re-try the QoS modification procedure if the HSS initiated QoS modification fails due to any of the following triggers:

- If S1-UE-CONTEXT-RELEASE is received when the Update Bearer procedure in progress.
- If there is an E-RAB modify failure.

**New Behavior:** New CLI keywords "pdn-modify retry-qos-modify" are introduced in the policy command under the MME Service Configuration mode, the user can either enable or disable the retry for QoS modification procedure in the next IDLE to ACTIVE transitions if the previous HSS initiated modification failed due to the following triggers:

- If S1-UE-CONTEXT-RELEASE is received when the Update Bearer procedure in progress.
- If there is an E-RAB modify failure.

If this configuration is enabled, the MME sends the Update-Bearer-Response with cause "EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS" for the first time when the HSS initiated modification fails due to either no response for ERAB-MODIFY from eNodeB or ERAB modify failure and moves the UE to IDLE state.

The basic assumption is that the PGW will retry the Update-Bearer-Request due to the cause sent by the MME in Update-Bearer-Response, this results in PAGING towards the UE and the UE triggers an IM-EXIT procedure. As part of IM-EXIT procedure, the updated QoS values are sent in the INITIAL-CONTEXT-SETUP message towards eNodeB and "MODIFY-EPS-BEARER-CONTEXT-REQUEST" in Downlink NAS message towards UE. This planned retry procedure is performed once after the HSS initiated QoS modification procedure fails due to any of the triggers mentioned above. The MME does not perform the re-try when the UBR gets rejected either partially or a negative response is received from the UE (for example, EGTP Cause - UE REFUSES), validation failures (for example, EGTP Cause - MANDATORY IE INORRECT, MANDATORY IE MISSING, CONTEXT NOT FOUND) and other successful scenarios.

Command Changes

**policy pdn-modify**
Configures policy for PDN modification procedures.

configure
context context_name
mme-service service_name
[no] policy pdn-modify retry-qos-modify
end

- The keyword no removes the existing configuration on the re-try of the Modify Bearer Command.
- The keyword pdn-modify specifies that the policy applies to the PDN modification procedure.
• Use the keyword **retry-qos-modify** to configure the retry of failed HSS initiated QoS modification procedure in next IDLE to ACTIVE transition.

Use this command to either enable or disable the retry for QoS modification procedure in the next IDLE to ACTIVE transitions if the previous HSS initiated modification failed due to the following triggers:

• If S1-UE-CONTEXT-RELEASE is received when the Update Bearer procedure in progress.

• If there is an E-RAB modify failure.

If this configuration is enabled, the MME sends the Update-Bearer-Response with cause "EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANOVER_IN_PROGRESS" for the first time when the HSS initiated modification fails due to either no response for ERAB-MODIFY from eNodeB or ERAB modify failure and moves the UE to IDLE state.

The basic assumption is that the PGW will retry the Update-Bearer-Request due to the cause sent by the MME in Update-Bearer-Response, this results in PAGING towards the UE and the UE triggers an IM-EXIT procedure. As part of IM-EXIT procedure, the updated QoS values are sent in the INITIAL-CONTEXT-SETUP message towards eNodeB and "MODIFY-EPS-BEARER-CONTEXT-REQUEST" in Downlink NAS message towards UE. This planned retry procedure is performed once after the HSS initiated QoS modification procedure fails due to any of the triggers mentioned above. The MME does not perform the re-try when the UBR gets rejected either partially or a negative response is received from the UE (for example, EGTP Cause - UE REFUSES), validation failures (for example, EGTP Cause - MANDATORY IE INCORRECT, MANDATORY IE MISSING, CONTEXT NOT FOUND) and other successful scenarios.

**MME Allows PDN-CONNECTIVITY-REQUEST with PDN-Type IPv4v6**

CSCva19951 - MME should allow conditional ipv4v6 PDN type overwrite when ipv4 + v6

**Feature Changes**

**Previous Behavior:** The MME rejects the PDN-CONNECTIVITY-REQUEST with the ESM cause "SINGLE ADDRESS BEARERS ONLY ALLOWED(0x34)" when the UE requested PDN-Type is "IPv4v6" and the subscription has supported PDN-Type of "IPv4-OR-IPv6" for the requested APN.

**New Behavior:** The MME allows the PDN-CONNECTIVITY-REQUEST with PDN-Type as "IPv4v6" and the subscription has support for the PDN-Type as "IPv4 or IPv6".

The HSS stores one PDN type per APN in the subscription data. During the Attach or UE requested PDN connectivity procedure the MME compares the requested PDN type to the PDN type in the subscription records for the given APN and sets the PDN type as follows:

• If the PDN-Type override configuration is enabled to use either IPv4 or IPv6 for the UE requested PDN-Type "IPv4v6" and Attach Accept carries the ESM cause as either "IPv4 only allowed" or "IPv6 only allowed".

• If the PDN-Type override configuration is not configured the default PDN-Type "IPv4" is used for the UE requested PDN-Type "IPv4v6" and Attach Accept carries the ESM cause as "SINGLE ADDRESS BEARERS ONLY ALLOWED(0x34)". This is to inform the UE to use the alternate PDN-Type in the next PDN creation for the same APN.

This enhancement is in compliance with 3GPP 23.401 version 11.8.0 Release 11, Section 5.3.1.1.
New Configurable Result Codes for Mapping to EMM Cause Code

CSCva07190 - "s6a diameter_result_code" not compliant with TS 29.272

Feature Changes

New CLI options are provided for mapping Diameter cause codes (3003 and 3002) to EMM-NAS-Cause code 15. If the mapping is not configured, then the default emm-cause-code #15 "No suitable cells in tracking area" will be sent as per the 3GPP standard TS 29.272 specification.

Previous Behavior: MME used to send the cause as Network-Failure when Diameter Result-Code 3002 or 3003 is received from HSS.

New Behavior: In S6a message (AIA/ULA), if the Result-Code is returned as 3002 (diameter-unable-to-deliver) or 3003 (diameter-realm-not-served), then MME returns EMM cause as #15 "No suitable cells in tracking area" in NAS message. For other non-3GPP Result-Codes, the previous behavior of sending Network-Failure is continued. CLI mapping is provided to override the EMM cause code.

Command Changes

diameter-result-code-mapping

The following configuration allows the operator to map the Diameter result codes "diameter-unable-to-deliver (3002)" and "diameter-realm-not-served (3002)" to the configured NAS EMM cause codes.

configure
call-control-profile profile_name
diameter-result-code-mapping s6a diameter-realm-not-served mme-emm-cause mme-emm-cause-code
diameter-result-code-mapping s6a diameter-unable-to-deliver mme-emm-cause mme-emm-cause-code
end

Notes:

• If the new mapping option is configured, then this local configuration is given higher precedence.

• Use the remove diameter-result-code-mapping s6a { diameter-realm-not-served | diameter-unable-to-deliver } CLI command to remove the mapping for the specified Diameter result code.

• For information on the other existing Diameter result code mapping options, see the Command Line Interface Reference guide.

S1 NAS Cause Code Mapping

CSCva44545 - Enhancement to have more options under "s1-ue-context-release" command

This feature defines the cause code mapping for S1-NAS cause sent in the S1-UE-CONTEXT-RELEASE for both ATTACH/TAU Rejects with a specific EMM cause code value or any EMM cause code value. S1 NAS Cause Code Mapping is further explained in the following sections:
Feature Description

This feature is enhanced to achieve S1 NAS Cause Code Mapping with a specific EMM cause code or ‘any’ EMM cause code value.

Earlier, the S1 NAS cause code sent in the S1-UE CONTEXT-RELEASE was indicated as "Unspecified" for most of the scenarios during ATTACH/TAU Rejects with a specific or any EMM cause code. The NAS cause "Unspecified" reflects as an error resulting in RAN KPI degradation.

A new CLI configuration is implemented at an MME Service level to achieve a successful cause code mapping during ATTACH and TAU Rejects. The newly configured S1 NAS cause is sent in the MME initiated S1-UE-CONTEXT-RELEASE message after an ATTACH or TAU Reject with the specific EMM cause code or ‘any’ EMM cause code.

Note

The ‘any’ EMM cause code is a new keyword introduced as part of the CLI configuration. This allows the operator to map with any of the available EMM cause code value instead of a specific EMM cause code value.

How It Works

Currently, the operator can configure the cause code mapping of either NAS or Radio Layer cause when MME triggers an S1-UE-CONTEXT-RELEASE upon the reception of any initial UE messages during a valid S1 connection.

A new configuration is implemented to configure S1 NAS cause code mapping from X to Y for both ATTACH and TAU Reject with a specific EMM cause code or any cause code. On implementation of this configuration, the EMM cause code value is pushed to the Session managers to update the S1 NAS cause code mapping configuration locally, which is used to fill the S1 NAS cause in S1-UE-CONTEXT-RELEASE message sent by MME during S1 RELEASE.

The MME continues to use the current default S1 NAS cause code value in the S1-UE-CONTEXT-RELEASE message if the S1 NAS cause code is not configured under the MME Service.

MME uses the newly configured S1 NAS cause code when it finds a cause code mapping entry for the trigger (ATTACH/TAU Reject).

MME uses the newly configured S1 NAS cause code from the mapping entry with the specific EMM cause code when it finds multiple matches with either a specific EMM cause code or any EMM cause code.

Note

The recovery of S1 NAS cause code mapping configuration is already implemented at the MME Service level.

Configuring S1 NAS Cause Code Mapping

This section describes the configuration of S1 NAS cause code mapping for ATTACH/TAU Reject messages. The configuration is done in the MME Service Configuration mode.

This configuration allows the MME to configure the S1 NAS cause code mapping to be sent in S1-UE-CONTEXT-RELEASE initiated from the MME after an ATTACH or TAU is rejected with a specific
EMM cause code or any EMM cause code. The newly configured S1 NAS cause code is sent in the UE-CONTEXT-RELEASE message whenever MME releases the existing SIAP connection with the configured S1 NAS cause after an ATTACH/TAU message gets rejected, along with a specific EMM cause or any EMM cause code based on the configuration.

```plaintext
configure
   context context_name
      mme-service service_name
         [ no ] | s1-ue-context-release reason { attach-reject | tau-reject } emm-cause-code { value specific_emm_value | any } s1-nas-cause cause_value |
   end

Notes:

- The no option removes the cause code mapping entry from the mme-service level configuration.
- The attach-reject keyword specifies the ATTACH reject message sent by the MME.
- The tau-reject keyword specifies TAU reject message sent by MME.
- The emm-cause-code keyword specifies the EMM Cause Code value for which mapping needs to be applied.
- The value keyword specifies the specific EMM Cause Code.
- The any keyword specifies any EMM Cause Code.
- The s1-nas-cause keyword specifies the S1 NAS cause code that needs to be mapped.
- The new-s1-nas-cause keyword specifies the S1 NAS cause code value that needs to be sent in the S1-UE-CONTEXT_RELEASE, which is sent from the MME.

Verifying S1 NAS Cause Code Mapping

The following command displays the S1 NAS configuration on the MME:

```plaintext
show configuration context ingress | more
```

On execution of the above command the following output is displayed:

```
[local]asr5000# show configuration
config
     ... ...
     context ingress
     .... ...
     mme-service mmesvc
     s1-mme actp port 25
     mme-id group-id 32777 mme-code 2
     plmn-id mcc 123 mnc 456
     ... ...
     s1-ue-context-release reason attach-reject emm-cause-code value 15 s1-nas-cause 3
     new-s1-nas-cause 0
     s1-ue-context-release reason attach-reject emm-cause-code any s1-nas-cause 3
     new-s1-nas-cause 0
     s1-ue-context-release reason tau-reject emm-cause-code any s1-nas-cause 3
     new-s1-nas-cause 0
     exit
     ... ...
     ... ...
     end
```
MME Enhancements for 19.4

This section identifies all of the MME enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your MME.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Checking for S5/S8 PGW Data IP Address in Received CSR

CSCuy19662 - Session Manager restarts on failed assert in sn_gt_encode_pdp_context_ie

**Feature Changes**

**Previous Behavior:** In situations where the S5/S8 PGW data IP address is not available in the Create Session Response (CSR) for an Attach Request/PDN Connectivity Request, the MME continues the attach/PDN connectivity procedure.

**New Behavior:** The MME now checks for the S5/S8 PGW data IP address when CSR is received as part of an Attach Request/PDN Connectivity Request, and if the S5/S8 PGW data IP address is not included, then the MME sends Delete Session to the SGW and rejects the Attach Request/PDN Connectivity Request.

**Customer Impact:** Customer should not experience Session Manager crashes later in the call flow as a result of Gn handovers (SRNS or context transfer).
Configurable Deactivation of PDN when CC Changes

CSCux79888 - MME does not update CC in APN Subscription following ISDR
CSCux81813 - pdn-deactivate-cc: 3GTo4G TAU rejected when no CC in cont res and ULA

Feature Changes

Old Behavior:
The MME updates the Charging Characteristics (CC) for an APN in the subscriber DB and keeps the PDN active when the CC information changes in or is absent from the Insert Subscriber Data Request (ISDR).

New Behavior:
Based on new CLI keyword 'pdn-deactivate cc-change' for the policy command in the MME service configuration (new CLI is defined in the Command Changes section below), the MME can be configured to deactivate the PDN when the CC information changes in or is absent from the Insert Subscriber Data Request (ISDR).

With the new configuration:

• Besides deactivating the PDN, the MME updates the subscriber DB with the CC information so that the MME would be able to create a PDN connection with the new CC values.

• If the deactivated PDN is the last PDN, then the UE is detached from the network and during the UE's next Attach procedure the updated CC information is taken from the subscriber DB and included in a Create Session Request.

• If the CC information is absent from the DB, and if CC IE is not present in transferred PDNs of Context Response message during 3G to 4G TAU, then the MME does not send local default CC IE in Create Session Request and the PDN is activated.

Customer Impact:
CC changes can update faster to the PGW.

Command Changes

A new keyword, pdn-deactivate with cc-change filter, allows the operator to configure the MME to deactivate a PDN connection if the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

config
c\ncontext context_name
\n  mme-service service_name
  [ no ] policy pdn-deactivate cc-change
end

Notes:

• For information about existing commands, refer to the Command Line Interface Reference.

• no - This command filter instructs the MME to disable the PDN deactivation configuration defined with this policy command.

• pdn-deactivate - This keyword configures the MME to deactivate the PDN connection based on the AVP included to filter the keyword.
- **cc-change** - This filter represents the charging characteristics AVP. If it is included in the command, then the MME deactivates the PDN connection when the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

**Usage Information:**

- With **pdn-deactivate cc-change** configured, the MME updates the subscriber DB with the CC information so that the MME would be able to create a PDN connection with the new CC values.

- If the deactivated PDN is the last PDN, then the UE is detached from the network and during the UE's nextAttach procedure the updated CC information is taken from the subscriber DB and included in an Update Location Answer and/or a Create Session Request.

- If the CC information is absent from the DB, and if CC IE is not present in transferred PDNs of Context Response message during 3G to 4G TAU, then the MME does not send local default CC IE in Create Session Request and the PDN is activated.

- 'Disabled' is the default behavior. If deactivation for CC changes is not enabled, then the MME updates the APN's CC information in the subscriber DB and keeps the PDN active if the CC information changes in or is absent from the ISDR.

**Verification:**

To confirm the MME's current configuration regarding PDN deactivation, use one of the following show commands.

The following illustrates a small portion of the 'show mme-service' output to indicate the current configuration, which will be either 'enabled' or 'disabled'.

```
show mme-service name service_name
...
Policy S1-Reset : Idle-Mode-Entry
Policy PDN-Deact CC-Change : Enabled
Policy Nas-Non-Del : Disabled
...
```

If PDN deactivation has been configured, then the following partial illustration represents what you would see:

```
show configuration verbose
...
... mme-service mmesvc
   no policy inter-rat indirect-forwarding-tunnels
   no policy inter-rat select-topologic-sgw interface gn
   no policy srvcc purge-timer
   policy pdn-deactivate cc-change
...
```

Please note, if PDN deactivation is not enabled, then there would not be a line for policy pdn-deactivate in the output generated by the 'show configuration verbose' command.

---

**Connection for Responding CLA**

CSCuz22536 - CLR received over one diamproxy is responded to over other diamproxy
Feature Changes

Previous Behavior: The HSS sends the MME a Cancel-Location-Request (CLR) over a diamproxy connection. The MME responds with Cancel-Location-Answer (CLA) sent over the local diamproxy connection where the Session Manager with the subscriber information resides.

New Behavior: Now, the MME responds with CLA on the same diamproxy connection on which the CLR is received.

DDN Option in 'network-overload-protection' Configuration

CSCu68559 - [MME] network-overload-protection mme-new-connections-per-second

Feature Changes

Previous Behavior:
Previously, when configuring 'network-overload-protection mme-new-connections-per-second' as part of the MME's Global Configuration, 'ddn' was a mandatory keyword.

New Behavior:
Now, when configuring 'network-overload-protection mme-new-connections-per-second' as part of the MME's Global Configuration, 'ddn' is an optional keyword. If the 'ddn' option is not configured, then the default action is to drop the Downlink Data Notification (ddn). 'ddn drop' will only be visible in verbose mode.

For details about the 'network-overload-protection mme-new-connections-per-second' command and other associated keywords, refer to the Command Line Interface Reference.

Deactivation of Dedicated GBR Bearers on SCTP Failure

CSCux44173 - MME needs to deactivate GBR Bearers (Dedicated) during eNodeB failure.

Feature Changes

Previous Behavior: In earlier releases, GBR Bearers were not deactivated on SCTP failure.

New Behavior: In release 19.4, the MME is modified to deactivate GBR Bearers (dedicated bearers) on SCTP failure. The deactivation is CLI controlled.

In this new behavior, the deactivation of GBR Bearers can be controlled by the CLI configuration in the following ways:

1. As a default behavior, the dedicated GBR Bearers are deleted and the non-GBR bearers are preserved, when moving the UE to Idle state.
2. An option to configure default system behavior is possible by using `sctp-down idle-mode-entry` command.
3. Dedicated GBR bearers can be retained using `sctp-down idle-mode-entry preserve-gbr-dedicated-bearers` command.
4. The UE can be detached by using `sctp-down detach-ue` command.
5. The new keyword `preserve-gbr-dedicated-bearers` provides backward compatibility, which is the previous behavior.
Command Changes

preserve-gbr-dedicated-bearers

The preserve-gbr-dedicated-bearers is a new keyword that is added to both MME-Service and Call Control Profile configuration modes.

This keyword is used to deactivate dedicated GBR Bearers during an SCTP failure.

Under MME-Service, this keyword is configured as shown below:

```config
context context_name
  mme-service service_name
    policy sctp-down idle-mode-entry preserve-gbr-dedicated-bearers
  end
end
```

Under Call-Control-Profile, this keyword is configured as shown below:

```config
call-control-profile profile_name
  sctp-down idle-mode-entry preserve-gbr-dedicated-bearers
  end
end
```

Performance Indicator Changes

show-mme-service-all

On executing the above command, the following new field is added to the output:

- Policy SCTP-Down

Disabling MSC Fallback on Failure Based on SRVCC Cause

CSCuy44854 - MME wrongly tries to establish call with other MSC during SRVCC failure

Feature Changes

Old Behavior:

If a voice call can be handed over to one of multiple MSC IP addresses during SRVCC handover and if the PS-CS Response from the first MSC returns with a negative cause, then the next MSC is tried.

New Behavior:

If a voice call can be handed over to one of multiple MSC IP addresses during SRVCC handover and if the PS-CS Response from the first MSC returns with a negative cause and that cause has been included in the MME’s Call-Control Profile configuration with the new `msc-fallback-disable` command, then the MME fails the SRVCC HO and does not try the next available MSC.

The new command is explained in the Command Changes section below. If this command is not used to define SRVCC causes, then the MME will use default behavior to select the next MSC to retry PS-CS Request.
Command Changes

A new command, `msc-fallback-disable`, enables the operator to define all SRVCC causes for which the MME does not try sending PS-CS Request to a next available MSC during an SRVCC handover if the MME received one of the configured SRVCC causes in the PS-CS Response from the first MSC.

```plaintext
configure
  call-control-profile profile_name
    | remove | msc-fallback-disable srvcc-cause cause
end
```

Notes:

- For information about existing commands, refer to the Command Line Interface Reference.
- `remove` - This command filter instructs the MME to delete the specified SRVCC cause code definition.
- `srvcc-cause cause` - This keyword configures an SRVCC cause code. If the MME receives this SRVCC cause code in a negative PS-CS Response from the first MSC tried in an SRVCC handover, then the MME sends SRVCC HO Failure and no other MSCs are tried. The `cause` must be any integer from 0 to 255, as defined in 3GPP TS 29.280.
- This command can be repeated to configure more than one SRVCC cause.
- This command is only applicable for PS-CS Requests and not for PS to CS complete messages.
- This command is applicable for both statically configured MSC addresses (in an MSC Pool) and for MSC addresses returned by DNS.
- If this command is not used to define SRVCC causes, then the MME will use default behavior for MSC fallback on failure to select the next MSC to retry PS-CS Request.

Verification:

To confirm the MME’s current configuration of SRVCC causes, use the following show command to generate an output similar to that shown below - three separate cause codes have been configured:

```plaintext
show call-control-profile full name profile_name
...
...
MSC-fallback disabled SRVCC causes : 8 9 10
```

Displaying NPU Flow-related Information for SGs Service

CSCuy45926 - MME to provide debug info for NPU flow add/deletion for SGs interface

Feature Changes

Previous Behavior: Output screens generated by the `show sgs-service vlr-status full` and the `show sgs-service vlr-status vlr-name vlr_name full` commands only displayed Flow ID if the association state was UP.

New Behavior: Now for the SGs Service, Flow ID information display is unlinked from the SCTP association state and is generated if flow is successfully installed.

As well, the outputs generated by the `show sgs-service vlr-status full` and the `show sgs-service vlr-status vlr-name vlr_name full` commands are enhanced to display NPU flow-related information: statistics and status. To avoid information cluttering the show output displays, values will only be displayed if they are non-zero.
The following lists the possible statistics and/or status which can be displayed when values are non-zero:

- NPU Flow created for Primary IPA
- NPU Flow created for Secondary IPA
- Primary IPA flow add requests sent
- Secondary IPA flow add requests sent
- Primary IPA flow add success received
- Secondary IPA flow add success received
- Primary IPA flow add failed
- Secondary IPA flow add failed
- Primary IPA flow alloc failed
- Secondary IPA flow alloc failed
- Primary IPA flow insert failed
- Secondary IPA flow insert failed
- Primary IPA flow delete requests sent
- Secondary IPA flow delete requests sent
- Primary IPA flow delete success
- Secondary IPA flow delete success
- Primary IPA flow delete failed
- Secondary IPA flow delete failed
- Primary IPA flow delete no match
- Secondary IPA flow delete no match
- Primary IPA invalid flowid
- Secondary IPA invalid flowid
- Primary IPA invalid NPU response
- Secondary IPA invalid NPU response
- Max per VLR associations reached
- Invalid NPU response codes
- Primary IPA flow resp code count
- Secondary IPA flow resp code count

Emergency Call Support Irrespective of UE's Advertised Algorithm Support

CSCuz40177 - Task restart due to memory access fault while aborting Attach procedure
**Feature Changes**

**Previous Behavior:** The MME rejects emergency calls if the Attach Request is received with:

- no support indicated for any security or confidentiality algorithms, or
- a mismatch in the algorithms announced by the UE and the algorithm preference configured at the MME (with `ue-validation-level` command under LTE Emergency Profile configuration mode).

**New Behavior:** MME code has been modified to avoid rejecting emergency calls in the above scenario. Now for such a scenario, the MME uses NULL algorithms (EEA0 and EIA0) in response to emergency call Attach Requests even if the UE does not advertise the support of these algorithms.

**Customer Impact:** VoLTE emergency calls are successful for all UEs, no matter the UE's validation level.

---

**Enhanced IMEI-TAC-based Operator Policy Selection**

CSCuz53891 - More granular IMEI-TAC based operator policy selection

**Feature Changes**

**Previous Behavior:**

With Releases 18.6 and higher, the operator is allowed to configure selection of the operator policy based on IMEI-TAC of the UE. Use cases indicate a clear requirement for more granular selection criteria in addition to the IMEI-TAC.

**New Behavior:**

With Release 19.4 and higher, the operator is allowed more granular control of configuration for operator policy selection. Besides operator policy selection based on IMEI-TAC of the UE, the operator can optionally expand selection based on the UE's IMSI and/or MCC-MNC and/or the serving PLMN. The MME uses this configuration to select the operator policy whenever it retrieves the IMEI/IMEI-SV from either a UE or a peer for all non-emergency calls.

**Customer Impact:**

The operator has more granular control of the selection of an operator policy.

**Command Changes**

No new or modified keywords have been added to the `precedence` command. The existing `imsi` and/or `service-plmnid` keywords have been modified with enhanced abilities - they can be selected to include additional granularity into the IMEI-TAC-based operator policy selection.

To setup IMEI-TAC-based operator policy selection, use the `precedence` command in the LTE Subscriber Map configuration mode to:

- set the order of precedence for the subscriber map,
- set which type of matching criteria is to be used to determine which operator policy to select - for this procedure, use the `imei-tac` keyword and identify the previously configured IMEI-TAC group,
- optionally, setup additional IMEI-TAC matching criteria, either singly or in pairs:
  - mcc + mnc
Enhanced IMEI-TAC-based Operator Policy Selection

- imsi
- service-plmnid

- identify the operator policy that deals with subscribers meeting the match criteria.

**Important**
The following example details configuration for IMEI-TAC-based selection and other match-criteria options are not included here. For more details, refer to the Command Line Interface Reference.

```plaintext
configure
lte-policy
subscriber-map map_name
   precedence precedence_number match-criteria imei-tac group group_name | imsi mcc mnc mnc mnc | mnc | mnc | first start-msin-value last end-msin-value } [ ] [ ] | service-plmnid plmnid | operator-policy name policy_name
   no precedence precedence_number
end
```

Notes:

- The precedence level given by the operator is used to resolve the selection of the operator policy when multiple variable combinations match for a particular UE. The lower precedence number takes increased priority during selection.
- As none of the keywords and options for the precedence command are new, we suggest that you refer to the LTE Subscriber MAP Configuration Mode chapter in the Command Line Interface Reference for details about each of the keywords and their possible values.

Usage Options:

- Operator policy selection based on IMEI-TAC only, syntax example:
  ```plaintext
  precedence 1 match-criteria imei-tac-group myGroup operator-policy-name BESTpol
  ```

- Operator policy selection based on IMEI-TAC + Service PLMNID, syntax example:
  ```plaintext
  precedence 1 match-criteria imei-tac-group myGroup service-plmnid 12345
  operator-policy-name policy_name
  ```

- Operator policy selection based on IMEI-TAC + MCC-MNC of UE, syntax example:
  ```plaintext
  precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 operator-policy-name policy_name
  ```

- Operator policy selection based on IMEI-TAC + MCC-MNC of UE + Serving PLMNID, syntax example:
  ```plaintext
  precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 service-plmnid 56789
  operator-policy-name policy_name
  ```

- Operator policy selection based on IMEI-TAC + IMSI, syntax example:
  ```plaintext
  precedence 1 match-criteria imei-tac-group myGroup imsi mnc 123 mnc 234 msn first 1223 last 2333 operator-policy-name policy_name
  ```
• Operator policy selection based on IMEI-TAC + IMSI + Serving PLMNID, syntax example:

precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 msin first 1223 last 2333 service-plmnid 56789 operator-policy-name BESTpol

Handling of CLR on Different Diameter Proxy Connections

CSCuy81279 - MME Rejects Attach/TAU Request w/ EMM Cause: Network failure (17)

Feature Changes

During PDN or TAU attach, a session manager (MME) sends an Update Location Request (ULR) to HSS through a Diameter proxy connection and the HSS immediately sends a Cancel Location Request (CLR) for the same IMSI on a different Diameter proxy connection. This might be because of the old stale sessions existing in the HSS. This is resulting in ATTACH/TAU rejection in MME after the upgrade.

Previous Behavior: If the server initiated messages were received on a different diamproxy connection, a response was sent as an acknowledgment with the result code as DIAMETER_SUCCESS and action is taken as per the message.

New Behavior: For a server initiated S6a message received on a different diamproxy connection, a response message will be sent with the Experimental-Result-Code as DIAMETER_USER_UNKNOWN except for CLR. If CLR is received on different diamproxy connection, then CLA is sent with Result-Code "DIAMETER_SUCCESS" but no action is taken in MME. This CLR will not result in ATTACH/TAU rejection.

HO Continues Despite Illegal ME Indication

CSCux71332 -- Sessmgr restarts to recover from error during DDN with error indication

Feature Changes

Previous Behavior: If a Downlink Data Notification (DDN) with cause #6 (Illegal ME) arrives on the S11 when either an S1-HO or X2 HO is in progress, then the HO is aborted, the DDN continues, and the UE is paged.

New Behavior: When the SGW tries to send downlink data packets to an eNb and the eNb does not have an eRab context corresponding to the data packet, then the eNb sends an error indication to the SGW. The SGW sends a Downlink Data Notification (DDN) with cause #6 (Illegal ME) to the MME. MME code has been changed so that if a DDN with cause #6 arrives at the MME on the S11, when either an S1-HO or X2 HO is in progress, then the HO continues and is not aborted, the DDN is acknowledged.

IMSI_Detach_Indication Retried If UE Moves to Idle State

CSCux84847 - CSFB:IMSI DETACH IND not retried on policy idle-mode detach implicit
**Feature Changes**

In accordance with 3GPP TS 29.118, Release 9.3.0, Section 5.6.2, if the policy under the MME Service is configured for ‘idle-mode detach implicit’, then the MME should retry IMSI_Detach_Indication toward the MSC under the following conditions:

1. The UE makes Combined Attach
2. The UE moves to Idle
3. At some point, Delete Bearer Request is sent for Default Bearer
4. The MME sends Delete Bearer Response to the SGW/PGW and IMSI_Detach_Indication towards the MSC
5. if IMSI_Detach_Ack is not sent in response by the MSC

**Previous Behavior:** For the above scenario, the MME was not compliant and did not retry sending IMSI_Detach_Indication towards the MSC.

**New Behavior:** The MME has been modified so that it is now compliant with 3GPP TS 29.118, Release 9.3.0, Section 5.6.2, so that at the end of step 5 in the above scenario, the MME starts the TS10 timer for SGs IMSI_DETACH_INDICATION. If the MSC does not respond to the SGsAP.IMSI_DETACH_INDICATION message before timer the TS10 expires, then the MME repeats sending the SGsAP.IMSI_DETACH_INDICATION message a maximum of 2 times. The state of the SGs association during the acknowledgement procedure remains SGs-NULL.

The duration of the TS10 timer is configurable from 1 to 30 seconds with a default of 4 seconds. Configure the duration of the TS10 timer with the `timer ts10` command in the SGs Service Configuration Mode.

---

**IMSI Manager Overload Control**

**Feature Description**

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mappings maintained for all registered subscribers are synchronous with the Session Managers.

When the incoming attach rate is high at the IMSIMGR in a short span of time, the CPU consumption is very high and affects the normal processing activities of the IMSI Manager. At times this can lead to an IMSI Manager crash. Overload control methods are devised through this feature enhancement to keep the IMSI Manager CPU under control.

---

**Important**

This feature is enabled by default.

**IMSI Manager Overload Control**

IMSI Manager Overload control is implemented on both SGSN and MME call flows. Attach rate throttling (network overload protection) is implemented in IMSI Manager to cap the rate at which new requests are accepted by SGSN and MME. This feature helps us process the incoming new subscriber requests (for example ATTACH/ISRAU) at a configured rate, therefore the HLR and other nodes are not overloaded. The SGSN and MME have separate pacing queues in the IMSI Manager to monitor the incoming rate of requests and have a separate network overload configuration as well.
For the SGSN, the following requests are paced using the pacing queues:

- Initial ATTACH (with IMSI, L-PTMSI, F-PTMSI)
- Inter-SGSN RAU
- Empty-CR requests

In the MME, new connections are setup for the following events:

- UE initiated initial Attach
- All types of attach – IMSI, local GUTI, foreign GUTI, mapped GUTI, emergency and so on.
- UE initiated Inter-CN node TAU request requiring context transfer from old MME/SGSN
- TAU request with foreign GUTI or mapped GUTI
- Peer SGSN/MME initiated forward relocation request via Gn/S10/S3

With this feature enhancement when the incoming attach rate is high, the pacing queue becomes full and the further requests are either dropped or forwarded to Session Manager. The Session Manager in turn sends the reject response based on the configuration. When network overload protection action is set as "reject", the IMSI Manager has to forward overflowing requests from the pacing queue to Session Manager through a messenger call to send back error response. The IMSI Manager spends more time on messenger read and write. The IMSI Manager CPU reaches high values when the incoming call rate is very high (both SGSN/MME) though the network overload protection is configured. To ensure that the IMSI Manager CPU is under control, the IMSI Manager reduces certain messenger activities on reaching the default CPU threshold of 70%. This threshold value is fixed and this feature is enabled by default. This value is currently non-configurable. The IMSI Manager drops the overflowing requests from the pacing queue when the CPU crosses 70% mark instead of rejecting the request. Every IMSI Manager instance monitors its CPU usage independently and actions are taken according to the CPU usage.

**Relationships to Other Features**

Attach throttling feature will have an impact due to this feature enhancement. Once the CPU reaches the threshold of 70%, the messages will be dropped (irrespective of configured action).

**Monitoring and Troubleshooting IMSI Manager Overload Control**

New statistics are introduced as a part of feature which can be viewed in the Debug mode. The operator can use these statistics to find the number of requests dropped due to overload.

**Show Command(s) and/or Outputs**

This section provides information regarding show commands and/or their outputs:

`show demuxmgr statistics imsimgr all`

These counters are available for both MME and SGSN separately.

- Requests dropped due to pacing queue with High Imsimgr CPU

Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics imsimgr all. The show output is realigned for better readability. Debug logs are also provided to display the current CPU usage.
Integrity and Confidentiality Algorithms for UE

CSCu29758 - MME: Selection of integrity, confidentiality algorithm for VoLTE emergency

This chapter describes the implementation of Integrity and Confidentiality Algorithms for UEs in Limited Service Mode (LSM), and UEs that cannot be authenticated by the MME, to establish emergency calls.

Feature Description

In this feature, UEs that are in limited service mode (LSM) and UEs that cannot be authenticated by the MME are allowed to establish emergency calls.

MME uses EEA0 (Integrity) and EIA0 (Ciphering) algorithms for emergency attach requests even if the UE does not advertise the support of these algorithms in the request message, to successfully process the VoLTE emergency calls. These algorithms successfully process the VoLTE calls irrespective of the validation level configured for a UE.

The MME provides options to authenticate emergency attaches using the following CLI:

```
ue-validation-level { auth-only | full | imsi | none }
```

Using the above command syntax, it is possible to configure the MME to allow or disallow unauthenticated UEs in LSM to establish bearers for emergency calls. To establish bearers for an emergency call for unauthenticated UEs in LSM, the MME allows NAS protocol to use EIA0 and EEA0 as the integrity and ciphering algorithm respectively.

If the MME allows an unauthenticated UE in LSM to establish bearers for emergency calls on receiving an emergency attach request message from the UE, the MME:

- Selects an algorithm based on the UE's announcement only if the MME supports the requested algorithm. If the MME does not support the requested algorithm or if there is no algorithm announced, then the EEA0 and EIA0 algorithms are used.
- Set the UE EPS security capabilities to only contain EIA0 and EEA0 when sending these to the eNB in the following messages:
  - S1 UE INITIAL CONTEXT SETUP
  - S1 UE CONTEXT MODIFICATION REQUEST
  - S1 HANDOVER REQUEST

Note

As a result, the MME only sends a UE with EPS security capability containing EIA0 and EEA0 to the eNB when selecting EIA0 for NAS integrity protection because the eNB is only capable of selecting EIA0 for AS integrity protection and EEA0 for AS confidentiality protection. In general, if EIA0 is used for NAS integrity protection, then EIA0 will always be used for AS integrity protection or vice-versa.

The rules for when the MME selects the EIA0 for NAS integrity protection, and when the UE accepts a NAS security mode command selecting EIA0 for NAS integrity protection depends on whether the UE and MME can be certain that no EPS NAS security context can be established. For more information on these rules, refer to 3GPP 33.401 specifications document.
Configuration Information

The MME provides options to authenticate emergency attaches using the following CLI:

```
ue-validation-level { auth-only | full | imsi | none }
```

- The `auth-only` keyword specifies that only authenticated UEs are allowed to use the emergency bearer services.
- The `full` keyword specifies that only UEs that have been authenticated, and have successfully passed subscription and location validation, are allowed to use the emergency bearer services.
- The `imsi` keyword specifies that UEs with an International Mobile Subscriber Identity are allowed to use the emergency bearer services regardless of authentication. Even if authentication fails, the UE is granted access to use emergency bearer services.
- The `none` keyword specifies that all UEs are allowed to use the emergency bearer services. This keyword is used as a default option.

LI Cell Based IRI Reporting

CSCuy29717 - MME: LI Cell Based IRI Reporting

Refer to the LI Configuration Guide for information about this feature.

Lowercase Displayed for Received APN Names

CSCuy40169 - MME ignores APN config from subscription and uses wildcard APN config

Feature Changes

**Previous Behavior:** In earlier releases, the output generated by the "show mme-service db record imsi <imsi-value>" command displayed the letters in the APN names in the case (uppercase or lowercase) in which they were received from the HSS.

**New Behavior:** The output generated by the "show mme-service db record imsi <imsi-value>" command now displays as all lowercase letters for the received APN names; no matter the case in which they were received from either the HSS or the UE.

Disabling MSC Fallback on Failure Based on SRVCC Cause

CSCuy44854 - MME wrongly tries to establish call with other MSC during SRVCC failure

Feature Changes

**Old Behavior:**
If a voice call can be handed over to one of multiple MSC IP addresses during SRVCC handover and if the PS-CS Response from the first MSC returns with a negative cause, then the next MSC is tried.

**New Behavior:**
If a voice call can be handed over to one of multiple MSC IP addresses during SRVCC handover and if the PS-CS Response from the first MSC returns a negative cause and that cause has been included in the MME's Call-Control Profile configuration with the new `msc-fallback-disable` command, then the MME fails the SRVCCHO and does not try the next available MSC.

The new command is explained in the `Command Changes` section below. If this command is not used to define SRVCC causes, then the MME will use default behavior to select the next MSC to retry PS-CS Request.

**Command Changes**

A new command, `msc-fallback-disable`, enables the operator to define all SRVCC causes for which the MME does not try sending PS-CS Request to a next available MSC during an SRVCC handover if the MME received one of the configured SRVCC causes in the PS-CS Response from the first MSC.

```configure
call-control-profile profile_name
    [ remove ] msc-fallback-disable srvcc-cause cause
end
```

Notes:

- For information about existing commands, refer to the `Command Line Interface Reference`.
- `remove` - This command filter instructs the MME to delete the specified SRVCC cause code definition.
- `srvcc-cause cause` - This keyword configures an SRVCC cause code. If the MME receives this SRVCC cause code in a negative PS-CS Response from the first MSC tried in an SRVCC handover, then the MME sends SRVCC HO Failure and no other MSCs are tried. The `cause` must be any integer from 0 to 255, as defined in 3GPP TS 29.280.
- This command can be repeated to configure more than one SRVCC cause.
- This command is only applicable for PS-CS Requests and not for PS to CS complete messages.
- This command is applicable for both statically configured MSC addresses (in an MSC Pool) and for MSC addresses returned by DNS.
- If this command is not used to define SRVCC causes, then the MME will use default behavior for MSC fallback on failure to select the next MSC to retry PS-CS Request.

**Verification:**

To confirm the MME's current configuration of SRVCC causes, use the following show command to generate an output similar to that shown below - three separate cause codes have been configured:

```show call-control-profile full name profile_name
...MSC-fallback disabled SRVCC causes : 8 9 10 ...
```

### Processing PDN Disconnect Requests from UE

CSCuy38570 - MME rejects PDN disconnect request with code 98
Feature Changes

Previous Behavior: In cases where the UE sent PDN Activation Request and then during the setup the UE sent PDN Disconnect Request for same PDN, the MME would reject the PDN Disconnect Request.

New Behavior: In cases where the UE sends PDN Activation Request and then during the setup the UE sends PDN Disconnect Request for same PDN, the MME accepts and processes the PDN Disconnect Request to clear the connection. This enables the MME to accept the next connection request.

Customer Impact: PDN disconnect procedures are handled properly and signaling may be reduced.

Rejection of Additional PDN Connectivity Procedures

CSCuy01529 - E-RAB Setup Failed With X2-HO-Triggered Leads PDN Connectivity Reject

Feature Changes

Previous Behavior: MME rejects additional PDN Connectivity procedures if E-RAB setup receives a response with radio network cause code "X2-HO / S1-HO triggered"

New Behavior: If E-RAB setup receives a response with cause code "X2-HO / S1-HO triggered", then MME will suspend additional PDN Connectivity procedures until a handover is successfully completed.

Impact on Customer: Improved success rate in processing additional PDN Connectivity procedures.

S1-AP Inbound and Outbound Error Statistics

CSCux45930 - S1-AP Inbound and Outbound Error Statistics

Feature Changes

The following behavior change enables the carrier to track Radio Network and Protocol error statistics separately for transmitted and received errors.

Previous Behavior: Tracking support was only available for outbound, and not for inbound, error messages.

New Behavior: The "show mme-service statistics s1ap" command is enhanced to display separately transmitted and received radio network error statistics and protocol error statistics. As well, new bulk statistics are added to the MME Schema for received radio network and protocol error statistics.

Performance Changes

show mme-service statistics

New output counters are bolded in the following sample display:

show mme-service statistics s1ap

... Radio Network Error Statistics:

Transmitted:

Unknown MME UE S1AP Id: Unknown ENB UE S1AP Id:
Unknown UE S1AP Id Pair:

Received:

Unknown MME UE S1AP Id: Unknown ENB UE S1AP Id:
Unknown UE S1AP Id Pair:

Protocol Error Statistics:
MME Schema

Corresponding bulk statistic variables are added to the MME schema for received error statistics:

- s1ap-err-rcv-unknownmme-ues1apid
- s1ap-err-rcv-unknownenb-ues1apid
- s1ap-err-rcv-unknownpair-ues1apid
- s1ap-err-rcv-tfr-synerr
- s1ap-err-rcv-semanticerr
- s1ap-err-rcv-msgnotcompatible
- s1ap-err-rcv-aseignore-notify
- s1ap-err-rcv-asefalsely-constrmsg

The following bulk statistics are not new with this change, however, they have been modified in terms of their functionality for transmitted error statistics:

- s1ap-err-unknownmme-ues1apid
- s1ap-err-unknownenb-ues1apid
- s1ap-err-unknownpair-ues1apid
- s1ap-err-tfr-synerr
- s1ap-err-semanticerr
- s1ap-err-msgnotcompatible
- s1ap-err-aserej
- s1ap-err-aseignore-notify
- s1ap-err-asefalsely-constrmsg

For detailed information on these statistics, refer to the BulkstatStatistics_documentation.xls spreadsheet that is included as part of the software companion package for this release.
SCTP Peer Receive Window Size

CSCus55772 - MME stopped sending SCTP Data to ENB

Feature Changes

New Behavior: With release 19.4, the MME now tracks the number of times the SCTP stack adjusts the SCTP peer receive window size. This additional information related to the SCTP flow is displayed with a new counter, 'Receive Window Adjusted', in an enhanced output generated by the following commands:

- show mme-service statistics
- show mme-service statistics sctp
- show mme-service statistics sctp verbose

Customer Impact: This information enhances analytics of the network situation and behavior of the SCTP algorithms to facilitate debugging issues related to SCTP.

UE-Radio-Capability Length Increased

CSCur60578 - Need UERadioCapblty length to be increased

Feature Changes

Previous Behavior:
MME truncates and stores the UE-Radio-Capability information to 256 bytes even though it receives UE-Radio-Capability which is more than 256 bytes. This results in the MME sending the truncated UE-Radio-Capability information to the eNodeB in a subsequent Initial-Context-Setup Request.

New Behavior:
The MME now stores the complete UE-Radio-Capability information received from the UE, irrespective of the length. The MME sends that same information, up to a maximum limit that can be accommodated in an S1AP message, back to the eNodeB in a subsequent Initial-Context-Setup Request. Currently, the S1AP protocol has a message limit of 6144 bytes.

MME Enhancements for 19.3

This section identifies all of the MME enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the MME Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your MME.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Create Bearer Request during X2 HO

CSCuu70119 - Create Dedicated Bearer Fails - Path Switch Causes NAS Accept Msg Delay

**Feature Changes**

**Previous Behavior:** MME rejects Create Dedicated Bearer procedure if MME receives E-RAB Setup Response with "Multiple-ERAB-ID-Instances".

**New Behavior:** The MME now sends an E-RAB Release Request if an E-RAB Setup Response is received with "Multiple-ERAB-ID-Instances". As well, the MME sends an E-RAB Setup Request to the eNodeB after E-RAB Release Response. The Create Bearer procedure will complete successfully if the MME receives the E-RAB Setup Response without errors.

**Customer Impact:** Create Bearer procedure success rate is high with little additional signaling.

Emergency Bearer Support per TAC

CSCuv47804 - CLI support to disable emergency bearer support per TAC

**Important**

This feature was initially included in Release 19.2 as Lab Quality. With this release, this feature is now available as fully qualified Deploy Quality.

**Feature Changes**

**Previous Behavior:** In earlier releases, disabling of emergency bearer services was not supported in the MME.
New Behavior: In this release, MME supports disabling Emergency Bearer Services. A new command `emergency-services-not-supported` is added to the CLI, which can be configured at the TAI management database level to disable emergency service support per TAC.

As of release 19.2, the following functions are added in support of disabling emergency services:

- MME Capabilities:
  - Emergency Bearer Service profile configuration. The profile should include the following to complete the profile configuration: APN name, PGW FQDN or IP Addresses and QoS parameters to setup a session.
  - Configuration to disable emergency services at TAI management object level to reject emergency calls for a configured list of TAI.

- Attach for Emergency Bearers: MME rejects the emergency attach procedure if emergency services are disabled for a TAI from which attach request is initiated.

- PDN Connectivity for Emergency Bearer Service: the MME rejects emergency PDN activation if emergency services are disabled for a TAI.

- Tracking Area Update Procedure: If a TAU is received after an emergency attach procedure, which arrives from an area whose emergency services are disabled, MME provides the following functions:
  - Rejection of TAU in case of single emergency PDN.
  - De-activation of all emergency PDNs in case of multiple PDNs.

- Inbound Relocation Procedures: S1 and X2 handovers occurring after an emergency attach from an area where emergency services are disabled, is allowed to continue in connected mode.

**Important**

This feature is released with a feature license that will not be enforced until Release 20.0.

## Command Changes

**emergency-services-not-supported**

This command is added at TAI management object level to disable emergency services. If the emergency request is received from a TAC, for which emergency services are disabled, then the request would be rejected.

```plaintext
configure
  lte-policy
    tai-mgmt-db db_name
    tai-mgmt-obj obj_name
      emergency-services-not-supported
    end
end
```

**Notes:**

- The `emergency-services-not-supported` is a newly added keyword to disable emergency bearer services.
Performance Indicator Changes

**show mme-service all**

On running the above command, the following new field is displayed:

- Emergency Service Profile : None

**show lte-policy tai-mgmt-db name db_name**

On running the above command, the following new field is displayed:

- emergency-service-not-supported

**show mme-service statistics mme-service mmesvc**

On running the above command, the following new fields are displayed:

- Attach Reject:
  - Emergency-services-disabled: 1
- TAU Reject Total:
  - Emergency-services-disabled: 2
- TAU Reject Intra MME:
  - Emergency-services-disabled: 1
- TAU Reject Inter MME:
  - Emergency-services-disabled: 1
- PDN Connectivity Reject:
  - Emergency-services-disabled: 1

Limiting 'network-feature-support-ie'

CSCux62899 - MME should not expand 'network-feature-support-ie ims-voice-over-ps'

**Previous Behavior:**

When the call-control profile's 'network-feature-support-ie ims-voice-over-ps' command was configured, without including either the 'supported' or 'not-supported' keyword, the 'supported' keyword was appended automatically. This resulted in the MME indicating network feature support in the Attach Accept sent to the UE and adding the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages sent to the HSS, with the value set to "Supported". This indicated that IMS Voice over PS was supported in all Tracking Areas.

**New Behavior:**

When the call-control profile's 'network-feature-support-ie ims-voice-over-ps' command is configured, without including either the 'supported' or 'not-supported' keyword, then the MME indicates network feature support in the Attach Accept sent to the UE and includes the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages sent to the HSS, with the value set to "Not Supported". This indicated that IMS Voice over PS is supported in all Tracking Areas.
Paging Pre-Emption

CSCux40546 - MME higher paging precedence does not take over paging in progress

Feature Changes

Previous Behavior: By default, the MME does not support immediate paging pre-emption. The MME waits until the current paging procedure times out and then picks the new precedence based on the paging precedence configuration and then immediately sends another Paging Request.

New Behavior: While the default behavior has not changed, a new CLI makes it possible for the operator to override the default behavior and enable immediate paging pre-emption causing the MME to stop an on-going paging procedure for any paging trigger and adopt a newly received paging trigger of higher paging precedence.

Command Changes

heuristic-paging

A new keyword, preempt-immediately, has been added to the heuristic-paging command to allow the operator to enable immediate paging pre-emption.

configure
  context context_name
  mme-service service_name
    heuristic-paging paging-map map_name | preempt-immediately |
  end

Notes:

• preempt-immediately - In situations where the MME receives paging triggers with higher paging precedence, this keyword causes the MME to override the default behavior for paging precedence handling, so that the MME discontinues use of the current paging procedure to adopt a newly received paging trigger of higher paging precedence.

• This behavior change has no impact on the t3413-timeout configuration.

Performance Indicator Changes

show mme-service all

The display resulting from this command includes the following new field:

Heuristic Paging Preempt Immediately : Enabled/Disabled

SMS Behavior When VLR Is Unreliable

CSCux74778 - Abnormal behavior when SMS is sent from UE and the VLR is not reliable

Feature Changes

Previous Behavior:

The MME forwards the UE's MO-SMS to the VLR even if the VLR has reset and is currently unreliable. This can result in a lack of SMS service for the UE.
New Behavior:
If the MME receives an MO-SMS from the UE and the VLR is currently unreliable, the MME sends an IMSI Detach to the UE so that the UE can re-attach with the VLR once it stabilizes.

MME Enhancements for 19.2

This section identifies all of the MME enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your MME.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Cause Code Mapping for UE-CONTEXT-RELEASE Sent from MME

CSCux13166 - MME releases UE context with Category NAS Unspecified for non-TAU

Feature Changes

Previous Behavior: By default, an MME initiated the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME received a TAU Request over Initial-UE if the UE was in the connected state.
CLI was available which allowed the operator to specify the cause code mapping for MME-initiated S1-UE-CONTEXT-RELEASE whenever the MME received a TAU over Initial-UE message from the eNodeB. For all non TAU scenarios, MME initiated the UE-CONTEXT-RELEASE with cause NAS/Unspecified by default whenever it receives any message other than TAU over Initial-UE if its in connected state.

**New Behavior:** Now by default, the MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a request over Initial-UE (for all TAU and non-TAU scenarios such as Service Request, Attach, and Extended-Service-Request), if the UE is in the connected state.

The existing CLI has been modified to enable the operator to specify the cause code mapping for the MME-initiated S1-UE-CONTEXT-RELEASE whenever the MME receives an Initial-UE request message from the eNodeB, irrespective of the procedure if the UE is in the connected state. CLI changes are explained in the following section.

**Command Changes**

`s1-ue-context-release`

The original `init-ue-from-enodeb-for-tau` keyword name and functionality have been modified. The new keyword is `init-ue-from-enodeb`. New functionality allows the MME to send the configured cause code mapping in the MME-initiated UE-CONTEXT-RELEASE in response to *any unexpected procedure* over Initial-UE from the eNodeB, such as TAU, Service Request, Extended Service Request, Attach Request.

---

**Important**  
In support of backward compatibility, the MME will accept configurations with either form of the keyword. When the operator explicitly saves the configuration, the configuration will save using the new form of the keyword.

```
configure
center context_name
mme-service service_name
s1-ue-context-release reason init-ue-from-enodeb cause type { nas value nas_value | radio value radio_value }
default s1-ue-context-release reason init-ue-from-enodeb cause
end
```

**Notes:**

- The configured cause code will be sent in the UE-CONTEXT-RELEASE message whenever the MME releases the existing S1AP connection in response to unexpectedly receiving an Initial-UE message for any procedure such as TAU, Service Request, Extended Service Request, Attach Request.
- Currently, the only release reason possible is `init-ue-from-enodeb`.
- There are two cause options for which cause code values can be assigned:
  - `nas value nas_value` options are:
    - 0 - Normal Release (default value)
    - 1 - Authentication Failure
Emergency Bearer Support per TAC

CSCuv47804 - CLI support to disable emergency bearer support per TAC

Important: This feature is being released as Lab Quality. Full support for this feature is planned for a future release.

Feature Changes

Previous Behavior: In earlier releases, disabling of emergency bearer services was not supported in the MME.

New Behavior: In this release, MME supports disabling Emergency Bearer Services. A new command `emergency-services-not-supported` is added to the CLI, which can be configured at the TAI management database level to disable emergency service support per TAC.

As of release 19.2, the following functions are added in support of disabling emergency services:

- MME Capabilities:
  - Emergency Bearer Service profile configuration. The profile should include the following to complete the profile configuration: APN name, PGW FQDN or IP Addresses and QoS parameters to setup a session.
  - Configuration to disable emergency services at TAI management object level to reject emergency calls for a configured list of TAI.

- Attach for Emergency Bearers: MME rejects the emergency attach procedure if emergency services are disabled for a TAI from which attach request is initiated.

- PDN Connectivity for Emergency Bearer Service: the MME rejects emergency PDN activation if emergency services are disabled for a TAI.

- Tracking Area Update Procedure: If a TAU is received after an emergency attach procedure, which arrives from an area whose emergency services are disabled, MME provides the following functions:
  - Rejection of TAU in case of single emergency PDN.
  - De-activation of all emergency PDNs in case of multiple PDNs.

- Inbound Relocation Procedures: S1 and X2 handovers occurring after an emergency attach from an area where emergency services are disabled, is allowed to continue in connected mode.
Important

This feature is released with a feature license that will not be enforced until Release 20.0.

Command Changes

emergency-services-not-supported

This command is added at TAI management object level to disable emergency services. If the emergency request is received from a TAC, for which emergency services are disabled, then the request would be rejected.

configure
  lte-policy
  tai-mgmt-db db_name
  tai-mgmt-obj obj_name
  emergency-services-not-supported
  end

Notes:

- The emergency-services-not-supported is a newly added keyword to disable emergency bearer services.

Performance Indicator Changes

show mme-service all

On running the above command, the following new field is displayed:

- Emergency Service Profile : None

show lte-policy tai-mgmt-db name db_name

On running the above command, the following new field is displayed:

- emergency-service-not-supported

show mme-service statistics mme-service mmesvc

On running the above command, the following new fields are displayed:
Event Logging

CSCuw12198 - EDRs support on MME

**Important**
With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

**Feature Changes**

The MME handles numerous subscriber calls from different eNodeBs in the network. In order to troubleshoot any issues for a particular subscriber, the events that caused the issue is recorded. The events could be individual procedures such as ATTACH, DETACH, TAU, Handovers and so on.

The Event Data Record is a proprietary feature of StarOS. In this feature, MME provides a debugging framework to capture procedure level information for each subscriber. On the completion of a procedure successfully or unsuccessfully, the MME generates a procedure summary. This summary provides details of the events and issues, which is nearly comparable to real-time debugging.

**Previous Behavior**: Earlier, MME did not support Event Data Records (EDRs) for Event Logging.

**New Behavior**: From this release onwards, MME supports EDRs for events such as ATTACH, DETACH, TAU and Handovers during Event Logging.

**Customer Impact**: The addition of the EDR support for Event Logging aids in debugging.

**Command Changes**

reporting-action

This is a new command added in the Call Control Profile Configuration, along with a new keyword `mme-event-record` to enable Event Logging.

```bash
config
call-control-profile profile_name
    reporting-action mme-event-record
exit
```

To enable EDR logs use the following configuration:

```bash
config
ccontext context_name
edr-module active-charging-service reporting
cdr { push-interval interval_time | remove-file-transfer | use-harddisk | transfer-mode { pull | push primary { encrypted-url | url } url | secondary { encrypted-secondary | secondary-url } url
```
To configure File Parameters use the following configuration:

cfg

context context_name

session-event-module

file name file_name current-prefix current_file_prefix rotation volume file_rotation_size rotation time file_rotation_time field-separator underscore sequence-number padded charging-service-name

include compression gzip

end

Notes:

• The call-control-profile configuration enables Event Logging for MME, provided this profile is associated to the mme-service through operator policy and subscriber map.

• reporting-action enables procedure reports.

• mme-event-record reports MME procedures in the form of event records using CDRMOD.

Performance Indicator Changes

show call-control-profile full name <profile_name>

The following new field is added to the output of this command for this feature:

• GBR Bearer Preservation Timer

MME QoS Profile

CSCuu91775 - MME control of QoS 4G received from HPLMN

Important With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

Feature Changes

Previous Behavior: In previous releases, QoS parameters are enforced using the configuration of the APN profile.

New Behavior: The MME QoS Profile feature provides flexibility to define a Quality of Service (QoS) profile for a given APN for EPS or 4G subscribers. Further, the MME QoS Profile feature provides bearer-level QoS control through a new Bearer Control profile. One or more Bearer Control profiles can be associated to a QoS profile on per QCI or for a range of QCI.

A QoS profile is defined by:

• List of bearers to be rejected on QCI basis

• Operator provided values for capping AMBR (UL and DL)
A Bearer Control profile is defined by:

- Remapping matrix for QCI
- Operator provided values for capping ARP PL/PCI/PVI
- Operator provided values for capping MBR and GBR (UL and DL)

Now, all QoS parameters are taken from the QoS profile and Bearer Control profile. These profiles and associated functionality are designed to deal with EPS network QoS characteristics. These new profiles enable PDN-level and bearer-level control of QoS parameters received from the HSS or PGW.

To maintain backward compatibility, the MME still honors the QoS values from the APN profile if/when the QoS profile is not associated to an EPS Network in the APN profile.

Please note that a feature license is not required for this 19.2 release of this feature, however, a license will be needed for non-standard QCIs in Release 20.

**Customer Impact:** Greater control over QoS parameters.

---

**Important**

This feature is released with a feature license that will not be enforced until Release 20.0.

---

**Command Changes**

**quality-of-service-profile**

This command is now available for the use of the MME in the Global Configuration mode. This command enables the operator to create and configure an instance of a QoS profile for the MME.

```bash
configure quality-of-service-profile qos_profile_name
end
```

**Notes:**

- `qos_profile_name` - The defined value identifies the name of the QoS profile being created for the MME. The name must be an alphanumeric string of 1 through 100 characters and we recommend that the profile name be unique for the system. This profile name will be needed for other configuration tasks. The system enters the QoS Profile configuration mode and presents the following prompt:

  [local]host_name(quality-of-service-profile-qos_profile_name)#.

- Multiple QoS parameters can be configured for the QoS profile. Refer to the *QoS Profile* section of the *Command Line Interface Reference* for command information.

---

**Important**

The QoS profile does not become valid until it is associated with an APN profile with access type "eps". For more information, refer to the *APN Profile Configuration Mode* section in the *Command Line Interface Reference*.

---
bearer-control-profile

This command is new in the Global Configuration mode. This command enables the operator to create and configure an instance of a Bearer Control profile as part of the MME QoS Profile feature.

```
configure
  bearer-control-profile bc_profile_name
end
```

Notes:

- **bc_profile_name** - The defined value identifies the name of the Bearer Control profile being created for the MME. The name must be an alphanumeric string of 1 through 64 characters and we recommend that the profile name be unique for the system. This profile name will be needed for other configuration tasks. The system enters the Bearer Control Profile configuration mode and presents the following prompt: [local]/host_name(bearer-control-profile-bc_profile_name)#.

- The Bearer Control Profile configuration mode provides commands to configure QoS parameters for dedicated bearers (see dedicated-bearer section below) and for default bearers (see default-bearer section below.

- Bearer level parameters such as ARP-PL, ARP-PVI, ARP-PCI, MBR, GBR, remap QCI value can be configured here independently for default/dedicated bearer along with the action to be taken, such as prefer-as-cap or pgw-upgrade. Bearer Control profile can be applied for specific QCIs or range of QCIs.

associate

Use the new associate command in Quality of Service Profile configuration mode to associate the Bearer Control profile with the QoS profile and map a specific QCI or a range of QCI to the Bearer Control profile being associated with the QoS profile.

```
configure
  quality-of-service-profile qos_profile_name
    associate bearer-control-profile bc_profile_name qci qci_value [ to end_qci_value ]
end
```

Notes:

- **qos_profile_name** - Identifies the name of the QoS profile. Enter 1 to 64 alphanumeric characters.

- **bc_profile_name** - Identifies the name of the bearer control profile being associated with the QoS profile. Enter 1 to 64 alphanumeric characters.

- **qci** - Identifies either a specific QoS class identifier (QCI) or a range of QCI:

  - **qci_value** - Enter an integer from 1 through 9 to identify a specific QCI.
  - **to end_qci_value** - Type "to" and then enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range.

- A specific QCI cannot be associated to more than one bearer control profile. The QCI of the bearer is used to identify the applicable bearer control profile.

  - For dedicated bearer, the QCI of bearer is initially determined by the QCI value received from PGW during dedicated bearer activation or the value received from peer MME/S4-SGSN.
  - For default bearer, the QCI of bearer is initially determined by the subscription from HSS or the value received from peer MME/S4-SGSN during inbound relocation.
To delete the Bearer Control profile association with the QoS profile, issue the following command:

```
remove associate bearer-control-profile bc_profile_name
```

### qci-reject

Use the new `qci-reject` command in Quality of Service Profile configuration mode to identify a specific QCI or a range of QCI for which the MME must reject bearer establishment or modification.

```
configure
  quality-of-service-profile qos_profile_name
    qci-reject { default-bearer | dedicated-bearer } qci_value | to end_qci_value |
end
```

Notes:

- `qos_profile_name` - Identifies the name of the QoS profile.
- `dedicated-bearer` - Identifies either a specific QoS class identifier (QCI) or a range of QCI for the dedicated-bearer:
  - `qci_value` - Enter an integer from 1 through 9 to identify a specific QCI.
  - `to end_qci_value` - Type "to" and then enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range.
- `default-bearer` - Identifies either a specific QoS class identifier (QCI) or a range of QCI for the default-bearer:
  - `qci_value` - Enter an integer from 5 through 9 to identify a specific QCI.
  - `to end_qci_value` - Type "to" and then enter an integer from 6 through 9 that is greater than the QCI value entered for the beginning of the range.

The MME can reject default-bearers and dedicated-bearers based on QCI received from the subscription or the peer-MME/S4-SGSN during inbound relocation or the Create Session Response/Update Bearer Request/Create Bearer Request procedure.

To delete the QCI rejection configuration issue the following command:

```
remove qci-reject
```

### apn-ambr

Use the `apn-ambr` command in the Quality of Service Profile configuration mode to set local values for capping -type and action to be taken for APN-AMBR.

```
configure
  quality-of-service-profile qos_profile_name
    apn-ambr max-ul max_ul_val max-dl max_dl_val { pgw-upgrade | prefer-as-cap } { local | minimum | rej-if-exceed }
  remove apn-ambr
end
```

Notes:
• This keyword **max-ul** sets the local value for the maximum uplink bit rate. **max_ul_val** must be an integer from 0 through 1410065408.

• This keyword **max-dl** sets the local value for the maximum downlink bit rate. **max_dl_val** must be an integer from 0 through 1410065408.

• This command sets the QoS capping mechanism to be applied for the APN-AMBR received from HSS/PGW/peer-node. One or both **prefer-as-cap** and/or **pgw-upgrade** must be configured to override the default behavior, which is to accept the received value from the HSS/peer-node/PGW.

• **prefer-as-cap** - This keyword configures the capping that is applied on the subscription value received from the HSS or the value received from the peer-node (MME/S4-SGSN) during inbound relocation. One of the following actions must be configured under **prefer-as-cap** -- Note that the resulting value is used for the QoS parameter and sent in the Create Session Request or the ModifyBearer Command (in case of HSS-initiated QoS/APN-AMBR modification) message:
  
  * **local** - The configured local value will be used.
  * **minimum** - The minimum (lowest) value of the configured local value or the HSS-provided value will be used.
  * **reject-if-exceed** - The request/procedure is rejected if the HSS-provided value exceeds the configured local value.

• **pgw-upgrade** - This keyword configures the QoS capping to be applied on the values received from the PGW during Attach / PDN-connectivity / Bearer-creation / Bearer-modification procedures. One of the following actions must be configured under **pgw-upgrade** -- Note that the resulting value is used for the QoS parameter and sent to the UE:
  
  * **local** - The configured local value will be used.
  * **minimum** - The minimum (lowest) value of the configured local value or the PGW-provided value will be used.
  * **reject-if-exceed** - The request/procedure is rejected if the PGW-provided value exceeds the configured local value.

• To delete the APN-AMBR capping configuration issue the following command:
  
  remove apn-ambr

**dedicated-bearer or default-bearer**

The **dedicated-bearer** and **default-bearer** commands, in the Bearer Control Profile configuration mode, are used to configure the QoS control parameters separately for (one or both) default-bearers and dedicated-bearers. The operator provided values are configured for ARP-PL, ARP-PCI, ARP-PVI, MBR, GBR, QCI along with their prefer-as-cap or pgw-upgrade capping.

```
configure
  bearer-control-profile be_profile_name
    dedicated-bearer { arp { preemption-capability | preemption-vulnerability | priority-level } pgw-upgrade { local | minimum | rej-if-exceed } | gbr gbr-up gbr_up_value gbr-down gbr_down_value pgw-upgrade { local | minimum | rej-if-exceed } | mbr mbr-up mbr_up_value mbr-down mbr_down_value pgw-upgrade { local | minimum | rej-if-exceed } }
    default-bearer { arp { { preemption-capability | preemption-vulnerability | priority-level } | pgw-upgrade | prefer-as-cap } { local | minimum | rej-if-exceed } } | qci { remap | pgw-upgrade { local | }
```

---

**Release Change Reference, StarOS Release 19**

**MME Changes in Release 19**

**MME QoS Profile**
minimum | rej-if-exceed } } }

remove { dedicated-bearer | default-bearer } { arp | gbr | mbr | qci }
end

Notes:

• Use the following command to delete either the default-bearer or dedicated bearer configuration:
  remove { dedicated-bearer | default-bearer } { arp | gbr | mbr | qci }

• The command dedicated-bearer sets the capping for the dedicated-bearer with the following parameters.

• The command default-bearer sets the capping for the default-bearer with the following parameters.

• The arp keyword configures the allocation and retention priority parameters:
  * preemption-capability - Enter an integer, either 0 (may) to specify that this bearer may pre-empt other lower priority bearers if required, or 1 (shall-not) to specify that this bearer shall not pre-empt other lower priority bearers.
  * preemption-vulnerability - Enter an integer, either 0 (pre-emptible) to specify that this bearer is preemptible by other high priority bearers, or 1 (not-pre-emptible) to specify that this bearer is not pre-emptible by other high priority bearers.
  * priority-level - Enter an integer 1 through 15, with 1 as the highest priority, to specify the allocation/retention priority level.

• The pgw-upgrade keyword can be included in the command with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the PGW and the options include:
  * local - Instructs the MME to select locally configured values for QoS capping.
  * minimum - Instructs the MME to select the lower value, of the two values locally configured or received value, to use as the QoS capping value.
  * rej-if-exceed - Instructs the MME to reject the call if the received value exceeds the locally configured value.

• The prefer-as-cap keyword can be included with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the HSS or from the peer-MME/S4-SGSN:
  * local - The configured local value will be used.
  * minimum - The minimum (lowest) value of the configured local value or the HSS-provided value will be used.
  * reject-if-exceed - The request/procedure is rejected if the HSS-provided value exceeds the configured local value.

• The gbr keyword configures the Guaranteed Bit Rate values. This keyword is only used for the dedicated-bearer configuration.
  * gbr-up - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
  * gbr-down - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.
• The **mb**r keyword configures the Maximum Bit Rate values. This keyword is only used for the dedicated-bearer configuration.

  * **mb-up** - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
  * **mb-down** - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.

• The **qci remap** keyword sets the locally configured QCI. Enter an integer from 1 through 9. The QCI remap mechanism maps an incoming QCI or a range of QCI to the configured QCI or range of QCI. QCI remap is the first configuration that is applied, from the bearer control profile configuration, and it is applicable only during Create Session Request and Create Bearer Request procedures. The Bearer Control profile associated to the remapped QCI value is used for capping the remaining QoS parameters.

• **QoS Computation** - The following explains how the resultant QoS values are derived for the **minimum** and **reject-if-exceed** actions configured under **prefer-as-cap** or **pgw-upgrade**.

  * **QCI**

    * Every standard GBR/non-GBR QCI is associated with a priority level as per 3GPP TS 23.203 v12.10.0, Table 6.1.7.

    | QCI | Resource Type | Priority |
    |-----|---------------|----------|
    | 1   | GBR           | 2        |
    | 2   | GBR           | 4        |
    | 3   | GBR           | 3        |
    | 4   | GBR           | 5        |
    | 5   | non-GBR       | 1        |
    | 6   | non-GBR       | 6        |
    | 7   | non-GBR       | 7        |
    | 8   | non-GBR       | 8        |
    | 9   | non-GBR       | 9        |

    * Priority Level 1 has the highest priority and in case of congestion lowest priority level traffic would be the first to be discarded.

    * **minimum**: The QCI with lower priority level will be used.

    * **rej-if-exceed**: If the received QCI has higher priority level than the configured local QCI, then the procedure will be rejected.

* **ARP Priority Level**

  * ARP Priority level decreases on increasing value (1 to 15). ARP Priority level 1 has the highest priority value.

  * **minimum**: The lower ARP Priority level (i.e. higher value) will be used.
* **rej-if-exceed**: If the received ARP Priority level is higher (i.e. value is lesser) than the CLI configured local ARP Priority level, then the procedure will be rejected.

* **ARP-PCI**

* Preemption capability indicator can have either of the following two values, where may (0) > shall-not (1)
  * **may** - specifies that this bearer may preempt other lower priority bearers, if required
  * **shall-not** - specifies that this bearer shall-not pre-empt other lower priority bearers.

* Following table indicates the resultant pre-emption capability for the *minimum* prefer-as-cap or pgw-upgrade:

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>may</td>
<td>may</td>
<td>may</td>
</tr>
<tr>
<td>may</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>may</td>
<td>shall-not</td>
</tr>
<tr>
<td>shall-not</td>
<td>shall-not</td>
<td>shall-not</td>
</tr>
</tbody>
</table>

* **rej-if-exceed**: If the received ARP-PCI value is *may* and the configured local value is *shall-not*, then the procedure will be rejected.

* Default value set by MME if not provided by HSS/PGW: *shall-not*

* **ARP-PVI**

* Preemption vulnerability indicator can have either of the following two values, where *not-pre-emptible* (1) > *pre-emptible* (0)
  * **pre-emptible** - specifies that this bearer is pre-emptible by other high priority bearers
  * **not-pre-emptible** - specifies that this bearer is NOT pre-emptible by other high priority bearers

* Following table indicates the resultant pre-emption vulnerability for the *minimum* prefer-as-cap or pgw-upgrade:

<table>
<thead>
<tr>
<th>Received value</th>
<th>Configured local value</th>
<th>Resultant value to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>pre-emptible</td>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>pre-emptible</td>
<td>pre-emptible</td>
</tr>
<tr>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
<td>not-pre-emptible</td>
</tr>
</tbody>
</table>

* **rej-if-exceed**: If the received ARP-PVI value is *not-pre-emptible* and the configured local value is *pre-emptible*, then the procedure will be rejected.
° Default value set by the MME if not provided by the HSS/PGW: pre-emptible

° MBR / GBR

° minimum:

◦ Uplink - The lower of the values, comparing the received values and the configured local value, will be used for APN-AMBR/MBR/GBR.

◦ Downlink - The lower value of the received value and configured local value will be used for APN-AMBR/MBR/GBR.

° rej-if-exceed: If the received Uplink value is greater than the configured local Uplink value or the received Downlink value is greater than the configured local Downlink value, then the procedure will be rejected.

associate

Use the associate command in the APN Profile Configuration Mode to associate the MME's QoS profile with an APN profile. A new option, eps, has been provided for the access-type keyword to indicate the QoS profile supports 4G/EPS network requirements. Associating the QoS profile with the APN profile makes the QoS profile "valid".

configure

apn-profile apn_profile_name
  associate quality-of-service-profile qos_profile_name access-type eps
  remove associate quality-of-service-profile access-type eps
end

Notes:

• qos_profile_name This value identifies the name of the QoS profile for the MME. The name must be an alphanumeric string of 1 through 100 characters and we recommend that the profile name be unique for the system.

  Important Only one QoS profile for the MME can be associated with a single APN profile.

• The eps option for the access-type keyword associates the EPS network-type with this QoS profile. Selecting this type is required to enable the MME QoS Profile support functionality.

• To delete the QoS profile association with the APN profile, issue the following command:
  remove associate quality-of-service-profile access-type eps

• For additional information about the apn-profile commands and the QoS parameters that can be configured under the APN profile, refer to the section on APN Profile Configuration Commands in the Command Line Interface Reference.

  Important Once the MME's QoS profile is configured, these QoS parameter values override the QoS configurations in the APN profile.
The APN profile is not valid until the APN profile is associated with an operator policy via the `apn` command. For more information, refer to the *Operator Policy Configuration Mode* section in the *Command Line Interface Reference*.

## Operator Policy Selection Based on IMEI-TAC

CSCuw97149 - Operator Policy based on IMEI TAC selection.

### Feature Changes

Operator policies (proprietary Cisco functionality) empower the carrier/network operators to configure preferred call handling controls not typically used in all applications and to determine the granularity of the implementation of any operator policy; to groups of incoming calls or simply to one single incoming call.

**Previous Behavior:** The MME selects an operator policy to guide call handling based on the UE's international mobile subscriber identity (IMSI) and PLMN-ID.

**New Behavior:** Now, the MME can select/re-select an operator policy based on the UE's IMSI or based on the UE's unique international mobile equipment identity - type allocation code (IMEI-TAC). Including the type allocation code (TAC) in the operator policy selection process results in the network access restrictions based on the type of wireless device as identified by the IMEI-TAC.

This IMEI-TAC-based selection functionality is configured with the new command changes (see *Command Changes* below) then, except for emergency calls, the MME will select/re-select the operator policy whenever the MME retrieves the IMEI or IMEI-SV in one of the following scenario:

- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Identity-Request with IMEI.
- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (`policy attach imei-query-type` under MME service must be enabled).
- normal 4G TAU when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (`policy tau imei-query-type` under MME service must be enabled).
- inbound handover when IMEI/IMEI-SV is received with IMSI via the Forward-Relocation-Request.
- S10 and S3 Attaches when IMEI/IMEI-SV is retrieved with IMSI via EGTP-Identification-Request.
- Inter-RAT TAU and Intra-RAT TAU with MME change when IMEI/IMEI-SV is received with IMSI in Context-Response.

### Command Changes

The operator policy(s) and call control profile(s) must first be configured according to the instructions in the section on *Operator Policy* in the *MME Administration Guide*. 

---

**Important**

Release Change Reference, StarOS Release 19
To setup IMEI-TAC based operator policy selection, use the new `imei-tac` keyword to configure either a particular IMEI-TAC value or a range of IMEI-TAC values as matching criteria. As well, associate an operator policy and assign an order of precedence for this IMEI-TAC value or range.

```
configure
  lte-policy
    subscriber-map map_name
      precedence precedence_number match-criteria imei-tac { range start_tac_value to end_tac_value | value tac_value } operator-policy-name policy_name
      no precedence precedence_number
end
```

Notes:

- `tac_value` is an 8 digit number that identifies a specific type allocation code. The TAC, the first eight digits of the 15-digit IMEI or 16-digit IMEI-SV, identifies the equipment manufacturer, the device type and the model number (if there is one).

---

**Paging Priority IE**

CSCuv35352 - Paging priority support in MME for CSFB

**Important**

With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

---

**Feature Changes**

This feature is developed to provide Paging Priority support on the MME. Paging priority support is provided for Mobile Originating and Mobile Terminating CSFB calls.

**Mobile Terminating CSFB calls:** Mobile terminating CSFB calls are prioritized by providing paging priority information to the eNodeB during CSFB calls; the eNodeB in turn pages the UEs accordingly. If the MME is configured to send paging priority to the eNodeB, when a paging request message is received on the SGs interface with an indication of the eMLPP priority level, the MME sends the paging priority value in the S1AP paging message request to the eNodeB. This priority value is used to provide preferential treatment to the paging of the UE and also to the subsequent CS fallback procedures as compared to other normal procedures.

**Mobile Originating CSFB calls:** In Mobile originating CSFB calls if the UE is subscribed for eMLPP services, the MME uses the mps-cs-priority received in the subscription to set the priority as "CSFB High Priority" in "CS Fallback Indicator IE". This priority value is sent in the SIAP UE Context Setup/Modification message to the eNodeB, the eNodeB then initiates the CSFB procedure with priority.

The MME relays the eMLPP priority value received from MSC/VLR as paging priority-ie in SIAP paging-request message to eNodeBs. With the implementation of this feature a new CLI command `paging-priority cs` is introduced under the Call Control Profile configuration mode through which the operator can configure the system to control sending of the paging priority value to the eNodeB. The operator can configure the system to ignore the eMLPP priority value received from MSC and configure the MME to send user-defined value as paging-priority to eNodeB. The operator can also choose to completely ignore eMLPP priority and disable sending priority value. Operator can configure the system to send paging priority IE always in SIAP Paging request irrespective of whether MSC/VLR include/supports eMLPP priority or not. This applicable to mobile terminating CS fall back call.

- Paging Priority is not supported for PS paging.
Inclusion of Additional CSFB indicator for CSFB MO Emergency calls is not supported

Note
This feature is license controlled. Please consult your Cisco Account Representative for information about the specific license.

Important
This feature is released with a feature license that will not be enforced until Release 20.0.

Command Changes

paging-priority cs
The following new CLI command under the Call Control profile configuration mode is configured to support sending of paging-priority value in S1AP paging-request message to the eNodeB. This command helps the operator to prioritize the Mobile terminated CSFB voice calls of a set of subscribers irrespective of them subscribed for eMLPP services or not.

configure
call-control-profile cc_profile_name
[remove] paging-priority cs value
exit

Notes:
• By default, sending of paging priority-ie in S1AP paging-request message to eNodeBs is enabled. The priority value received from the MSC/VLR is relayed to the eNodeB.
• The keyword cs is used to configure the value of paging-priority sent to eNodeB for CS paging. The paging priority value is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.
• A lower value of paging priority indicates a higher priority.
• Older values of paging priority are overridden by configuring new values.
• The remove keyword deletes the existing configuration.

mpc cs-priority
The following new CLI command under the Call Control profile configuration mode is configured to support multimedia priority service in the CS domain. This command helps the operator to prioritize the Mobile originating voice calls of a set of subscribers irrespective of them subscribed for eMLPP services or not.

cfg

call-control-profile cc_profile_name
[remove] mps cs-priority { subscribed | none }
exit

Notes:
• By default MME sets the value of "CS fallback indicator IE" as "CSFB High Priority" in the S1AP UE Context Setup/Modification if the MPS-CS-Priority value is set in "MPS-Priority" in EPS Subscription from HSS

• The keyword cs-priority configures support for priority service in the CS domain.

• The keyword subscribed configures support for priority service in the CS domain. The "CS Fallback Indicator IE" is set to "CSFB High Priority" in the S1AP UE Context Setup/Modification message.

• The keyword none configures disables support for priority service in the CS domain. The "CS Fallback Indicator IE" is set to "CSFB Required" in the S1AP UE Context Setup/Modification message.

• The remove keyword deletes the existing configuration.

Performance Indicator Changes

show call-control profile full all

The following new fields are added to the show output to display the paging priority configuration for Mobile originating and terminating CSFB calls:

• Paging priority to be sent to eNodeB

• MPS CS priority

Purge Request Behavior

CSCuv27053 - Purge-request towards only one HSS after sessmgr crash

Feature Changes

Previous Behavior: After a Session Manager recovers from a crash, the MME sends the Purge Request to the default home HSS identified in the MME service configuration for any UE (homer or roamer) that had detached

New Behavior: After a Session Manager recovers from a crash, the MME sends the Purge Request to the default home HSS identified in the MME service configuration for any IMSIs (homer) that had detached. The MME does not send any Purge Requests for detached roamer IMSIs post session recovery.

TAC to LAC Mapping

CSCuw23234 - Increase TAC/LAC Mapping from 512 to 1024

Important

With Release 19.2.1, this feature is available as fully qualified Deploy Quality.
**Feature Changes**

**Previous Behavior:** Earlier, the TAC to LAC mapping was restricted to only 512 entries.

**New Behavior:** In this release, the TAC to LAC mapping entries have been increased from 512 to 1024 entries.

**Target Access Restriction**

CSCux33388 - InterSGSN 3G to 2G HO fails
CSCur41900 - Rollback Behavior in EPC during TAU/RAU Needs to be Corrected

**Feature Changes**

Target Access Restriction feature was added to the SGSN and MME in release 17.4. The purpose of this feature is to avoid rollback behavior that exists in RAU and TAs by checking target RAT Type IE present in the Context Request at the source node, and then rejecting the TAU/RAU based on the subscriber's ARD profile earlier in the cycle if the target RAT is restricted for the subscriber. Rollback behavior caused late TAU/RAU rejection, resulting in PDP/bearer deletion for the MME, PGW, and the SGSN, requiring the UE to reattach and reinitialize lost PDP/bearer.

**Previous Behavior:** As a part of this functionality, the target access restriction feature instructs the source-SGSN or the source-MME to reject outbound RAU when the target access was restricted for the subscriber. Rejection was performed without checking "access-restriction-data no-check" in the call control profile configuration.

**New Behavior:** With release 17.6.1, a new command keyword **target-access-restriction** has been introduced to the call control profile configuration to control (enable/disable) target access restriction functionality. Target access restriction is now disabled by default on both the SGSN and the MME. Refer to the **Command Changes** section below for the command information to enable/disable this functionality.

The default behaviors for the SGSN and the MME now differ:

- **New Behavior for the MME only:** "target-access-restriction" keyword configuration will control the target access restriction feature for the MME without other consideration:
  - **No Rejection:** if "target-access-restriction" is not enabled, then the source-MME will not reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
  - **Rejection:** if "target-access-restriction" is enabled, then the source-MME will reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

- **New Behavior for the SGSN only:** "target-access-restriction" keyword configuration enables/disables the target access restriction feature. The SGSN also considers "access-restriction-data no-check" in the call control profile configuration prior to rejecting outbound RAU when target access restriction functionality is enabled. The SGSN's target access restriction behavior is dependent upon the SGSN's "access-restriction-data no-check" configuration:
• **No Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

• **Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will ignore the "target-access-restriction enabled" configuration and the source-SGSN will *reject* the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

### Command Changes for the MME

**access-restriction-data**

With release 17.6.1, the MME has access to this command in the call-control-profile configuration mode. The new keyword *target-access-restriction* enables or disables rejection of the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

```bash
configure
call-control-profile ccprof_name
    access-restriction-data target-access-restriction
    remove access-restriction-data [ target-access-restriction ]
end
```

**Notes:**

- Including the *target-access-restriction* keyword with the command enables the target access restriction feature.
- Including the *remove* command filter disables the target access restriction feature. Inclusion of the *target-access-restriction* keyword in the remove command is currently optional.

### Command Changes for the SGSN

**access-restriction-data**

With release 17.6.1, the new keyword *target-access-restriction* enables or disables the Target Access Restriction feature.

```bash
configure
call-control-profile ccprof_name
    access-restriction-data [ eutran-not-allowed | failure-code | no-check | target-access-restriction ]
    access-restriction-data no-check
    remove access-restriction-data [ target-access-restriction ]
end
```

**Notes:**

- Including the *target-access-restriction* keyword with the command enables the target access restriction feature.
With the target access restriction feature enabled, including the no-check keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Including the remove command filter with the target-access-restriction keyword disables the target access restriction feature.

With the target access restriction feature enabled, including the remove command filter with the no-check keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Performance Indicator Changes

show call-control-profile

The Target Access Restriction field will display in the output with Enabled or Disabled and it will appear similar to the following:

```
[local] test# show call-control-profile full name ccprof1
...
Authentication Detach : Not configured
Regional Subscription Restriction Failure Code Value : 13
ARD-Checking : Enabled
ARD Failure Code : Disabled
Access Restriction Data : EUTRAN Allowed
Target Access Restriction : Enabled
Zone-Code Check : Enabled
...
```

show configuration verbose

The access-restriction-data target-access-restriction field displays in the output without the "remove" prefix to indicate it is Enabled or with the "remove" prefix to indicate the feature is Disabled. The output will appear similar to the following when the feature is enabled:

```
[local] test# show configuration verbose
...
call-control-profile ccprof1
  remove rau-inter ctxt-xfer-failure
  no subscriber-control-inactivity
...
  access-restriction-data target-access-restriction
...
```

UDPC2 Support for SGSN/MME

CSCuw02651 - MME MMEmgrs Scaling and new config support on different platforms

**Important** With Release 19.2.1, this feature is available as fully qualified Deploy Quality.
**Feature Changes**

The MME and SGSN now support the UDPC2 hardware. The maximum number of MME managers supported per chassis on ASR 5500 with DPC is 24, to support UDPC2 on ASR 5500 the maximum number of MME managers have been increased to 36. The CLI command `task facility mmemgr per-sesscard-density { high | normal }` under the Global configuration mode is used to configure the density (number of MME managers) of MME managers per session card. The disadvantage of this command is it does not allow configuration of specific number of MME managers per card, but allows the operator to configure only high or normal density. This CLI is deprecated and new CLI commands are introduced to provide the operator with more flexibility to configure number of MME managers per active session cards (or per active session VM in case of VPC) and the total number of MME managers. The MME managers are now moved to Non-Demux card, therefore the number of managers depends on the number of session cards per chassis. The new CLI command enables the operator to spawn the maximum or desired number of MME managers even when the chassis is not fully loaded in the case of ASR 5K and ASR 5500 platforms. For VPC D1 the operator can restrict max number of MME managers per chassis, if operator desires to scale with more session VMs without requiring additional MME managers.

In UDPC2, the number of Session Managers in ASR5500 is increased from 336 to 1008.

**Note**
The StarOS does not support an ASR5500 deployment with mixed usage of DPC and DPC2 cards. All session cards in one ASR5500 have to be of the same type.

**Note**
All product specific limits, capacity and performance, will remain same as compared to ASR5500 with DPC.

**Command Changes**

`task facility mmemgr per-sesscard-density { high | normal }`

This CLI command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid till release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command `task facility mmemgr per-sesscard-count count`.

`configure`

`task facility mmemgr per-sesscard-density { high | normal }`

`exit`

Notes:

- This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.
- New commands are introduced to provide more flexibility to the operator to configure required number of MME managers per session card and to configure the desired number of MME managers per chassis.
task facility mmemgr per-sesscard-count

This CLI command is introduced to configure the desired number of MME managers per session card.

configure
  task facility mmemgr per-sesscard-count count
  default task facility mmemgr per-sesscard-count
  exit

Notes:

- The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to 6.

- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.

- This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.

- The keyword default resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured default number of MME managers per session card will be selected based on platform and card type. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>4</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>6</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>1</td>
</tr>
</tbody>
</table>

- The keyword per-sesscard-count count is used to set the maximum number of MME managers per session card.
  - The value of count is an integer with range 1 up to 6.

Listed below is the maximum number of MME managers allowed per session card based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>2</td>
</tr>
</tbody>
</table>
### Platform/VM and card type

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 5500 DPC</td>
<td>6</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>6</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>2</td>
</tr>
</tbody>
</table>

---

**task facility mmemgr max**

This CLI command is introduced to configure the desired number of MME managers per chassis.

**configure**

```bash
task facility mmemgr max value
default task facility mmemgr max
exit
```

**Notes:**

- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.

- The maximum number of MME managers that can be configured per chassis varies based on the platform. However, the upper limit of MME managers per chassis is set to 36.

- This CLI is not configured by default. The keyword `default` resets the number of MME managers per chassis to the default values. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>36</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>1</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
</tbody>
</table>

- The keyword `max value` is used to set the maximum number of MME managers per chassis.
  - The maximum value is an integer with range 1 up to 36.
Listed below is the maximum number of MME managers allowed per chassis based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>36</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
</tbody>
</table>

**MME Enhancements for 19.0**

This section identifies all of the MME enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your MME.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
• System and Platform Enhancements

**Cause Code Mapping of ESM #66 by SGSN and MME**

CSCut50598 - 3GPP 24.301 R11 new cause code '#66'

**Feature Changes**

This feature is developed to achieve compliance with Release 11 3GPP Technical Specifications. The Release 11 3GPP Technical Specification introduced a new ESM/SM cause code 'Requested APN not supported in current RAT and PLMN combination (cause code #66)'. This ESM/SM cause is used by the network to indicate that the procedure requested by the UE is rejected as the requested APN is not supported in the current RAT and PLMN. A UE which receives this cause will stop accessing the APN in the current RAT, but as soon as it enters another RAT type it will retry the APN.

In earlier releases only cause code #27 and cause code #33 were supported, these codes were not very effective in restricting APN in a particular RAT. For example, UE which has received cause #27 (with timer = 24 hours) will stop retrying a PDN connection in every RAT for 24 hours. This is not the desired behavior in some cases APN cannot be restricted in a particular RAT. If the SGSN sends cause code #33 to the UE for an IMS APN, the UE/MS stops retrying the PDN connection for some time, but UE/MS will not automatically retry this APN in 4G, even though the APN is available there. The introduction of cause code #66 resolves this issue as the operator can block access to IMS APN in 2G/3G and can allow access in 4G.

---

**Note**

This feature is applicable for both SGSN and MME.

---

**Important**

This is a 3GPP Release 11 compliance feature and will be applicable only to UEs capable of decoding ESM/SM cause code 66.

---

**Command Changes**

**restrict access-type**

The *restrict access-type* command under the APN profile configuration mode is used to configure PDP activation restriction on the basis of access type. A new command option *eps* for EPS networks is introduced for this feature. In earlier releases this command was supported only for GPRS and UMTS networks to perform QoS related restrictions. Now this command is also used to configure the APN not supported in particular RAT and PLMN combinations. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

```plaintext
configure

apn-profile <profile_name>

    [ no ] restrict access-type { eps | { { gprs | umts } | qos-class { background | conversational | interactive | streaming } } ]
```

---

**Release Change Reference, StarOS Release 19**

217
default restrict access-type { eps | gprs | umts }
end

Notes:
- This command is disabled by default.
- In earlier releases this command was applicable only for SGSN. It is now supported by MME also.
- If the operator does not include the optional QoS-Class keyword option, then complete APN restriction is enabled and QoS related restrictions have no impact as QoS restriction is a subset of a complete APN restriction.

local-cause-code-mapping apn-not-supported-in-plmn-rat

This command remaps the EMM/ESM/SM cause codes to operator-preferred codes in the Call Control Profile. These replacements codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

configure
call-control-profile profile_name
    local-cause-code-mapping apn-not-supported-in-plmn-rat { emm-cause-code emm_cause_number 
esm-cause-code esm_cause_number | attach | [ tau ] } | esm-cause-code esm_cause_number esm-proc | 
sm-cause-code sm_cause_number }
    remove local-cause-code-mapping apn-not-supported-in-plmn-rat | attach | esm-proc | 
sm-cause-code | tau |
end

Notes:
- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies that the configuration maps operator-preferred replacement cause codes when a call is rejected because the requested APN is not supported in current RAT and PLMN combination.

- **emm-cause-code emm_cause_number esm-cause-code esm_cause_number | attach | [ tau ]**
  - The keyword **emm-cause-code** configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.
    * **emm_cause_number** specifies the EMM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 2 through 111.
    * **esm-cause-code** configures the operator preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.
    * **esm_cause_number** specifies the ESM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 8 through 112.
    * The **attach** keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.
    * The **tau** keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

- **esm-cause-code esm_cause_number esm-proc**
*esm-cause-code* configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

*esm_cause_number* specifies the ESM cause code replacement integer in the range 0 through 255.

* The *esm-proc* keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

• **sm-cause-code** *sm_cause_number* specifies the SM cause code replacement value and this keyword is only for the SGSN's call control profile.

**local-cause-code-mapping apn-not-supported-in-plmn-rat**

This command remaps use of the 3GPP Release 11 rejection code #66 to the EMM/ESM cause codes preferred by the operator and records the remapping in the MME service configuration. These replacement codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

```
configure
  context context_name
  mme-service service_name
    local-cause-code-mapping apn-not-supported-in-plmn-rat { emm-cause-code
      emm_cause_number esm-cause-code esm_cause_number [ attach ] [ tau ] } | ems_cause_number esm-proc
    default local-cause-code-mapping apn-not-supported-in-plmn-rat [ attach ] esm-proc [ tau ]
  end
```

Notes:

• The keyword **apn-not-supported-in-plmn-rat** specifies that the cause codes to be used for a rejection due to the requested APN not being supported in the current RAT and PLMN combination are those that are mapped in the MME service configuration.

• **emm-cause-code** *emm_cause_number esm-cause-code esm_cause_number [ attach ] [ tau ]*

  * The keyword **emm-cause-code** configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.

  * *emm_cause_number* specifies the EMM code replacement integer in the range 0 through 255.

  * **esm-cause-code** configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.

  * *esm_cause_number* specifies the ESM code replacement integer in the range 0 through 255.

  * The **attach** keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.

  * The **tau** keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

• **esm-cause-code** *esm_cause_number esm-proc*
* **esm-cause-code** configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

* **esm_cause_number** specifies the ESM cause code replacement integer in the range 0 through 255.

* The **esm-proc** keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

**Performance Indicator Changes**

**MME Schema**

The following new statistics have been added to the MME schema to track MME support of the 3GPP Release 11 code for call rejections due to the APN not being supported under the PLMN / RAT combination:

- inter-node-srns-proc-fail-apn-not-supported
- inter-node-tau-proc-fail-apn-not-supported
- tai-esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- tai-epm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- attach-proc-fail-apn-not-sup-in-plmn-rat
- esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- epm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- emmdisc-apnnotsupinplmnrat

For descriptions of these variables, see *MME Schema Statistics* in the *Statistics and Counters Reference*.

**show configuration**

The following new parameters have been added to the show configuration command for this feature:

- restrict access-type umts/gprs/eps
- local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code <cause_number>
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code <cause_number> esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 32 esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 15 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau
show apn-profile full

The following new parameters have been added to the show apn-profile command for this feature:

- Service Restriction for Access Type UMTS
- Complete APN restricted
- Service Restriction for Access Type GPRS
- Complete APN restricted
- Service Restriction for Access Type EPS

show call-control-profile full

The following new parameters have been added to the show call-control-profile command for this feature:

- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination
- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Requested service option not subscribed (33)
- Cause Code Mapping
- APN not supported PLMN-RAT esm-proc: Operator Determined Barring (esm-8)
- APN not supported PLMN-RAT Attach: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT TAU: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)

show gmm-sm statistics verbose

The following new parameters are added to this show command to display the statistics for this feature:

- 3G-Pri-Actv-APN-Not-Sup-Rej
- 2G-Pri-Actv-APN-Not-Sup-Rej
- 3G-APN-Not-Supported-in-PLMN-RAT
- 2G-APN-Not-Supported-in-PLMN-RAT
- APN Not Supported in PLMN RAT combination Statistics
- 3G-Pdp-Dropped-During-New-SGSN-RAU
- 2G-Pdp-Dropped-During-New-SGSN-RAU
- 3G-Pdp-Dropped-During-New-SGSN-SRNS
- Pdp-Dropped-During-3G-To-2G-IRAT
- 3G-Actv-NRPCA-Reject
- Pdp-Dropped-During-2G-To-3G-IRAT
- APN not sup PLMN-RAT
Inbound Inter node SRNS failure
APN not sup in PLMN/RAT

**show mme-service name**

The following new parameters are added to this show command to display the statistics for this feature:

- APN not supported PLMN-RAT esm-proc: Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT Attach: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT TAU: No Suitable Cells In tracking area (emm-15)

**CSFB for 1xRTT**

CSCuu36311, CSCup66691, CSCuq25983 - eCSFB support for CDMA Network

**Feature Changes**

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This functionality is released as Deploy Quality. This feature is license-controlled and the commands to configure and manage the feature interfaces require a feature license key. Speak with your Cisco Representative for information about this license.</td>
</tr>
</tbody>
</table>

With this release, the MME expands support of circuit-switched fall back (CSFB) to enhanced circuit-switched fall back (CSFB) for CDMA 1x (single-carrier) radio transmission technology (1x-RTT) networks. The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWF/MSC to support the following CS services:

- MO/MT Voice calls
- MO/MT SMS
- Emergency calls

**Command Changes**

If you have a license, the following new or modified commands should be visible to you in this release.

- **s102-service**

  The S102 Service configuration enables you to create an instance of the S102 service and within that service to define the characteristics for a specific S102 interface, including:

  - configuring the interface to work with CSFB for the 1xRTT CDMA2000 messaging.
  - binding or unbinding a logical IPv4 address and ports to the S102 service.
• configuring an IPv4 address and ports for the IWS/MSC in the S102 service configuration.

```plaintext
config
ccontext context_name
 | no | s102-service service_name
 | no | 1xRTT csfb
 | no | bind ipv4-address ipv4_address port port_number
 | no | msc msc_name
 | no | ipv4-address ipv4_address port port_number
exit
non-pool-area non_pool_area_name msc msc_name msc-id msc_id cell-id cell_id +
no non-pool-area non_pool_area_name cell-id cell_id +
 | no | pool-area pool_area_name
 | no | cell-id cell-id
 | no | hash-value { hash_value | non-configured-values | range lower_hash_value to higher_hash_value } { msc msc_name }
 | no | msc-id msc-id
exit
end
```

Notes:

• `context_name` enter a string of 1 to 79 alphanumeric characters to define the name of the context in which the S102 service is configured. You can configure the S102 service in the same context in which the associated MME service is configured.

• `service_name` enter a string of 1 to 63 alphanumeric characters to define the name. We recommend that each service name be unique on this MME.

• The MME supports configuration of an undefined number of S102 services (interfaces). As there is a 1-to-1 correlation between S102 service configurations and MME services, the only limiting factor is the maximum number of MME services that can be configured per system; maximum number is 8.

• `1xrtt` configures the S102 interface to provide either CSFB or SRVCC capabilities for the 1xRTT CDMA2000 network. The 1xrtt command can be repeated so that a single S102 interface provides both CSFB and SRVCC functionality.

• `bind ipv4-address ipv4_address port port_number` binds the S102 interface to the specified source (MME) IPv4 interface address, and optionally to a specific port number if the port option is included. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.

• `msc msc_name` enter 1 to 63 alphanumeric characters to define a unique name for the MSC. Executing the msc command causes the system to enter the S102-MSC configuration mode to define the target IPv4 address (and optionally the port ID). This associates the S102 interface to the specified MSC.

• `ipv4-address ipv4_address port port_number` identifies IPv4 interface address of the MSC, and optionally a specific port number if the port option is included. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.

• It is possible to associate up to 10 IWS/MSCs with the S102 interface/service configuration. Repeat the `msc`, `ipv4-address`, and `exit` commands sequence as often as needed to identify all MSCs.

• `non_pool_area_name` enter a string of 1 to 63 alphanumeric characters to uniquely identify the non-pool-area definition used for MSC selection (for details on this function, refer to the CSFB for 1xRTT section of the MME Administration Guide).
• `msc msc_name` enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.

• `msc-id msc_id cell-id cell_id +`
  * `msc_id` enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
  * `cell_id` enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this non-pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.

• `plmnid { any | mcc mcc_id mnc mnc_id }` is not operationally supported at this time. The code is included for future development.

• `pool-area pool_area_name` enter a string of 1 through 63 alphanumeric characters to create a unique name of an MSC pool area configuration. After the command is entered, the system enters the S102-Pool-Area configuration mode.

• `cell-id cell-id [cell-id + ]` enter an integer from 1 through 65535 to identify a CDMA2000 reference cell ID that you are assigning to this pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.

• `hash-value`
  * `hash_value` enter an integer from 0 through 999 to identify a specific MSC.
  * `non-configured-values msc msc_name` assigns all non-configured hash values to use the named MSC.
  * `range lower_hash_value to higher_hash_value msc msc_name` specifies the range of hash values for an MSC:
    * `lower_hash_value` enter an integer from 0 through 999 to identify the start value for a range of hash. The `lower_hash_value` must be lower than the `higher_hash_value`.
    * `higher_hash_value` enter an integer from 0 through 999 to identify the end value for a range of hash. The `higher_hash_value` must be higher than the `lower_hash_value`.

• `msc_id` enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.

• `plmnid { any | mcc mcc_id mnc mnc_id }` is not operationally supported at this time. The code is included for future development.

• `no` prefix included with a command, disables and/or erases the specified configuration from the MME’s configuration.

• `default` prefix is unused at this time and is available for future development.

• Use the `show s102-service name s102_service_name` command to verify the S102 configuration that you have entered following the steps outlined above.

• Use the `show configuration` command to view the S102 pool area and S102 non-pool area configuration.
mme-service

Use the following to add an association between a previously configured MME service and an S102 service.

```plaintext
config
  context context_name
  mme-service mme_service_name
  associate s102-service s102_service_name [ context context_name ]
end
```

Notes:

- `context context_name` enter a string of 1 to 79 alphanumeric characters to identify the name of the context in which the S102 service is configured. We recommend that you identify the context if it is not the same one in which the associated MME service is configured.
- Use the `show mme-service name mme_service_name` command to verify the S102 association that you have entered following the steps outlined above.

Performance Indicator Changes

MME Schema

At the MME level, the MME tracks the number of CSFB 1xRTT calls using the following variables:

- `s1ap-transdata-dlinktunnel`
- `s1ap-recdata-ulinktunnel`

S102 Schema

This new schema includes the following variables:

- `vpname`
- `vpnid`
- `servname`
- `servid`
- `s102ap-tx-a21-air-signal-msg`
- `s102ap-tx-a21-ack-msg`
- `s102ap-tx-a21-evtnfy-msg`
- `s102ap-tx-unknown-msg`
- `s102ap-rex-a21-air-signal-msg`
- `s102ap-rex-a21-ack-msg`
- `s102ap-rex-a21-evtnfy-msg`
- `s102ap-rex-unknown-msg`
- `s102ap-rx-a21-air-signal-msg`
• s102ap-rx-a21-ack-msg
• s102ap-rx-a21-evnt-ntfy-msg
• s102ap-rx-unknown-msg
• s102ap-encode-errors
• s102ap-missing-mandatory-ies
• s102ap-corelation-mismatch
• s102ap-decode-errors
• s102ap-syntax-errors
• s102ap-misc-errors

Traps

Traps are defined to indicate when an S102 service starts or stops. The trap information includes the context identification in which the S102 service is configured the unique identification of the S102 service. The following are examples of how the traps would appear:

Internal trap notification <XXXX> (S102ServiceStop) context S102 service s102-service
Internal trap notification <YYYY> (S102ServiceStart) context S102 service s102-service

DDN Throttling

CSCut42662 - MME Support for DDN Throttling

Feature Changes

Important

A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

In this feature, MME is provisioned to reject non-priority (traffic based on ARP and LAPI) Downlink Data Notification (DDN) requests when the UE is in idle mode. Additionally, MME dynamically requests S-GW to reduce the number of DDN requests based on a throttling factor and a throttling delay specified in the DDN Ack message.

Previous Behavior: In earlier releases, rejection was supported in the Congestion Action Profile only for a few procedures such as: ps-attach, handovers and so on. The command reject was implemented for rejection.

New Behavior: From 19.0 onwards, rejection is also supported for Download Data Notification (DDN) procedure, in the Congestion Action Profile. Rejection for DDN is configured using the existing CLI command along with new parameters such as LAPI, ARP and Cause values.
Command Changes

reject

The **ddn** is a newly added keyword to this command. This keyword allows the operator to reject DDN requests during congestion. The operator can reject DDN requests based on ARP or LAPI values or both. An option is provided to reject all DDN requests without using ARP/LAPI values.

```
configure
  lte-policy
    congestion-action-profile profile_name
      reject ddn [ arp-watermark arp_value | lapi ] [ cause cause_value ]
      none ddn [ lapi | arp-watermark ]
    end
```

Notes:

- The **ddn** keyword configures action to be taken for all DDN requests
- The **lapi** keyword indicates that DDN reject is applicable for UEs with LAPI.
- The **arp-watermark** keyword indicates that DDN reject is applicable for ARP values greater than or equal to the ARP specified. The ARP value ranges from 1 through 15.
- The **cause** keyword rejects DDN with the specified cause value. The valid cause value ranges from 1 through 255. The default value is 90 with the display message 'Unable to page ue'.
- **none** disables DDN configuration.

---

**Important**

If the value of arp-watermark does not match with the DDN's arp value, then the DDN will not be rejected and all bearers will remain active.

ddn sgw-throttling

The **sgw-throttling**, **throttle factor** and **delay** are new keywords added to this command in this release. This Command allows the operator to configure the throttling factor and throttling delay values to be sent in DDN Ack message.

```
configure
  lte-policy
    congestion-action-profile profile_name
      ddn sgw-throttling throttle-factor percentage_value delay delay_time
      no ddn sgw-throttling
    end
```

Notes:

- Throttling delay value will be converted internally to seconds, minutes or hours as defined in the 3gpp Spec 29.274.
• The `sgw-throttling` keyword enables DDN throttling towards SGW.
• The `throttle-factor` keyword indicates throttling factor as a percentage from 1 to 100.
• The `delay` keyword indicates the amount of time taken for throttling delay in seconds. The delay value ranges from 2 to 1116000 seconds.
• `no` removes DDN throttling towards SGW.

**Performance Indicator Changes**

`show lte-policy congestion-action-profile name <profile_name>`

This command displays the following new fields in the Congestion Action Profile for this feature:

- `none ddn`
- `ddn sgw-throttling throttle-factor delay`

`show congestion-control statistics mme critical`

The below given counters are added in the Congestion Action Profile test, they are displayed on executing this show command.

- DDN Request
- Rejected:
  - ARP-Based
  - LAPI-Based

`show congestion-control statistics mme major`

The below given counters are added in the Congestion Action Profile test, they are displayed on executing this show command.

- DDN Request
- Rejected:
  - ARP-Based
  - LAPI-Based

`show congestion-control statistics mme minor`

The below given counters are added in the Congestion Action Profile test, they are displayed on executing this show command.

- DDN Request
- Rejected:
**show congestion-control statistics mme full**

The below given counters are added in the Congestion Action Profile test, they are displayed on executing this how command.

- DDN Request
- Rejected:
  - ARP-Based
  - LAPI-Based

---

**Enhanced Multimedia Broadcast Multicast Services**

CSCut39580 - eMBMS M3 and Sm interfaces

**Feature Changes**

<table>
<thead>
<tr>
<th>Important</th>
<th>This feature is currently supported as lab quality only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
<td>A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.</td>
</tr>
</tbody>
</table>

In an LTE network, the operator can provide an Multimedia Broadcast Multicast Services (MBMS) data service using the e-MBMS solution proposed in 3GPP TS 23.246. The e-MBMS solution includes involvement of the following nodes:

- MBMS manager – Schedules the MBMS session, identifies the service area to be served and triggers the setting up of the MBMS session by informing the BM-SC
- BM-SC – Sets up the e-MBMS session. Initiates delivery of the content by pulling it from the content server. Uses appropriate CODEC on the content. Collects the reception receipt from the UEs for certain kinds of content.
- MBMS-GW – Creates MBMS bearer, allocated a multicast transport address and performs the GTP-U encapsulation of the MBMS data.
- MME – Sets up a bearer and supports the e-MBMS session setup/teardown.
- eNodeB/MCE – Involved in session setup and broadcasting of MBMS data on the broadcast channel on the air.

When this new functionality is fully implemented, it will include support for two new interfaces:
• the Sm interface between the MME and the MBMS GW
• the M3 interface providing the reference point for the control plane between the MME and the E-UTRAN

Command Changes

mme-embms-service

The new `mme-embms-service` command creates an e-MBMS service configuration for the MME in a new configuration mode that includes the following commands:

• `associate`
• `bind`
• `mmemgr-recovery`
• `plmn-id`
• `sctp`
• `setup-timeout`

Performance Indicator Changes

show mme-embms-service

The following show command is new in support of the MME’s implementation of e-MBMS:

• `show mme-embms-service { all | m3ap statistics | mce-association { all | name | path-info [ all | mme-embms-service ] <mme_embms_service_name> }

GUTI Re-allocation

CSCut09240 - MME Support for GUTI Re-allocation

Feature Description

Overview

The Globally Unique Temporary Identity (GUTI) is assigned to the UE by the MME the GUTI is used to support subscriber identity confidentiality. The GUTI has two parts, the Globally Unique Mobility Management Entity Identifier (GUMMEI), which identifies the network, and the M-TMSI, which identifies the device. This feature enables GUTI Re-allocation for an UE based on time and frequency of access attempts per UE.
How It Works

The MME currently performs GUTI allocation during UE attaches. The GUTI once allocated is retained until the DB associated with the UE is purged. This feature introduces MME support to perform GUTI Reallocation for securing the TMSI allocated to UE. GUTI Reallocation is triggered based on configured frequency of access attempts or periodicity.

A configured frequency of "n" requests triggers GUTI Reallocation for every "nth" ATTACH / TAU / SERVICE REQUEST received from the UE. Here 'n' is the sum of the received ATTACH / TAU/ SERVICE Request. A configured periodicity of "t" minutes triggers GUTI Reallocation at every "t" minutes for a UE.

The frequency-based GUTI reallocation is independent of the configured periodicity. However, periodicity-based GUTI reallocation attempts are relative to the last attempted UE GUTI Reallocation time. The last attempted GUTI Reallocation time for a UE is updated whenever a GUTI Reallocation for a UE is attempted irrespective of the trigger (frequency/periodicity).

The MME initiates GUTI Reallocation only if the NAS signaling connection with the UE is present. If the NAS signaling connection is not present the UE shall not be paged. If the NAS signaling connection with the UE is absent, GUTI reallocation is performed whenever the NAS signaling connection with the UE is established.

Note

GUTI Reallocation is not triggered when UE is always in connected mode as, GUTI Reallocation based on periodicity is performed only when the either Attach, periodic TAU, Service request is received by MME and the configured periodicity time has been reached. For a UE that is always in connected mode neither of these events occur. The session are not disturbed during GUTI Reallocation, idle-active transitions are a frequent occurrence in the network, therefore GUTI Reallocation should happen for most UE's at the configured periodicity/frequency during service request procedure.

The Reallocated GUTI is sent in the NAS Attach Accept, NAS TAU Accept and NAS GUTI Relocation Command messages.

Limitations

The MME does not perform GUTI Reallocation if the subscriber is marked for offload or if the subscriber is executing an outbound handover procedure.

The GUTI reallocation retries for UE’s which do not adhere to specifications is limited by the MME. MME detaches such UEs after "10" consecutive failure attempts of GUTI Reallocation. This behavior and number of consecutive failures to trigger detach is not configurable.

The frequency and periodicity configured to trigger authentication/GUTI reallocation requires the new session setup message (NAS Attach/TAU) to be processed by the Session Manager instance which has the corresponding MME DB for the subscriber. If the MME DB is not available the frequency and periodicity triggers will not work. For example, if the mobile identifier in the NAS Attach/TAU message is a foreign GUTI and additional GUTI is not present, the MME does not trigger authentication/GUTI reallocation for the subscriber based on frequency/periodicity.

Reallocated GUTI is not sent in TAU accept for TAU with type TA Update. In this scenario, once the frequency criteria for TAU is met, GUTI reallocation is performed on receiving the next periodic TAU or Service request. This to prevent the case where, TAU complete for an TAU accept with Reallocated GUTI is not received by MME. Wherein upon receiving a paging trigger, MME needs to page the UE in both the TAI lists (before and after TAU) with both the GUTI (previous and reallocated). In the case of SGSN, paging message is sent to...
the RNC with acknowledged PTMSI and unacknowledged (reallocated) PTMSI. However paging is sent only for the current RAI. Similarly in the case of MME, MME has to send paging message to the eNodeB’s with acknowledged GUTI and unacknowledged GUTI (reallocated). But paging needs to be sent in both current TAI list and previous TAI list.

**Flows**

The following diagram illustrates the messages exchanged during network-initiated GUTI re-allocation:

*Figure 1: GUTI Re-allocation*

1. The MME sends GUTI REALLOCATION COMMAND message to the UE. The time duration for the T3450 timer starts. This timer starts when the MME initiates a Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.
2. The UE sends a GUTI REALLOCATION COMPLETE message to the MME on completion of the GUTI Re-allocation procedure. The T3450 timer stops once the MME receives the GUTI REALLOCATION COMPLETE message.

**Configuring GUTI Re-allocation**

The following configuration command is used to configure the periodicity (time interval) / frequency of GUTI Reallocation for a UE:

```
config call-control-profile <profile_name>
    [ remove ] guti reallocation [ frequency <frequency> | periodicity <duration> ]
end
```

Notes:

- The keyword **guti** identifies the Globally Unique Temporary UE Identity (GUTI).
- The keyword **reallocation** specifies reallocation of GUTI.
- The **frequency** configured specifies the GUTI reallocation frequency. The frequency is an integer with a range "1" up to "65535" requests.
- The **periodicity** configured specifies GUTI reallocation periodicity. The periodicity is an integer with a range "1" up to "65535" minutes.
- GUTI reallocation is disabled by default. The **remove** keyword is used to remove the configured GUTI reallocation frequency and periodicity specified in the call control profile configuration.
Monitoring and Troubleshooting GUTI Re-allocation

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

GUTI Re-allocation Show Command(s) and/or Outputs

show call-control-profile full all

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- GUTI Reallocation
- GUTI Reallocation Frequency
- GUTI Reallocation Periodicity

show session disconnect-reasons verbose

The following new disconnect reason is added for GUTI Reallocation:

- mme-guti_realloc_failed-detach

show mme-service statistics

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- GUTI Reallocation
- Attempted
- Failures
- Success
- GUTI Reallocation
- Attach Accept
- Retransmission
- TAU Accept
- Retransmission
- GUTI Reallocation cmd
- Retransmission

Below is an example displaying the EMM Statistics listed above:

EMM Statistics:

GUTI Reallocation:
Attempted : 176807
Success : 176691
Failures : 116

Below is an example displaying the Total EMM Control Messages listed above:

Total EMM Control Messages:

GUTI Reallocation:
Attach Accept: 180094 Retransmissions: 0
show mme-service db record all

The following new field is added to the show output to display the configured GUTI Reallocation parameters:

- REALLOCATED GUTI

show mme-service db record imsi

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- REALLOCATED GUTI
- PLMN
- MME Group ID
- MME Code
- M-TMSI
- GUTI Allocated time

Below is an example displaying the statistics listed above:

```
show mme-service db record imsi 123456710100158
Friday September 18 09:25:19 EDT 2015
DB RECORD
==========
Sessmgr Instance : 1
Imsimgr Instance : 1
MME Service : mmesvc
Lookup Keys
---------
IMSI : 123456710100158
Service-id : 7
GUTI
  PLMN : 123456
  MME Group ID : 32777
  MME Code : 2
  M-TMSI : 3221491713
REALLOCATED GUTI
  PLMN : 123456
  MME Group ID : 32777
  MME Code : 2
  M-TMSI : 3221491713
GUTI Allocated time : Fri Sep 18 08:29:16 2015
```

GUTI Re-allocation Bulk Statistics

The following bulk statistics are included in the MME Schema in support of this feature:

The following bulk statistics are included in the MME Schema in support of this feature:

- emm-msgtx-guti-reallocation
- emm-msgtx-guti-reallocation-retx
- emm-msgtx-guti-realloc-attach-accept
- emm-msgtx-guti-realloc-attach-accept-retx
• emm-msgtx-guti-realloc-tau-accept
• emm-msgtx-guti-realloc-tau-accept-retx
• guti-reallocation-attempted
• guti-reallocation-success
• guti-reallocation-failure

For descriptions of these variables, see "MME Schema Statistics" in the Statistics and Counters Reference.

HSS-based P-CSCF Restoration

CSCut99396 - PCSCF restoration support in MME

Feature Changes

Important
A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

The HSS-based P-CSCF Restoration is an optional mechanism during a P-CSCF failure. It applies only when the UE is using 3GPP access technologies. The P-CSCF restoration is possible if there are no other registration flows available for the terminating UE using an available P-CSCF.

The HSS-based P-CSCF restoration consists of a basic mechanism that makes use of a path through HSS and MME/SGSN to request the release of the IMS PDN connection to the corresponding UE, and an optional extension that avoids the IMS PDN deactivation and re-activation.

Previous Behavior: HSS-based P-CSCF Restoration was not supported.

New Behavior: In this release, MME is upgraded to implement HSS-based P-CSCF Restoration as an optional mechanism during P-CSCF failure.

Customer Impact: The HSS-based P-CSCF Restoration feature aids in successful establishment of MT VoLTE calls when the serving P-CSCF is unreachable.

Command Changes

pcsf-restoration

apn-type ims

The pcsf-restoration is a newly added command to enable HSS-based P-CSCF Restoration.

The following CLI configuration enables/disables support for HSS initiated P-CSCF restoration in the Call Control Profile mode.

configure
call-control-profile profile_name
  | remove | pcsf-restoration
end

Notes:
- The `pcscf-restoration` command in the above configuration enables HSS-based P-CSCF restoration. When enabled, MME supports P-CSCF Restoration on the S6a interface towards HSS for IMS PDN.

- The `remove` keyword disables HSS-based P-CSCF Restoration in the MME.

- By default, the above configuration is disabled.

- To select the method for P-CSCF Restoration, use the `pcscf-restoration` keyword in `apn-type ims` command under APN Profile Configuration mode.

The `apn-type ims` command identifies APN as IMS APN, and indicate whether the PGW supports optional extension or MME initiates PDN deactivation for HSS initiated P-CSCF restoration.

The `pcscf-restoration { pco-update | pdn-deactivate }` keywords are newly introduced for this command to select the method for P-CSCF Restoration. The P-CSCF Restoration method is configured under the APN Profile Configuration mode.

```
configure
  apn-profile profile_name
    apn-type ims [ pcscf-restoration { pco-update | pdn-deactivate } ]
  end
```

Notes:

- The `apn-type ims` command for MME identifies the type of APN. If an IMS APN is present, the Modify Bearer Request will be delayed during Inbound SRNS relocation.

- The `pcscf-restoration` keyword identifies P-CSCF restoration for IMS PDN. This keyword is functional only if the feature license is installed.

- The `pco-update` keyword selects P-CSCF restoration method as PDN Modification through PCO update.

- The `pdn-deactivate` keyword selects P-CSCF restoration method as PDN Deactivation.

- To enable HSS-based P-CSCF Restoration, use the `pcscf-restoration` command under the Call Control Profile mode.

---

**Important**

If only 'apn-type ims' is configured then default P-CSCF restoration method 'pdn-deactivate' is enabled.

---

**Performance Indicator Changes**

**show call-control-profile full all**

The following new field is added to the output of this command for this feature:

- P-CSCF Restoration

**show apn-profile full all**

The following new field is added to the output of this command for this feature:

- PCSCF Restoration Type
show mme-service statistics
The following new fields are added to the output of this command for this feature:

- HSS P-CSCF Restoration
- PDN Deactivation
- PDN Modification

Local Emergency Numbers List

CSCtw98505 - MME Support for Local Emergency Numbers List download to the UE

Feature Changes

Important
A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

Local Emergency Numbers List contains a list of emergency numbers that a caller uses to contact emergency services for assistance. It contains additional emergency numbers used by the serving network. This list can be downloaded by the network to the User Equipment (UE) at successful registration and subsequent registration updates.

Previous Behavior: Local Emergency Number List IE was not supported in Attach Accept and TAU Accept messages.

New Behavior: From 19.0 release onwards, the Local Emergency Number List IE is supported in Attach Accept and TAU Accept messages. A new configuration is added to support Local Emergency Number List.

Customer Impact: Local Emergency Numbers can be downloaded to the UE during Attach and TAU exchanges.

Command Changes

local-emergency-num

The **local-emergency-num** is a new command that is used to configure local emergency numbers to be sent over both Attach and TAU messages.

```plaintext
configure
tlte-policy
  lte-emergency-profile profile_name
    [ no ] local-emergency-num emergency_number { ambulance | custom custom_name | fire | marine-gaurd | mountain-rescue | police }
end
```
local-emergency-num-ie

The **local-emergency-num-ie** is a new command that is used to configure local emergency numbers to be sent only over TAU messages.

```plaintext
configure
  lte-policy
    lte-emergency-profile profile_name
      local-emergency-num-ie { inter-mme-tau | tau }
      no local-emergency-num-ie
    end
end
```

Notes:

- The **local-emergency-num** keyword configures the Local Emergency Numbers to be sent in Attach or TAU responses.
- The **no** command prefix removes the configured Local Emergency Numbers from the list. Only one local emergency number is removed for a single instance of the **no** prefix.
- `custom_number` is specific to the **custom** local emergency number. `custom_number` is an hexadecimal number from 0x1 to 0xFF
- The **local-emergency-num-ie** keyword with the **inter-mme-tau** option allows the configured local emergency number list to be sent in a TAU Accept during Inter-MME-TAUs, that is, when the UE switches from a 2G network to 4G network, from a 3G network to 4G network or from a 4G network to 4G network handover (for both idle and connected mode).
- The **local-emergency-num-ie** keyword with the **tau** option allows the configured local emergency number list to be sent in a TAU Accept message during all TAU (for example, periodic TAUs and so on).
- The **no** keyword removes its following options in the **local-emergency-num-ie** configuration.

**Performance Indicator Changes**

```plaintext
show lte-policy lte-emergency-profile
```

The following new fields are added to the output of this command for this feature.

- local-emergency-num 123 fire
- local-emergency-num 112 police
- local-emergency-num 110 ambulance
- local-emergency-num 118 custom 0x1f
- local-emergency-num-ie inter-mme-tau

**Selective Authentication**

CSCut09240 - Selective Authentication in MME
Feature Changes

The MME performs UE authentication on receiving NAS requests. Authentication procedures can be defined for Attach procedures, Service requests and Tracking Area Update (TAU) procedures. These authentication procedures increase signaling towards the RAN and HSS. Selective Authentication is adopted to reduce signaling traffic towards the RAN and HSS. Selective Authentication is achieved by implementing frequency and periodicity based authentication of UE.

In a frequency-based selective authentication scenario the UE is authenticated based on configured frequency of access attempts. The configured frequency specifies the access-attempts per-UE and not across UEs. For example if the configured frequency is "n", the UE is authenticated for every nth NAS request received. The decision to authenticate is based on every nth request and not based on 'n' requests since last authentication. Where the nth request is equal to a multiple of n. (for example if n = 2, it will be 2,4,6,8 and so on)

In a periodicity-based selective authentication scenario the UE is authenticated based on configured periodicity. For example if the configured periodicity is 't', the UE is authenticated at every 't' minutes.

The frequency-based authentication is independent of the configured periodicity. However, periodicity-based authentication attempts are relative to the last UE authentication time. The last UE authentication attempt time is updated whenever an UE authentication is attempted irrespective of the authentication trigger.

Note

The MME does not maintain periodicity and frequency across session recovery.

Note

The frequency and periodicity configured to trigger authentication/GUTI reallocation requires the new session setup message (NAS Attach/TAU) to be processed by the Session Manager instance which has the corresponding MME DB for the subscriber. If the MME DB is not available the frequency and periodicity triggers will not work. For example, if the mobile identifier in the NAS Attach/TAU message is a foreign GUTI and additional GUTI is not present, the MME does not trigger authentication/GUTI reallocation for the subscriber based on frequency/periodicity.

Command Changes

authenticate attach

This command is used to configure the frequency and periodicity for selective UE authentication during Attach Procedures.

configure
call-control-profile profile_name
[remove] authenticate attach [inter-rat] { frequency frequency | periodicity duration }
no authenticate attach
exit

Notes:
• The **frequency** configured specifies the authentication frequency. The frequency is an integer with range '1' up to '16'. If the frequency is set for '12', then the service skips authentication for the first 11 events and authenticates on the twelfth event.

• The **periodicity** configured specifies authentication periodicity. The periodicity is an integer with a range '1' up to '10800' minutes. For example, if the configured periodicity is '20' minutes, the UE is authenticated at every '20' minutes.

• No authentication procedures are defined by default. The `remove` keyword is used to delete the defined authentication procedures for Attach Requests from the call control profile configuration file.

**authenticate tau**

This command is used to configure the frequency and periodicity for selective UE authentication during TAU Procedures.

```
configure
call-control-profile profile_name
    [remove] authenticate tau [ { inter-rat | intra-rat | normal | periodic } ] [ { frequency frequency | periodicity duration } ]
no authenticate tau
exit
```

Notes:

• The keyword **inter-rat** specifies authentication to be applied for Inter-RAT TAU.

• The keyword **intra-rat** specifies authentication to be applied for Intra-RAT TAU.

• The keyword **normal** specifies authentication to be applied for normal (TA/LA update) TAU.

• The keyword **periodic** specifies authentication to be applied for periodic TAU.

• The **frequency** configured specifies the authentication frequency. The frequency is an integer with range '1' up to '16'. If the frequency is set for '12', then the service skips authentication for the first eleven events and authenticates on the twelfth event.

• The **periodicity** configured specifies authentication periodicity. The periodicity is an integer with a range '1' up to '10800' minutes. For example, if the configured periodicity is '20' minutes, the UE is authenticated at every '20' minutes.

• No authentication procedures are defined by default. The `no` keyword disables the TAU authentication procedures specified in the call control profile configuration.

**authenticate all-events**

This command is used to configure the frequency and periodicity for selective UE authentication for all events (Attach/ TAU).

```
configure
call-control-profile profile_name
    [remove] authenticate all-events [ { frequency frequency | periodicity duration } ]
no authenticate all-events
exit
```

Notes:
• The **frequency** configured specifies the authentication frequency. The frequency is an integer with range '1' up to '16'. If the frequency is set for '12', then the service skips authentication for the first eleven events and authenticates on the twelfth event.

• The **periodicity** configured specifies authentication periodicity. The periodicity is an integer with a range '1' up to '10800' minutes. For example, if the configured periodicity is '20' minutes, the UE is authenticated at every '20' minutes.

• No authentication procedures are defined by default. The **remove** keyword is used to delete the defined authentication procedures for all events from the call control profile configuration file.

**authenticate service-request**

This command is used to configure the frequency and periodicity for selective UE authentication for all Service Requests.

```
call-control-profile <profile_name>
[remove] authenticate service-request [service-type { data | page-response | signaling } ] [ { frequency frequency | periodicity duration } ]
no authenticate service-request
exit
```

Notes:

• The keyword **service-type** specifies the service-type classification.

• The keyword **data** specifies service-type for data service requests.

• The keyword **page-response** service-type for service requests in response to paging.

• The keyword **signaling** specifies service-type for service requests due to other signaling.

• The **frequency** configured specifies the authentication frequency. The frequency is an integer with range '1' up to '16'. If the frequency is set for '12', then the service skips authentication for the first eleven events and authenticates on the twelfth event.

• The **periodicity** configured specifies authentication periodicity. The periodicity is an integer with a range '1' up to '10800' minutes. For example, if the configured periodicity is '20' minutes, the UE is authenticated at every '20' minutes.

• No authentication procedures are defined by default. The **remove** keyword is used to delete the Service Request authentication procedures specified in the call control profile configuration.

**Performance Indicator Changes**

**show call-control-profile full all**

The following new fields are added to the show output to display the configured Selective Authentication parameters:

• Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Frequency
• Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Frequency Value
• Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Periodicity
• Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Periodicity Value
• Authentication Attach ANY Frequency
• Authentication Attach ANY (UMTS/GPRS/EUTRAN) Frequency Value
• Authentication Attach ANY Periodicity
• Authentication Attach ANY Periodicity Value
• Authentication Attach Inter-rat ANY (UMTS/GPRS/EUTRAN) Frequency
• Authentication Attach Inter-rat ANY (UMTS/GPRS/EUTRAN) Frequency Value
• Authentication Attach Inter-rat ANY Periodicity
• Authentication Attach Inter-rat ANY Periodicity Value
• Authentication Service Req Frequency
• Authentication Service Req Frequency Value
• Authentication Service Req Periodicity
• Authentication Service Req Periodicity Value
• Authentication Service Req Data Frequency
• Authentication Service Req Data Frequency Value
• Authentication Service Req Data Periodicity
• Authentication Service Req Data Periodicity Value
• Authentication Service Req Signaling Frequency
• Authentication Service Req Signaling Frequency Value
• Authentication Service Req Signaling Periodicity
• Authentication Service Req Signaling Periodicity Value
• Authentication Service Req Page Response Frequency
• Authentication Service Req Page Response Frequency Value
• Authentication Service Req Page Response Periodicity
• Authentication Service Req Page Response Periodicity Value
• Authentication TAU Frequency
• Authentication TAU Frequency Value
• Authentication TAU Periodicity
• Authentication TAU Periodicity Value
• Authentication Inter-RAT TAU Frequency
• Authentication TAU Frequency Value
• Authentication TAU Inter-rat Periodicity
• Authentication TAU Inter-rat Periodicity Value
• Authentication Intra-RAT TAU Frequency
• Authentication Intra-RAT TAU Frequency Value
• Authentication TAU Intra-rat Periodicity
• Authentication TAU Intra-rat Periodicity Value
• Authentication Normal TAU Frequency
• Authentication Normal TAU Frequency Value
• Authentication TAU Normal Periodicity
• Authentication TAU Normal Periodicity Value
• Authentication Periodic TAU Frequency
• Authentication Periodic TAU Frequency Value
• Authentication TAU Periodic Periodicity
• Authentication TAU Periodic Periodicity Value

Single Level Redirection of NAPTR Requests

CSCuo13234 - MME behaviour when receiving NAPTR response with empty flag

Feature Changes

Previously, a roaming network returned an empty flag NAPTR response to a DNS NAPTR request, and the network further requests a NAPTR query to continue the process, this behavior was not supported. The MME behavior is now modified to support empty flag NAPTR requests and to initiate an additional NAPTR query. The Replacement Field information is used to process the additional NAPTR query. If the roaming network still sends an empty flag response, the DNS NAPTR request is rejected.

**Previous Behavior:** The MME rejects additional DNS NAPTR requests on receiving empty flag NAPTR responses.

**New Behavior:** MME is now modified to allow a single level redirection for NAPTR queries. If an empty flag is received in a NAPTR response, MME allows an additional NAPTR query to be processed in the network.

**Customer Impact:** Non-terminal NAPTR response RR will trigger another NAPTR query based on replacement-text provided in the NAPTR response.

SRVCC for 1xRTT

CSCuu36311, CSCuu02102 - SRVCC Implementation for 1XRTT
Feature Changes

Important
This functionality is released as Deploy Quality. This feature is license-controlled and the commands to configure and manage the feature interfaces require a feature license key. Speak with your Cisco Representative for information about this license.

The MME already supports single radio voice call continuity (SRVCC) for UTRAN/GERAN. With this release, the MME has expanded support to enhanced SRVCC (SRVCC) for CDMA 1x (single-carrier) radio transmission technology (1x-RTT) networks.

The primary purpose of SRVCC for 1xRTT is to enable a VoLTE UE to move between LTE and 3G/UMTS or 2G/GSM coverage areas with smooth handovers so that CDMA2000 messages are received from the UE and then relayed to the MSC (or vice-versa) through S1-AP and S102 interfaces.

For complete details about this feature, how it works and how it is managed, refer to the SRVCC for 1xRTT chapter in the MME Administration Guide.

Command Changes

If you have a license, the following new or modified commands should be visible to you in this release.

s102-service

The S102 Service configuration enables you to create an instance of the S102 service and within that service to define the characteristics for a specific S102 interface, including:

• configuring the interface to work with SRVCC for the 1xRTT CDMA2000 messaging.
• binding or unbinding a logical IPv4 address and ports to the S102 service.
• configuring an IPv4 address and ports for the IWS/MSC in the S102 service configuration.

```bash
cfg
  context context_name
    [ no ] s102-service service_name
    [ no ] 1xRTT srvcc
    [ no ] bind ipv4-address ipv4_address port port_number
    [ no ] msc msc_name
    [ no ] ipv4-address ipv4_address port port_number
    exit
    non-pool-area non_pool_area_name msc msc_name msc-id msc_id cell-id cell_id
    +
    no non-pool-area non_pool_area_name cell-id cell_id +
    [ no ] pool-area pool_area_name
    [ no ] cell-id cell-id cell-id
    [ no ] hash-value { hash_value | non-configured-values | range
    lower_hash_value to higher_hash_value } ( msc msc_name )
    [ no ] msc-id msc-id
    exit
  end
```

Notes:
• **context_name** enter a string of 1 to 79 alphanumeric characters to define the name of the context in which the S102 service is configured. You can configure the S102 service in the same context in which the associated MME service is configured.

• **service_name** enter a string of 1 to 63 alphanumeric characters to define the name. We recommend that each service name be unique on this MME.

• The MME supports configuration of an undefined number of S102 services (interfaces). As there is a 1-to-1 correlation between S102 service configurations and MME services, the only limiting factor is the maximum number of MME services that can be configured per system; maximum number is 8.

• **1xrtt** configures the S102 interface to provide either SRVCC or CSFB capabilities for the 1xRTT CDMA2000 network. The 1xrtt command can be repeated so that a single S102 interface provides both CSFB and SRVCC functionality.

• **bind ipv4-address** binds the S102 interface to the specified source (MME) IPv4 interface address, and optionally to a specific port number if the port option is included. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.

• **msc msc_name** enter 1 to 63 alphanumeric characters to define a unique name for the MSC. Executing the msc command causes the system to enter the S102-MSC configuration mode to define the target IPv4 address (and optionally the port ID). This associates the S102 interface to the specified MSC.

• **ipv4-address** identifies IPv4 interface address of the MSC, and optionally a specific port number if the port option is included. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.

• It is possible to associate up to 10 IWS/MSCs with the S102 interface/service configuration. Repeat the **msc, ipv4-address, and exit** commands sequence as often as needed to identify all MSCs.

• **non_pool_area_name** enter a string of 1 to 63 alphanumeric characters to uniquely identify the non-pool-area definition used for MSC selection (for details on this function, refer to the SRVCC for 1xRTT section of the MME Administration Guide).

• **msc msc_name** enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.

• **msc-id msc_id** cell-id cell_id +
  • **msc_id** enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
  • **cell_id** enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this non-pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.

• **plmnid** is not operationally supported at this time. The code is included for future development.

• **pool-area pool_area_name** enter a string of 1 through 63 alphanumeric characters to create a unique name of an MSC pool area configuration. After the command is entered, the system enters the S102-Pool-Area configuration mode.

• **cell-id cell-id** enter an integer from 1 through 65535 to identify a CDMA2000 reference cell ID that you are assigning to this pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.
• hash-value
  * hash_value enter an integer from 0 through 999 to identify a specific MSC.
  * non-configured-values msc msc_name assigns all non-configured hash values to use the named MSC.
  * range lower_hash_value to higher_hash_value msc msc_name specifies the range of hash values for an MSC:
    * lower_hash_value enter an integer from 0 through 999 to identify the start value for a range of hash. The lower_hash_value must be lower than the higher_hash_value.
    * higher_hash_value enter an integer from 0 through 999 to identify the end value for a range of hash. The higher_hash_value must be higher than the lower_hash_value.

• msc_id enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.

• plmnid { any | mcc mcc_id mnc mnc_id } is not operationally supported at this time. The code is included for future development.

• no prefix included with a command, disables and/or erases the specified configuration from the MME’s configuration.

• default prefix is unused at this time and is available for future development.

• Use the show s102-service name s102_service_name command to verify the S102 configuration that you have entered following the steps outlined above.

• Use the show configuration command to view the S102 pool area and S102 non-pool area configuration.

mme-service

Use the following to add an association between a previously configured MME service and an S102 service.

config
  context context_name
    mme-service mme_service_name
      associate s102-service s102_service_name [ context context_name ]
    end
end

Notes:

• [ context context_name ] enter a string of 1 to 79 alphanumeric characters to identify the name of the context in which the S102 service is configured. We recommend that you identify the context if it is not the same one in which the associated MME service is configured.

• Use the show mme-service name mme_service_name command to verify the S102 association that you have entered following the steps outlined above.

Performance Indicator Changes

MME Schema

The MME tracks the number of SRVCC 1xRTT calls and 4G-to-1xRTT handovers using the following variables:
• s1ap-transdata-dlinktunnel
• s1ap-recdata-ulinktunnel
• s1-ho-4gto1xrtt-cs-srvcc-attempted
• s1-ho-4gto1xrtt-cs-srvcc-success
• s1-ho-4gto1xrtt-cs-srvcc-failures

**S102 Schema**

This new schema includes the following variables

- vpnname
- vpnid
- servname
- servid
- s102ap-tx-a21-air-signal-msg
- s102ap-tx-a21-ack-msg
- s102ap-tx-a21-evt-ntfy-msg
- s102ap-tx-unknown-msg
- s102ap-retx-a21-air-signal-msg
- s102ap-retx-a21-ack-msg
- s102ap-retx-a21-evt-ntfy-msg
- s102ap-retx-unknown-msg
- s102ap-rx-a21-air-signal-msg
- s102ap-rx-a21-ack-msg
- s102ap-rx-a21-evt-ntfy-msg
- s102ap-rx-unknown-msg
- s102ap-encode-errors
- s102ap-missing-mandatory-ies
- s102ap-corelation-mismatch
- s102ap-decode-errors
- s102ap-syntax-errors
- s102ap-misc-errors
Traps

Traps are defined to indicate when an S102 service starts or stops. The trap information includes the context identification in which the S102 service is configured the unique identification of the S102 service. The following are examples of how the traps would appear:

Internal trap notification <XXXX> (S102ServiceStop) context S102 service s102-service
Internal trap notification <YYYY> (S102ServiceStart) context S102 service s102-service

Timer-based GBR Bearer Deactivation

CSCuu03739 - Enable Timer Based GBR Bearer Deactivation

Feature Changes

Important

A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

The Timer Based GBR Bearer Deactivation, a proprietary feature of StarOS, allows MME to retain dedicated bearers of a User Equipment (UE). MME provides a configurable timer for which the GBR bearers are preserved for a UE.

Previous Behavior: Earlier, on receiving the UE context release request with cause Radio Connection With UE Lost, the GBR bearers were released making it unable to service immediate subsequent requests.

New Behavior: In the 19.0 release, the GBR bearers are preserved for a configurable amount of time when a UE context release request with cause Radio Connection With UE Lost is received.

Customer Impact: The configurable timer addition to preserve GBR bearers decreases the time to re-establish GBR bearers in case UE looses radio connection and needs to connect immediately.

Command Changes

gbr-bearer-preservation-timer

The Timer Based GBR Bearer Deactivation is configured in the Call Control Profile Configuration Mode. The **gbr-bearer-preservation-timer** is a new command that allows the user to configure the timer, which defines the time allowed for the GBR bearers to be preserved when the UE Context Release Request message with the Radio Connection With UE Lost cause code is received from eNodeB.

```
configure
call-control-profile  profile_name
  gbr-bearer-preservation-timer  timer_value
  [  remove  ] gbr-bearer-preservation-timer
end
```

Notes:

- The **gbr-bearer-preservation-timer** command allows the operator to set the preservation time for the Bearer on receiving the UE Context Release with the Radio Connection With UE Lost cause code.
• The timer_value specifies the duration for preserving the bearers in seconds. It is an integer value ranging from 1 to 600.
• The remove command disables the timer configuration.

Performance Indicator Changes

show call-control-profile full name <profile_name>

The following new field is added to the output of this command for this feature:
• GBR Bearer Preservation Timer

VPLMN Allowed/Not Allowed Implementation

CSCur30377 - 'VPLMN Allow' flag for MME/LTE user

Feature Changes

The vplmn-address command was added to the code in the Call Control Profile configuration mode for the SGSN. This command enables an operator to anchor a session of a roaming UE to its own home GGSN/PGW rather than allowing the UE to use the visiting GGSN/PGW.

Previous Behavior: The vplmn-address command was visible in the code in the Call Control Profile configuration mode for the MME but it was not implemented for the MME.

New Behavior: The command has now been implemented for the MME so that the configured value takes precedence to override the HSS-provided values of the AVP 'VPLMN Dynamic Address Allowed'.

Customer Impact: This behavior change will only impact the customer if the command was already configured in the MME's Call Control Profile. If the CLI has not been configured then the customer will perceive no change of behavior.
NAT Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from NAT in StarOS 19 software releases.

- NAT Enhancements for 19.0, page 251

NAT Enhancements for 19.0

This section identifies all of the NAT enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the NAT Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Bulks Statistics Support for NBRs

CSCut64992 - New bulkstat variable for NBRs chunk allocations/deallocations in R17.x

Feature Changes

In this release, bulk statistics are added for NAT Binding Records (NBRs) that are generated for IP and Port chunk allocations/deallocations.

Performance Indicator Changes

ECS Schema

The following bulk statistics are new in the release:
Port Chunk Count in show subscribers full Command Output

CSCuu74463 - [NAT] "show sub full" fails when no. of chunks is > 2500

Feature Changes

Previous Behavior: In previous releases, the show subscribers full command displayed all chunks associated with a subscriber.

New Behavior: The show subscribers full command will display the first 2016 chunks associated with a subscriber. The count of the actual number of port chunks will also be displayed correctly. It is recommended to configure bigger port chunk size so that the number of port chunks allocated to a single subscriber will be less than 2016.

Reduction of Port Chunk Size

CSCuo77875 - [NAT] Reducing minimum port chunk size configurable to 8

Feature Changes

Reducing the port chunk size is one method of improving efficient usage of NAT IP addresses allocated to a given Sessmgr. By increasing the number of users per NAT IP, the number of NAT IPs required to handle the calls in a given Sessmgr could come down. This will free NAT IP addresses and can be used by other Sessmgrs for allocation.

Prior to Release 18, the minimum port chunk size was 32 and configurable in multiples of 32, that is, 32, 64, 96, and so on. If an operator wanted to configure more than 32, it was not possible to configure 40 or 48 as the next bigger size was only 64. If the operator required 40 ports, then two chunks each of size 32 will be allocated. Even if only 40 ports were required, 64 ports were given. This led to under-utilization of port chunks and NAT IP addresses.

As part of the enhancement in Release 19, the minimum port chunk size configurable is reduced to 8 and the chunk size can be configured in multiples of 8 starting 8, 16, 24, 32, and so on. The default chunk size will still be 32. If no chunk size is configured, then the chunk size is calculated by dividing the entire NAT port range by the number of users per NAT IP and then rounding off to the nearest multiple of 32. Session Recovery and ICSR support are also added for this enhancement.

Previous Behavior: The minimum supported port chunk size was 32 and the chunk size was configurable in multiples of 32, that is, 32, 64, 96, and so on. The maximum number of chunks per user was 2016. The maximum number of users per NAT IP address supported was 2016.

New Behavior: With this enhancement, the minimum port chunk size is reduced to 8. The chunk size is configured in multiples of 8 instead of 32. The operator can configure chunk sizes starting 8, 16, 24, 32, and so on. This enhancement provides more flexibility in deciding the actual port chunk size to be used, also
preventing under-utilization of port chunks and NAT IP addresses. The maximum number of chunks per user is 8064. The maximum number of users per NAT IP address supported is 8064.

**Command Changes**

```
ip pool
```

In this release, the **port-chunk-size** keyword can be configured in multiples of 8 as the port chunk size is reduced to 8. With minimum port chunk size of 8, a maximum of 8064 port chunks per NAT IP can be configured.

```
configure
  context context_name
    ip pool pool_name { [ range start_ip_address end_ip_address ] | napt-users-per-ip-address users_per_ip | max-chunks-per-user max_chunks_per_user | on-demand | port-chunk-size port_chunk_size } }
end
```

**Notes:**

- The **napt-users-per-ip-address** keyword must be an integer from 2 through 8064.
- The **max-chunks-per-user** keyword must be an integer from 1 through 8064.
- The **port-chunk-size** keyword must be an integer from 8 through 32256 (in multiples of 8).

**Support for Dynamic Configuration of Users per NAT IP**

CSCup26223 - [NAT] Support for dynamic configuration of number of users per NAT IP

**Feature Changes**

In previous releases, the number of users per NAT IP address could not be modified dynamically once the NAT pool was created. As part of this feature, the number of subscribers per NAT IP address can be configured dynamically for optimal utilization of NAT IP addresses.

Changing the chunk size dynamically also requires changing the number of users per NAT IP dynamically. Any new NAT IP allocated by VPN will take the configuration in the NAT pool. When a NAT IP is already allocated to Sessmgr, the change in configuration in NAT pool will not be applied to that NAT IP. This NAT IP will still use the value that was configured when it was allocated to Sessmgr by VPN.

With NAT pool groups, each pool in a group must have the same number of users per NAT IP configured. If number of users per NAT IP configured in pools are different, though the configuration will still be allowed, the distribution of calls across pools in the group may not be even. Both session recovery and ICSR support are also added as part of this enhancement.

**Previous Behavior:** The number of users per NAT IP address is configurable in the NAT pool. However the configuration could not be modified dynamically once the NAT pool is created, without deleting the pool.

**New Behavior:** The number of users per NAT IP address can be configured dynamically. The new NAT IP addresses will use the new NAT IP value and old NAT IPs will use the old value.

**Customer Impact:** Based on the ports usage by active subscribers, customers can modify the number of users per NAT IP for optimal utilization of NAT IP addresses.
Support for Dynamic Port Chunk Size Configuration

CSCuo78855 - [NAT] Support for dynamic port chunk size configuration

Feature Changes

In previous releases, the port chunk size configured in a NAT pool could not be modified dynamically. The NAT pool had to be deleted and reconfigured with the new port chunk size. As part of this enhancement, port chunk size is made configurable dynamically.

When port chunk size is modified at pool level, it is possible that some NAT IP addresses will be already in use; for those active NAT IPs older value of port chunk size will be used. Only new NAT IPs being allocated from VPN will take the modified port chunk size.

With NAT pool groups, each pool in a group must have the same port chunk size configured. If different chunk sizes are configured, though the configuration will still be allowed, the distribution of calls across pools in the group may not be even. Both session recovery and ICSR to support the modified port chunk size of active NAT IPs is also provided.

Previous Behavior: The port chunk size of a configured N:1 NAT pool could not be changed without reconfiguring the pool.

New Behavior: The port chunk size of an existing NAT pool can be changed dynamically without deleting it.

Customer Impact: This is a flexibility added to change the NAT port chunk size configuration on the fly.
CHAPTER 16

PDSN Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from PDSN in StarOS 19 software releases.

- PDSN Enhancements for 19.2, page 255

PDSN Enhancements for 19.2

This section identifies all of the PDSN enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the PDSN Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your PDSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
PDSN vPC-DI Qualification

CSCuw10077 - vPC-DI qualification for PDSN-Service

Feature Changes

With this release, the PDSN has been fully qualified to run on Cisco's virtual Packet Core (vPC) - Distributed Instance (DI) platform. In vPC-DI, multiple virtual machines (VMs) act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management.

For more information about the vPC-DI platform, refer vPC-DI System Administration Guide.
CHAPTER 17

P-GW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from P-GW in StarOS 19 software releases.

- P-GW Enhancements for 19.6.6, page 257
- P-GW Enhancements for 19.6.1, page 259
- P-GW Enhancements for 19.5, page 261
- P-GW Enhancements for 19.4.4, page 262
- P-GW Enhancements for 19.4, page 264
- P-GW Enhancements for 19.2, page 277
- P-GW Enhancements for 19.1, page 300
- P-GW Enhancements for 19.0, page 301

P-GW Enhancements for 19.6.6

This section identifies all of the P-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the P-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For detailed information on the show commands, refer to the Statistics and Counters Reference for this release. For detailed information on the counters and disconnect reasons, refer to the BulkstatStatistics_documentation.xls spreadsheet that is included as part of the software companion package for this release.

Important This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your P-GW.
Re-transmitted HTTP Packet Not Dropped by ECS Even with Zero Balance

Applicable Products: P-GW

Feature Changes

Previous Behavior: In earlier releases,
- For delay charging, the HTTP re-transmitted packets were not rule matched. The packets were matched to the last matched ruledef whenever the delay charging CLI was configured.
- For a flow which is in redirected state, the DCCA/Gy component used to forward the packets without checking the quota.

New Behavior: With this release,
- For delay charging, the HTTP re-transmitted packets are rule matched. The last match rule is not used in this case.
- For a flow which is in redirected state, the DCCA checks if RST has been sent to the server. If RST is sent to the server, the packet is forwarded, else, it is dropped.

Customer Impact: Number of rule matches will increase with the number of TCP re-transmission.

Rule Matching of Re-transmitted HTTP Data Packets

Applicable Products: P-GW

Feature Changes

Previous Behavior: If the case flow was marked as permanent failure, re-transmitted HTTP data packets did not match the http-error rule.

New Behavior: With this release, if the flow is marked as permanent failure, then the re-transmitted packet matches either the http-error rule (if configured), or L3/L4 rules.

Customer Impact: There is a change in rule-match behavior of the re-transmitted HTTP data packets depending on rulebase and ruledef configuration.
P-GW Enhancements for 19.6.1

This section identifies all of the P-GW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the P-GW Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For detailed information on the show commands, refer to the Statistics and Counters Reference for this release. For detailed information on the counters and disconnect reasons, refer to the BulkstatStatistics_documentation.xls spreadsheet that is included as part of the software companion package for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

---

**Handling IMEI or IMSI Mismatch During Handover**

CSCvc21444 - Option to reject the MBReq/UPC when IMEI in MBreq/UPC different than the session present in PGW

**Applicable Products:** GGSN, P-GW

**Feature Changes**

During certain network scenarios, when a subscriber's session using a control tunnel endpoint ID (TEID) with P-GW/GGSN is disconnected, the session might be cleared locally (P-GW/GGSN) while it remains active on the peer node. When another subscriber connects to P-GW/GGSN from a home network, there is a probability that P-GW/GGSN might assign the same TEID value that was allotted during the earlier session to this subscriber. When S-GW/SGSN forwards the MBReq/UPC message to P-GW/GGSN with the TEID from the stale session, the session is considered as a handover for the earlier subscriber and P-GW CDRs are generated for that subscriber. The earlier subscriber is thus charged incorrectly.
**Previous Behavior:** Handover of MBReq/UPC was accepted even when IMEI/IMSI in MBreq/UPC was different than the session present in P-GW/GGSN.

**New Behavior:** With this release, handover of MBReq/UPC is rejected when IMEI/IMSI in MBreq/UPC is different than the session present in P-GW/GGSN. This change in behavior is controlled by newly introduced keywords in `egtp modify-bearer-rsp` and `gtpc` CLI commands.

**Command Changes**

**egtp**

The `reject imei-mismatch` keywords are added to the `egtp modify-bearer-rsp` CLI command under the P-GW Service Configuration Mode for configuring the P-GW to reject IMEI in the MBReq message during handover, when the IMEI is different than the one present in P-GW.

configure
  context context_name
    pgw-service service_name
      | default | no | egtp modify-bearer-rsp reject imei-mismatch
end

**Notes:**
- **default**: Resets the command to the default setting.
- **no**: Disables the configuration statement.
- **reject**: Modify Bearer Response reject options.
- **imei-mismatch**: Rejects Modify Bearer Request (MBReq) with CONTEXT_NOT_FOUND (CC 64) cause if IMEI/IMEISV received in MBReq does not match with the IMEI/IMEISV of an existing session.
  - By default, the MBReq will be accepted even if IMEI/IMEISV received in MBReq does not match with the IMEI/IMEISV of an existing session.

**gtpc**

The `update-pdp-resp reject imsi-mismatch` keywords are added to the `gtpc` CLI command under the GGSN Service Configuration Mode for configuring the GGSN to reject IMSI in the MBReq message during handover, when the IMSI is different than the one present in GGSN.

configure
  context context_name
    ggsn-service service_name
      | default | no | gtpc update-pdp-resp reject imsi-mismatch
end

**Notes:**
- **default**: Resets the command to the default setting.
- **no**: Disables the configuration statement.
- **update-pdp-resp**: Updates PDP Response options.
- **reject**: Updates PDP Response reject options.
- **imsi-mismatch**: Rejects Update PDP Request with NON_EXISTENT (CC 192) cause if IMSI received in Update PDP Request does not match with the IMSI of an existing session.
• By default, the Update PDP Request will be accepted even if IMSI received in Update PDP Request does not match with the IMSI of an existing session.

Performance Indicator Changes

show pgw-service name <service_name>

This command is enhanced to display the current status of reject imei-mismatch option. The following sample display is only a portion of the output:

- EGTP Bit Rate in Rounded Down Kbps : Disabled
- EGTP Suppress Update Bearer Request (no bitrate change) : Disabled
- EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch : Enabled/Disabled

show ggsn-service name <service_name>

This command is enhanced to display the current status of the reject imsi-mismatch option. The following sample display is only a portion of the output:

- GTPC Prioritised Rel99 ARP(s) :
- GTPC Update PDP Response with Non Existent cause if IMSI mismatch : Enabled/Disabled
- 3GPP Qos to DSCP Mapping (for G-PDUs):

Handling TAU Modify Bearer Request Scenarios

CSCvc74089 - Rejecting MBReq fails when IMEI in MBreq is diff than sess present in PGW during S4SGSN to 4g Ho

Applicable Products: P-GW

Feature Changes

Previous Behavior: The Modify Bearer Request (MBReq) for Tracking Area Update (TAU) without S-GW change was accepted, if the IMEI present in MBReq was different than the IMEI of current session.

New Behavior: With this release, the MBReq for TAU without S-GW change is rejected, if IMEI present in MBReq is different than the IMEI of current session.

The Modify Bearer Response message is sent with message level cause as REQUEST_REJECTED (0x5E) and bearer context level cause as CONTEXT_NOT_FOUND (0x40).

P-GW Enhancements for 19.5

This section identifies all of the P-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the P-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.
**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For detailed information on the show commands, refer to the *Statistics and Counters Reference* for this release. For detailed information on the counters and disconnect reasons, refer to the *BulkstatStatistics_documentation.xls* spreadsheet that is included as part of the software companion package for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**Important**

Release 19.5 introduces a number of security enhancements which may affect existing system deployments. Refer to the *System Changes* chapter in this guide for detailed information.

---

### Packet With Unexpected GTP Version

CSCuz86464 - Packet with unexpected GTP version: Behavior change.

**Applicable Products**: P-GW, SAEGW, S-GW

**Packet With Unexpected GTP Version**

**Old Behavior**: Earlier, if GTP-v2 received messages with version v1, v0, or above v2 sent a response messages stating "version not supported".

**New Behavior**: Now, if GTP-v2 received messages with v1 or v0, messages would be silently discarded. However, if the version is above v2, GTP-v2 sends a response message stating "version not supported".

**Impact on Customers**: Since the v0 and v1 messages are silently discarded, peer may not see any response and retry the same.

### P-GW Enhancements for 19.4.4

This section identifies all of the P-GW enhancements included in this release:
**Feature Changes** - new or modified features or behavior changes. For details, refer to the *P-GW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For detailed information on the show commands, refer to the *Statistics and Counters Reference* for this release. For detailed information on the counters and disconnect reasons, refer to the *BulkstatStatistics_documentation.xls* spreadsheet that is included as part of the software companion package for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**Handling of DHCPv6 Unicast Messages**

*CSCvd10605* - DHCP relay from UE to external DHCP server - in R17 PGW forwards the message, in R19 PGW inter

**Applicable Products**: GGSN, P-GW, SAEGW

---

**Feature Changes**

Handling of DHCPv6 unicast messages has been modified with this release.

**Previous Behavior**: All the DHVPv6 messages originating from UE (access side) with destination port number as 547 were consumed by the DHVPv6 server running on the boxer. These messages included DHCPv6 messages sent to unicast, multicast, or both unicast and multicast destination address with destination port number = 547. Other DHCPv6 messages with destination port number != 547 were sent to Gi interface as is, that is without any processing.

**New Behavior**: Following is the behavior when the *dhcpv6-client-unicast* CLI command under DHCP Client Profile Configuration Mode is:

- Disabled (default behavior) – The P-GW only consumes DHCPv6 message received from UE which has destination address as multicast address (FF02::1:2) and port number as 547. This behavior is compliant as per RFC 3315. All other messages are forwarded to Gi interface as it is, without any
processing. To proxy the unicast messages, operators should configure `dhcp-client-profile` with `enable dhcpv6-client-unicast` CLI command.

- **Enabled** – The P-GW consumes DHCPv6 messages received from UE which has any destination address (unicast, multicast, or both unicast and multicast) and port number as 547. These messages are proxied to the external DHCPv6 server with the configured unicast address in DHCPv6-Service. The messages which do not satisfy this condition are forwarded as is, without any processing, to Gi interface.

**Customer Impact:** Changes in DHCPv6 signaling for unicast packets.

## P-GW Enhancements for 19.4

This section identifies all of the P-GW enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *P-GW Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

- **Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For detailed information on the show commands, refer to the *Statistics and Counters Reference* for this release. For detailed information on the counters and disconnect reasons, refer to the `BulkstatStatistics_documentation.xls` spreadsheet that is included as part of the software companion package for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

---

**Important**

Release 19.4 introduces a number of security enhancements which may affect existing system deployments. Refer to the *System Changes* chapter in this guide for detailed information.
IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

Feature Description

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into the following three features:

• IPv6 Prefix Delegation from the RADIUS Server
• IPv6 Prefix Delegation from the Local Pool
• IPv6 Interface ID from the RADIUS Server

IPv6 Prefix Delegation from the RADIUS Server

Important

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the delegated prefix from the RADIUS server to the UE or the CPE.

To enable the prefix delegation from the RADIUS server, first configure the APN on the P-GW. See Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96.

How It Works

This section describes functionality of the prefix delegation from the RADIUS server.

During initial authentication process, RADIUS AAA can authorize Framed-IPv6-Address and Delegated-IPv6-Prefix AVP. Prior to the introduction of this feature Cisco P-GW was able to process only Framed-IPv6-Address AVP. This AVP was treated as Default-Prefix for the attaching UE. P-GW used to allocate 64-bit Interface-ID and the combined 128-bit address. The 64-bit default-prefix, derived from Framed-IPv6-Address AVP, and locally generated 64-bit Interface-ID was sent to the UE during this initial attachment. This 64-bit default-prefix was then associated with the default bearer/PDN for the UE and is considered as the UE's IPv6 address.

With the introduction of this feature, P-GW is able to process Delegated-IPv6-Prefix AVP along with Framed-IPv6-Address. Delegated-IPv6-Prefix AVP is used to designate the Delegated Prefix of prefix length 48/52/56 bits. This AVP is treated differently than Framed-IPv6-Address. P-GW communicates this delegated prefix to the UE only using DHCPv6 message handshake SOLICIT/ADVERTISE/REQUEST/RESPONSE. Delegated-IPv6-Prefix is not associated with the default bearer and it is not considered as the UE IPv6 address.
1 Configure the APN on the P-GW, to enable the prefix delegation from the RADIUS server. For the configuration steps, see Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96.

2 Configure APN on the P-GW for the prefix delegation. RADIUS server may send delegated prefix in the Access-Accept message independent of the APN configuration on the P-GW. Based on the APN configuration and presence of delegate prefix in the Access-Accept message, the following combinations are possible. The PDN setup is rejected if:
   • The RADIUS server has not sent Delegated Prefix in the Access-Accept message
   • The `pd-alloc-method` in the APN configuration is `no-dynamic`

The following table lists all possible combination of the APN configuration and presence of delegated prefix in the Access-Accept message:

Table 3: Mapping of APN Configuration and RADIUS Message

<table>
<thead>
<tr>
<th>pd-alloc-method in APN Configuration</th>
<th>Delegated-IPv6-Prefix in Access-Accept RADIUS Message</th>
<th>PDN State</th>
</tr>
</thead>
</table>
| no-dynamic                          | Yes                                                   | PDN is set up if:
|                                     |                                                       | • The delegated prefix is successfully allocated after level1 and level2 validations are done
|                                     |                                                       | • Validation with the static pool, as mentioned in step 3, is successful
|                                     |                                                       | If validation fails, PDN is not set up. |
| no-dynamic                          | No                                                    | PDN is not set up. |
| local/dhcpv6-proxy                  | Yes                                                   | Delegated-IPv6-Prefix in Access-Accept RADIUS message is discarded.
|                                     |                                                       | PDN set up.
|                                     |                                                       | Delegate prefix is allocated to the UE, on receiving SOLICIT message, based on the configured `pd-alloc-method` in the APN. |
| local/dhcpv6-proxy                  | No                                                    | PDN is set up.
|                                     |                                                       | Delegated prefix is allocated to the UE, on receiving SOLICIT message, based on the configured `pd-alloc-method` in the APN. |

3 The P-GW then performs the following two level validation for the prefix length received in Access-Accept RADIUS message:
Level 1: Prefix length must be only one of the supported values, such as, 48 / 52 / 56. For any other length, delegate prefix is rejected and PDN is not set up.

Level 2: If level 1 validation is passed, the prefix length is compared with the `prefix-delegation-len` configured in the APN using the CLI command, `ipv6 address prefix-delegation-len`.

If there is a mismatch, delegate prefix is rejected and PDN is not set up.

Important

Level 2 validation is not done if `prefix-delegation-len` is not configured in the APN.

4 Only if the above two level validation is successful, the received delegate prefix is validated against the static `ipv6` prefix pool configured in the destination context. If validation with the static pool is successful, then the delegate prefix is stored on the P-GW. If validation with the static pool fails, the delegate prefix is rejected and PDN is not set up.

5 After the PDN is set up, the UE or the CPE sends a delegated prefix request by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix, which it had stored earlier, in the DHCPv6 ADVERTISE message to the UE.

6 Next, the UE sends the DHCPv6 REQUEST message to the P-GW and the P-GW sends the DHCPv6 REPLY message to the UE, which completes the DHCPv6 handshake.

1 When the DHCPv6 RELEASE message is received from the UE, P-GW blocks data from any sources IP address from the delegated prefix pool. The delegated prefix is not released to the static `ipv6` prefix pool from which it was allocated. If the DHCPv6 SOLICIT message is received again from the UE, the same delegate prefix is sent to the UE. The P-GW starts passing the data from the source address part of the said delegated prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests delegated prefix release by sending DHCPv6 RELEASE REQUEST message to the P-GW.

The DHCPv6 RELEASE REPLY message is not sent to the UE and no message is sent to the RADIUS server if:

- The delegated prefix is released when validity time configured in the DHCPv6 service expires
- When the PDN is cleared

Release triggered reason can be checked from the DHCPv6 statistics(output of the CLI command `show dhcpv6 statistics`), which are as follows:

```
  Session Release Reasons: (dhcp-prefix-delegation)
PDNs Released: 3 Lease Exp Policy: 0
  UE Initiated Release: 1 Other Reasons: 0
```

7 When the PDN is cleared, the delegate prefix is released to the static `ipv6` prefix pool from which it was allocated.

### Configuring APN to Enable Prefix Delegation From RADIUS Server

Use the following syntax to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the RADIUS Server.

```
config
c  ontext context_name
    apn apn_name
        ipv6 address alloc-method [dhcppv6-proxy | local | no-dynamic] allow-prefix-delegation
```
pd-alloc-method no-dynamic
ipv6 address prefix-delegation-len [48 | 52 | 56]
end

Notes:

• `dhcpv6-proxy`: Configures the IPv6 address from DHCP server for the APN.
• `dhcpv6-proxy`: Configures the IPv6 address from DHCP server for the APN.
• `local`: Configures the IPv6 address from the local pool configured.
• `no-dynamic`: Configures the IPv6 address as indicated by the authentication server.
• `allow-prefix-delegation`: Configures the APN to allow DHCPv6 prefix-delegation.
• `ipv6 address prefix-delegation-len`: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Verifying Prefix Delegation from the RADIUS Server

To verify the Prefix Delegation from the RADIUS Server, use the following show commands.

`show dhcpv6 statistics`

When APN is configured to receive Delegated Prefix from Radius Server, the sessions statistics is visible under CLI command output of `show dhcpv6 statistics` and displays the following output:

<table>
<thead>
<tr>
<th>DHCPv6 Session Stats:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Current:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP Proxy:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP Server:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP PD:</td>
<td>0</td>
</tr>
<tr>
<td>Radius PD:</td>
<td>0</td>
</tr>
<tr>
<td>Local PD:</td>
<td>0</td>
</tr>
<tr>
<td>Total Setup:</td>
<td>5</td>
</tr>
<tr>
<td>DHCP Proxy:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP Server:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP PD:</td>
<td>0</td>
</tr>
<tr>
<td>Radius PD:</td>
<td>1</td>
</tr>
<tr>
<td>Local PD:</td>
<td>4</td>
</tr>
<tr>
<td>Total Released:</td>
<td>5</td>
</tr>
<tr>
<td>DHCP Proxy:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP Server:</td>
<td>0</td>
</tr>
<tr>
<td>DHCP PD:</td>
<td>0</td>
</tr>
<tr>
<td>Radius PD:</td>
<td>1</td>
</tr>
<tr>
<td>Local PD:</td>
<td>4</td>
</tr>
</tbody>
</table>

Notes:

• The total current counter is incremented while sending request reply message to the UE.
• The total current counter is decremented while sending release reply message to the UE (in case of UE initiated release) in the following two cases:
  • on valid life timer expiry
  • when PDN is cleared
• The total current counter may be incremented/decremented multiple times during a PDN connection.
• The total setup counter is incremented multiple times during the PDN connection lifetime. For example, every-time when the SOLICIT message is processed, the PD is successfully allocated to the UE.
• The total release counter is incremented multiple times during a PDN connection lifetime. For example, everytime when the PD is released when DHCPv6 RELEASE message is processed from the UE and/or
PD is released due to VALID lifetime timer expiry event. Along with this Session Release Reasons: (dhcp-prefix-delegation) counters are also incremented to the corresponding release reasons.

- Hence in case of delegate prefix allocation from the RADIUS server, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all
This command displays the following output:

IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA

show sub pgw-only full all
This command displays the following output:

IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA

show sub saegw-only full all
This command displays the following output:

IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA

**IPv6 Prefix Delegation from the Local Pool**

**Important**
This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request the delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the prefix delegation from the local pool to the UE or the CPE.

To enable the prefix delegation from the local pool, first configure the APN on the P-GW. See Configuring APN for Private Pool Name, on page 99 and Configuring Prefix Delegation on Destination Context, on page 100.

**How It Works**
This section describes the functionality of the prefix delegation from the local pool.

1. Configure APN on the GGSN/P-GW/SAE-GW to enable the prefix delegation from the local pool. For configuration steps, see Configuring APN for Private Pool Name, on page 99

2. Once the APN is configured, configure the pool on destination context. See Configuring Prefix Delegation on Destination Context, on page 100.
3 The PDN is first set up with default ipv6 prefix of length 64.

4 Once the PDN is set up, User Equipment (UE) or a Customer Premises Equipment (CPE) can request delegated prefix by sending DHCPv6 SOLICIT message to P-GW.

5 The P-GW then performs the following two level validation for the prefix length:
   **Level 1:** The prefix length requested in DHCPv6 SOLICIT message must be only one of the supported values, 48 / 52 / 56. For any other length, the SOLICIT is silently dropped at P-GW.
   **Level 2:** If level 1 validation is successful, then the following validation is done. If `prefix-delegation-len` is configured in the APN, then delegate prefix allocation of this length is attempted from the local private pool. If `prefix-delegation-len` is not configured in the APN, then delegate prefix allocation of length requested in SOLICIT message is attempted from the local private pool.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The requested length for the delegate prefix must match with the prefix-length configured for the private pool. The requested prefix length is as configured in the APN as ipv6 address prefix-delegation-len 52. If it is not configured in the APN, it may also be from the SOLICIT message. Configure the prefix length for the private pool by using the CLI command, <code>ipv6 pool ipv6-private-prefix 5001::1/48 prefix-length 52 private 0</code>. Only when these lengths match, delegated prefix allocation from the local pool is successful.</td>
</tr>
</tbody>
</table>

6 The UE or a CPE can request the delegated prefix by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix allocated from the local pool, in the DHCPv6 ADVERTISE message to the UE.

7 Next, the UE sends the DHCPv6 REQUEST message to the P-GW. The P-GW sends the DHCPv6 REPLY message to the UE, which completed the DHCPv6 handshake.
   If the delegated prefix allocation from the local pool fails, the DHCPv6 SOLICIT message is silently dropped at the P-GW.

8 When the UE sends the DHCPv6 RELEASE message, the delegated prefix is released to the ipv6 prefix pool.
   DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests prefix delegation released by sending DHCPv6 RELEASE REQUEST message to the P-GW.
   DHCPv6 RELEASE REPLY message is not sent to UE if:
   - The prefix delegation is released when validity time configured in the DHCPv6 service expires
   - The PDN is cleared

   If DHCPv6 SOLICIT message is received again from the UE, a new delegated prefix is allocated from the local pool and sent to the UE.

   **Configuring APN to Enable Prefix Delegation From Local Pool**

Configuration Overview
To enable prefix delegation from a local pool, perform the following steps:

**Step 1** Configure the private pool name in the APN configuration mode, to be used for delegate prefix allocation.

**Step 2** Configure the APN to enable or disable IPv6 prefix delegation or default prefix delegation from the local pool.

**Configuring APN for Private Pool Name**

Use the following steps to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the local pool:

```
config
 context context_name
  apn apn_name
   ipv6 address delegate-prefix-pool pool_name
   no ipv6 address delegate-prefix-pool
 end

config
 context context_name
  apn apn_name
   ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic] allow-prefix-delegation
   pd-alloc-method local
   ipv6 address delegate-prefix-pool pool_name
   ipv6 address prefix-delegation-len [48 | 52 | 56]
 end
```

Notes:

- **delegate-prefix-pool**: Configures a pool of IPv6 address delegated prefix.
  - `pool_name`: Name of the pool with IPv6 address delegated prefix.
- **no**: Disables the pool of IPv6 address delegated prefix.
- **dhcpv6-proxy**: Configures the IPv6 address from the DHCP server for the APN.
- **local**: Configures the IPv6 address from the local pool configured.
- **allow-prefix-delegation**: Configures the APN to allow DHCPv6 prefix-delegation.
- **ipv6 address prefix-delegation-len**: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

**Configuring Prefix Delegation on Destination Context**

Use the following configuration to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the Local Pool:

```
config
 context context_name
  ipv6 pool ipv6-private prefix 5001::1/48 prefix-length [48 | 52 | 56] private 0
 end
```

Notes:
IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

- **ipv6 pool**: Modifies the current context's IP address pools by adding, updating, or deleting a pool. This command also resizes an existing IP pool.

**Important**  The ipv6 prefix pool must be of the type **private**.

**Verifying Prefix Delegation from the Local Pool**

To verify the Prefix Delegation from the local pool, use the following show commands.

**show dhcpv6 statistics**

When APN is configured to receive Delegated Prefix from the local pool, the sessions statistics is visible under CLI command output of **show dhcpv6 statistics** and displays the following output:

```
DHCPv6 Session Stats:
  Total Current: 0
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 0
  Local PD: 0
  Total Setup: 5
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 1
  Local PD: 4

  Total Released: 5
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 1
  Local PD: 4
```

**Notes:** In case of delegate prefix allocation from local pool, Total Setup is equal to Total Current + Total Released.

**show sub ggsn-only full all**

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```

**show sub pgw-only full all**

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```

**show sub saegw-only full all**

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```
IPv6 Interface ID from the RADIUS Server

This feature allows the RADIUS/AAA Server to send an Interface-ID to the GGSN/P-GW/SAEGW service, in the Access-Accept message. This interface-id is used by these services and is communicated to the UE or the CPE. In this case, the GGSN/P-GW/SAEGW do not allocate a local interface-id. If the RADIUS/AAA server do not send an interface-id, then GGSN/P-GW/SAEGW allocate an interface-id locally and send it to the UE.

show apn statistics

Following CLI command can be used to see the total current active counter for Interface-ID allocation.

```
IP address allocation statistics:
Total IPv6 Interface IDs allocated:
   AAA provided:  1
   Locally Generated:  2
```

Limitations

Following are the limitations of the IPv6 Prefix Delegation feature:

- RADIUS ACCOUNTING messages do not support delegated prefix.
- Zero PL in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- NULL PD prefix in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- For PDN type v4v6, the dhcpv6-proxy method of allocation for the default prefix is not supported.
- The UE-requested Delegated Prefix in SOLICIT message is not supported. If the UE sends SOLICIT message requesting Delegated Prefix, it is rejected.
- One PD prefix per PDN is supported; multiple PD-prefixes per PDN are not supported.
- P-GW and GGSN do not support local-based and RADIUS-based allocation of both DHCPv6 prefix delegation and framed prefix delegation from the same pool. Hence the allocation is done from separate pools. Framed prefix received in the access-accept message is not part of the delegated prefix range.

ECS Rules Written for IP Protocol

CSCuy14480 - ECS rules written for IP protocol 132 are not hit

Applicable Products: GGSN, P-GW, SAE-GW

Feature Changes

Previous Behavior: Earlier, SCTP downlink traffic passed through the default bearer instead of dedicated bearer, when the received packet was matched with the packet filter, which was configured in either of the following ways:

- Only source port or destination port was configured
- IP Address and port was configured
However, when the packet filter was configured for source and destination IP address, and the packet filter matched with the received packet, traffic passed through the dedicated bearer.

**New Behavior:** Now, SCTP downlink traffic pass through the dedicated when the received packet is matched with the packet filter, which was configured in either of the following ways:

- Source and destination IP address
- Only source port or destination port was configured
- IP Address and port was configured

### SPGW Incorrectly Sending UDPv6 Packets

CSCuy78988- SPGW incorrectly sending UDPv6 packets with 0x0 checksum against RFC2460

**Applicable Products:** GGSN, P-GW, SAEGW, S-GW

#### Feature Changes

**Previous Behavior:** Earlier, if the result of the UDPv6 checksum calculation is zero, GW used to send the same, which effectively disables checksum for that packet. This was not compliant with the RFC2460, which suggests the checksum value to be set to 0xFFFF if derived calculation is zero.

**New Behavior:** After the fix, the checksum value is set to 0xFFFF if the result checksum calculation is ZERO and the compliance is met.

**Impact on customer:** Packet drops might be seen at peer, which does not support of handling packet with 0xFFFF checksum as suggested by the RFC.

### P-GW to Initiate CRA IE in UBReq Immediately

CSCuy95645 - PGW to initiate CRA IE in UBReq immediately

**Applicable Products:** P-GW, SAEGW

#### Feature Changes

For activating location reporting for a UE over Gx, RAR from PCRF was sent with the event trigger "USER_LOCATION_CHANGE". On receiving this event trigger, P-GW should typically send CRA IE with "Start Reporting " towards the MME to enable the Location-Change reporting for the UE in an MME.

Earlier, P-GW was not initiating Update Bearer Request procedure explicitly to inform only CRA IE and was relying on any other procedure like QoS change happening at same time or in future. This resulted in delay in updating required action at the MME. After this feature change, P-GW would immediately initiate Update Bearer Request, even for updating only CRA IE, if there are no other changes detected in RAR received with ULI_LOCATION_CHANGE event trigger. If there are other changes detected in RAR, CRA IE would be combined with Update Bearer Request initiated for the same.

**Previous Behavior:** Earlier, P-GW initiated update Bearer procedure was not triggered when the ULI event trigger was received from a RAR than a CCA-U.
New Behavior: Now, P-GW initiated update bearer procedure for CRA IE is triggered, if RAR is received with the ULI trigger.

IPv4v6 PDN Rejection

CSCuz51684 - IPv6 pdn rejected if UE req v6 addr n Access-Accept has Framed Prefix

Applicable Products: P-GW, SAEGW

Feature Changes

IPv4 or IPv6 PDN were rejected, when the UE requests IPv4 or IPv6 static address when the CLI command `ipv6 address alloc-method no-dynamic` was configured under the APN. However, IPv4v6 PDN was accepted when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` was configured.

Old Behavior: Earlier, IPv4v6 PDN was accepted when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` was configured.

New Behavior: Now, IPv4v6 PDN is rejected when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` is configured.

L2TP Password Behavior Parity Between P-GW and GGSN

CSCuz59475 - L2TP password behavior parity between PGW and GGSN

Applicable Products: P-GW, SAEGW

Feature Changes

GGSN L2TP call received from the UE without PCO IE in CSReq is successful. However, P-GW/SAEGW fails PPP authentication for a L2TP call if PCO IE is not received or PCO IE is received without authentication information in the Create Session Request. As a result the call is rejected.

A new keyword has been added to the existing CLI command `PPP` at the APN level. This CLI command allows L2TP P-GW/SAEGW call's PPP authentication to be successful even if:

- PCO IE is not received in CSReq
- PCO IE is not received
- PCO IE is received without authentication information in the Create Session Request.

Old behavior: Earlier, P-GW/SAEGW failed PPP authentication for a L2TP call if PCO IE was not received or PCO IE was received without authentication information in the Create Session Request. As a result, the call was rejected.

New behavior: A new CLI keyword has been added to the existing CLI command `PPP` at the APN level. When this CLI command is enabled, P-GW/SAEGW allows PPP authentication for a L2TP call even if:

- PCO IE is not received
- PCO IE is received without the authentication information in the Create Session Request.
As a result, the call is successful.

When the CLI command is disabled, P-GW/SAEGW fails PPP authentication information in the Create Session Request. As a result, the call is rejected.

**Impact on the Customer:** Successful P-GW/SAEGW L2tp calls can be established even if PCO IE is not received or PCO IE is received without authentication information in Create Session Request.

**Command Changes**

**l2tp allow-auth-without-pco**

A new keyword has been added to the existing CLI command PPP at the APN level. This command allows L2TP P-GW/SAEGW call's PPP authentication to be successful even if:

- The PCO IE is not received in CSReq
- The PCO IE is not received
- The PCO IE is received without authentication information in the Create Session Request.

```configure
context context_name
  apn apn_name
    ppp l2tp allow-auth-without-pco
    { default | no } ppp l2tp allow-auth-without-pco
end
```

**Notes:**

- **l2tp:** Configures PPP L2TP specific parameters
- **allow-auth-without-pco:** allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request.
- **Default Behavior:** P-GW does not allow PPP authentication for a L2TP call to go through successfully when PCO IE is not received in Create Session Request.

**Performance Indicator Changes**

**show apn <apn_name> | all**

This command has been modified to display the following fields:

- **ppp keep alive period:** 32
- **ppp mtu:** 1500
- **ppp auth without pco for l2tp:** Enabled
- **ppp auth without pco for l2tp:** Disabled

**show config verbose output**

If the CLI command **ppp l2tp allow-auth-without-pco** is configured, the output of this command is modified to display the following:
• ppp l2tp allow-auth-without-pco

If no ppp l2tp allow-auth-without-pco or default ppp l2tp allow-auth-without-pco or no configuration is done, there is no change in the output of this show command.

```
show apn <apn_name>
```

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

Virtual APN Configuration:
- Preference Rule-Definition
- Selected-APN
  1. PDP Type = ipv4 telenor.ipv4v6
  2. PDP Type = ipv6 telenor.nat64
  3. PDP Type = ipv4v6
  Roaming mode = roaming telenor.nat64

---

Retaining Old IMEI Values

CSCuz67967 - Logging when GTPC TEID reuse with different IMEI in MBR

Applicable Products: P-GW, SAEGW

Feature Changes

For a PDN session, P-GW receives MBReq with IMEI value which is different from old IMEI value.

Old behavior: On receiving MBReq with different IMEI value, P-GW replaces old IMEI information with the new IMEI value and start using the new IMEI information on all interfaces. This impacts the P-GW CDRs generated for that PDN session. P-GW CDRs generated before the MBReq uses the old IMEI value and P-GW CDRs generated after the MBReq uses the new IMEI value, which is wrong and has impact on billing and revenue loss for the customer.

New behavior: If, P-GW receives MBReq with IMEI value which is different from old IMEI value, P-GW ignores the new IMEI value received as part of MBReq and retains the old IMEI information. Hence, P GW-CDRs generated before or after MBReq now use the old IMEI value. As a result, there is no impact on billing.

P-GW Enhancements for 19.2

This section identifies all of the P-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the P-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

**GTP S5/S8, S2a, and S2b Interface Specific Bulkstats for P-GW**

CSCup36540 - GTP S5S8/S2a/S2b interface specific message, cause code & bulk stats

**Applicable Products:** P-GW, SAEGW

**Feature Changes**

Since P-GW anchors different GTPv2 based interfaces, such as S5/S8, S2a, and S2b, support has been added to provide per-interface based GTP statistics and bulkstats.

**Important**

Use of WiFi Integration functionality requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

With wider deployment of SP-WiFi networks and VoWiFi service, separate statistics on a per-GTP-interface basis will help Operators with analysis and debugging.

**Important**

If the first message from any peer is rejected/discarded, it won't be counted anywhere in the eGTP-C interface statistics.
Command Changes

clear egtpc statistics

This command has been enhanced to clear statistics per the following eGTP-C sub-interfaces:

- S2a
- S2b
- S5/S8

Important The keywords s2a and s2b are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

clear egtpc statistics interface-type pgw-ingress interface { s2a | s2b | s5s8 }  
clear egtpc statistics egtp-service service_name interface-type { s2a | s2b | s5s8 }
Notes:

- interface-type pgw-ingress interface { s2a | s2b | s5s8 }: Clears the eGTP-C interface statistics of a particular sub-interface of P-GW ingress.
- egtp-service service_name interface-type { s2a | s2b | s5s8 }: Clears the eGTP-C sub-interface statistics only for the specified eGTP-C service.
- These commands do not clear all of the eGTP-C statistics, only the specified interface statistics.

show egtpc statistics

This command has been enhanced to display statistics per the following eGTP-C sub-interfaces:

- S2a
- S2b
- S5/S8

Important The keywords s2a and s2b are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

show egtpc statistics interface pgw-ingress interface-type { s2a | s2b | s5s8 } [verbose ] [ | { grep grep_options | more } ]  
show egtpc statistics egtp-service service_name interface-type { s2a | s2b | s5s8 } [verbose ] [ | { grep grep_options | more } ]  
Notes:

- interface pgw-ingress interface-type { s2a | s2b | s5s8 }: Displays the eGTP-C interface statistics of a particular sub-interface of P-GW ingress.
• `egtp-service service_name interface-type { s2a | s2b | s5s8 }`: Displays the eGTP-C sub-interface statistics only for the specified eGTP-C service.

• TX and RX counters have been optimized based on the applicable interface.

• `verbose`: All of the cause codes supported for GTPv2 are now displayed as part of this option. All the cause code values are shown for each of the messages.

Performance Indicator Changes

P-GW Schema

The following counters have been added to collect GTP sub-interface data statistics:

• `subdatastat-totulpktfwd-s5`
• `subdatastat-totdlpktfwd-s5`
• `subdatastat-totulbytefwd-s5`
• `subdatastat-totdlbytefwd-s5`
• `subdatastat-totulpktdrop-s5`
• `subdatastat-totdlpktdrop-s5`
• `subdatastat-totulbytedrop-s5`
• `subdatastat-totdlbytedrop-s5`
• `apnambratelimit-uppktdrop-s5`
• `apnambratelimit-downpktdrop-s5`
• `apnambratelimit-upbytedrop-s5`
• `apnambratelimit-downbytedrop-s5`
• `subdatastat-totulpktfwd-s8`
• `subdatastat-totdlpktfwd-s8`
• `subdatastat-totulbytefwd-s8`
• `subdatastat-totdlbytefwd-s8`
• `subdatastat-totulpktdrop-s8`
• `subdatastat-totdlpktdrop-s8`
• `subdatastat-totulbytedrop-s8`
• `subdatastat-totdlbytedrop-s8`
• `apnambratelimit-uppktdrop-s8`
• `apnambratelimit-downpktdrop-s8`
• `apnambratelimit-upbytedrop-s8`
• `apnambratelimit-downbytedrop-s8`
• subdatastat-totulpktfwd-s2a
• subdatastat-totdlpktfwd-s2a
• subdatastat-totulbytefwd-s2a
• subdatastat-totdlbytefwd-s2a
• subdatastat-totulpktdrop-s2a
• subdatastat-totdlpktdrop-s2a
• subdatastat-totulbytedrop-s2a
• subdatastat-totdlbytedrop-s2a
• apnambrratelimit-uppktdrop-s2a
• apnambrratelimit-downpktdrop-s2a
• apnambrratelimit-upbytedrop-s2a
• apnambrratelimit-downbytedrop-s2a
• subdatastat-totulpktfwd-s2b
• subdatastat-totdlpktfwd-s2b
• subdatastat-totulbytefwd-s2b
• subdatastat-totdlbytefwd-s2b
• subdatastat-totulpktdrop-s2b
• subdatastat-totdlpktdrop-s2b
• subdatastat-totulbytedrop-s2b
• subdatastat-totdlbytedrop-s2b
• apnambrratelimit-uppktdrop-s2b
• apnambrratelimit-downpktdrop-s2b
• apnambrratelimit-upbytedrop-s2b
• apnambrratelimit-downbytedrop-s2b

**pgw-egtpc-s2a Schema**

This schema has been added to collect eGTP-C S2a interface statistics.

---

**Important**

Use of WiFi Integration functionality requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

If WiFi Integration functionality is available, but S2a interface type is not configured for P-GW Ingress eGTP service, all statistics will be displayed as zero.
pgw-egtpc-s2b Schema

This schema has been added to collect eGTP-C S2b interface statistics.

Important

Use of WiFi Integration functionality requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

If WiFi Integration functionality is available, but S2b interface type is not configured for P-GW ingress eGTP service, all statistics will be displayed as zero. This feature is currently only supported for P-GW ingress interfaces.

pgw-egtpc-s5s8 Schema

This schema has been added to collect eGTP-C S5/S8 interface statistics.

SAEGW Schema

The following counters have been added to collect eGTP-C interface statistics:

- pgw-subdatastat-totulpktfwd-s5
- pgw-subdatastat-totdlpktfwd-s5
- pgw-subdatastat-totulbytefwd-s5
- pgw-subdatastat-totdlbytefwd-s5
- pgw-subdatastat-totulpktdrop-s5
- pgw-subdatastat-totdlpktdrop-s5
- pgw-subdatastat-totulbytedrop-s5
- pgw-subdatastat-totdlbytedrop-s5
- pgw-apnambrratelimit-uppktdrop-s5
- pgw-apnambrratelimit-downpktdrop-s5
- pgw-apnambrratelimit-upbytedrop-s5
- pgw-apnambrratelimit-downbytedrop-s5
- pgw-subdatastat-totulpktfwd-s8
- pgw-subdatastat-totdlpktfwd-s8
- pgw-subdatastat-totulbytefwd-s8
- pgw-subdatastat-totdlbytefwd-s8
- pgw-subdatastat-totulpktdrop-s8
- pgw-subdatastat-totdlpktdrop-s8
- pgw-subdatastat-totulbytedrop-s8
- pgw-subdatastat-totdlbytedrop-s8
• pgw-apnambrratelimit-uppktdrop-s8
• pgw-apnambrratelimit-downpktdrop-s8
• pgw-apnambrratelimit-upbytedrop-s8
• pgw-apnambrratelimit-downbytedrop-s8
• pgw-subdatastat-totulpktfwd-s2a
• pgw-subdatastat-totdlpktfwd-s2a
• pgw-subdatastat-totulbytefwd-s2a
• pgw-subdatastat-totdlbytefwd-s2a
• pgw-subdatastat-totulpktdrop-s2a
• pgw-subdatastat-totdlpktdrop-s2a
• pgw-subdatastat-totulbytedrop-s2a
• pgw-subdatastat-totdlbytedrop-s2a
• pgw-apnambrratelimit-uppktdrop-s2a
• pgw-apnambrratelimit-downpktdrop-s2a
• pgw-apnambrratelimit-upbytedrop-s2a
• pgw-apnambrratelimit-downbytedrop-s2a
• pgw-subdatastat-totulpktfwd-s2b
• pgw-subdatastat-totdlpktfwd-s2b
• pgw-subdatastat-totulbytefwd-s2b
• pgw-subdatastat-totdlbytefwd-s2b
• pgw-subdatastat-totulpktdrop-s2b
• pgw-subdatastat-totdlpktdrop-s2b
• pgw-subdatastat-totulbytedrop-s2b
• pgw-subdatastat-totdlbytedrop-s2b
• pgw-apnambrratelimit-uppktdrop-s2b
• pgw-apnambrratelimit-downpktdrop-s2b
• pgw-apnambrratelimit-upbytedrop-s2b
• pgw-apnambrratelimit-downbytedrop-s2b

**clear egtpc statistics**

This command now clears all of the eGTP-C statistics, including interface statistics.

**show egtpc statistics header-decoder-errors**

This output of this command has been enhanced to show header-decoder errors for P-GW sub interfaces:
• Message header decoder errors at EGTPC:
  • Incorrect GTP version:
  • Unsupported msg received:
  • Incorrect msg length:
  • Invalid msg format:
  • Invalid sequence number:

• Interface PGW Ingress:
  • Interface-Type S5/S8:
    • Incorrect GTP version:
    • Unsupported msg received:
    • Incorrect msg length:
    • Invalid msg format:
    • Invalid sequence number:

  • Interface-Type S2A:
    • Incorrect GTP version:
    • Unsupported msg received:
    • Incorrect msg length:
    • Invalid msg format:
    • Invalid sequence number:

  • Interface-Type S2B:
    • Incorrect GTP version:
    • Unsupported msg received:
    • Incorrect msg length:
    • Invalid msg format:
    • Invalid sequence number:

**clear egtpc statistics interface-type interface-pgw-ingress**

This command now clears all of the eGTP-C statistics, including interface statistics of all the interfaces applicable to the P-GW ingress.
show pgw-service statistics all

The output of this command has been enhanced to show eGTP-C statistics per interface:

• S5U Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:

• S8U Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
• Dropped Bytes Due To APN AMBR Rate Limit:

• S2A Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:

• S2B Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
**show saegw-service statistics all function pgw**

The output of this command has been enhanced to show P-GW eGTP-C statistics per interface:

- **S5U Total Data Statistics:**
  - Uplink:
    - Total Pkts:
    - Total Bytes:
    - Total Dropped Pkts:
    - Total Dropped Bytes:
    - Dropped Pkts Due To APN AMBR Rate Limit:
    - Dropped Bytes Due To APN AMBR Rate Limit:

  - Downlink:
    - Total Pkts:
    - Total Bytes:
    - Total Dropped Pkts:
    - Total Dropped Bytes:
    - Dropped Pkts Due To APN AMBR Rate Limit:
    - Dropped Bytes Due To APN AMBR Rate Limit:

- **S8U Total Data Statistics:**
  - Uplink:
    - Total Pkts:
    - Total Bytes:
    - Total Dropped Pkts:
    - Total Dropped Bytes:
    - Dropped Pkts Due To APN AMBR Rate Limit:
    - Dropped Bytes Due To APN AMBR Rate Limit:

  - Downlink:
    - Total Pkts:
    - Total Bytes:
    - Total Dropped Pkts:
    - Total Dropped Bytes:
    - Dropped Pkts Due To APN AMBR Rate Limit:
• Dropped Bytes Due To APN AMBR Rate Limit:

• S2A Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:

• S2B Total Data Statistics:
  • Uplink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
  • Downlink:
    • Total Pkts:
    • Total Bytes:
    • Total Dropped Pkts:
    • Total Dropped Bytes:
    • Dropped Pkts Due To APN AMBR Rate Limit:
    • Dropped Bytes Due To APN AMBR Rate Limit:
Same Packet Updated in Forwarded and Dropped Sections in APN Statistics

CSCuw02980 - Same packet is updated in Forwarded and Dropped section in APN stats

Applicable Products: GGSN, P-GW

Feature Changes

The same packet is reflected in "Downlink pkts dropped" and "Downlink pkts forwarded" in show apn statistics output for GGSN and P-GW.

Previous Behavior: When downlink packet was dropped due to ECS AMBR and MBR policing decision, the dropped packet was counted as forwarded towards UE.

New Behavior: When downlink packet is dropped due to ECS AMBR and MBR policing decision, the dropped packet will no longer be counted as forwarded towards UE; only those packets which are forwarded to UE will be shown as forwarded packets.

Customer Impact: Behavior is now the same as documented behavior.

Default Configuration Differences Between StarOS 16.3.1 and 16.4.3

CSCuu01012 - Default Configuration differences between StarOS 16.3.1 vs 16.4.3.

Applicable Products: P-GW

Feature Changes

The command output of show configuration in builds earlier to StarOS 16.4.x displayed the configuration command no gtpc ran-procedure-ready-delay in the output. In build StarOS 16.4.x and later, the output no longer displays the configuration command line no gtpc ran-procedure-ready-delay.

Previous Behavior: In releases earlier to StarOS 16.4.x, show config command displayed the configuration command no gtpc ran-procedure-ready-delay in the output.

New Behavior: In StarOS 16.4.x and later releases, show config command no longer displays the configuration command no gtpc ran-procedure-ready-delay in the output. This config line is now displayed with command show config verbose.

Performance Indicator Changes

show configuration

In releases earlier to StarOS 16.4.x, the output of this command displayed configuration command no gtpc ran-procedure-ready-delay. However, in StarOS 16.4.x and later releases, the output of command show configuration no longer displays the configuration command no gtpc ran-procedure-ready-delay.
DHCPv6 Unicast Address Support

CSCut92596 - DHCPv6 Unicast address support in message exchange.

**Applicable Products:** GGSN, P-GW, SAEGW

**Feature Changes**

| Important | Use of DHCPv6 Unicast Address Support requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license. |

The IPv6 prefix delegation for the requested UE is either allocated locally or from an external DHCPv6 server by P-GW, GGSN, SAEGW based on configuration at these nodes. Currently, these DHCPv6 messages are sent to the external DHCPv6 server using multicast address as destination address. In networks where there are large number of P-GW servers, but less number of DHCPv6 servers, the DHCPv6 messages with multicast address have to travel through the entire network. This increases load on the network. This feature adds Unicast address support which enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCPv6 service. The operator need to configure a CLI to support for client unicast operation to the DHCPv6 Server. By default client-unicast is disabled.

**Previous Behavior:** Earlier there was no support to send DHCPv6 messages to the server on a unicast address. Message exchange used to happen on a multicast address.

**New Behavior:** Now with this feature, support for sending all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in DHCPv6 service has been added.

**Customer Impact:** Operators will now be able to send DHCPv6 messages on a unicast address by using the config CLI mentioned below.

**Command Changes**

`dhcpv6-client-unicast`

A new command `dhcpv6-client-unicast` has been added to the existing command `dhcp-client-profile`. This CLI command enables support for client unicast operation to the DHCPv6 Server. By default client-unicast is disabled.

```plaintext
configure
   context context_name
dhcp-client-profile
   [ enable | disable ] dhcpv6-client-unicast
end
```

**Notes:**

- `dhcpv6-client-unicast`: enables client to send messages on unicast address towards server.
Performance Indicator Changes

show configuration

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

dhcp-client-profile clientprof
disable dhcpv6-client-unicast
request dhcp-option dns-address
request dhcp-option sip-server-address

show configuration

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

dhcp-client-profile clientprof
disable dhcpv6-client-unicast
dhcp-client-profile dhcp-client-profile
dhcpv6-client-unicast
dhcpv6-client-unicast
request dhcp-option sip-server-address

show configuration verbose

When client unicast is enabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

dhcp-client-profile clientprof
enable dhcpv6-client-unicast
dhcp-client-profile dhcp-client-profile

show dhcpv6-client-profile all

When client unicast is disabled under `dhcp-client-profile` command, the `show configuration` command shows the following output.

Client Profile name: clientprof
Context: egress
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
Net Bios address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: enabled
Client_identifier: IMSI
User Class Option: NONE
Client Profile name: dhcp-client-profile
Context: egress
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
Net Bios address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: enabled
Client_identifier: IMSI
User Class Option: NONE
Traffic Shaping at the APN-AMBR Data Rate Level

CSCu23766 - Traffic Shaping; CSCuw33511 - Reduce Policing bucket interval from 100 ms to 10 ms.

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Important

In StarOS release 19.2, this feature is supported as lab quality only. With StarOS release 19.2.1, this feature is fully qualified as Deploy Quality.

Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Traffic Shaping is a rate limiting method similar to Traffic Policing, but provides a buffer facility for packets exceeding the configured limit. Once packets exceed the data-rate, the packet is queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data, the system can be configured to either drop the packets or retain it for the next scheduled traffic session.

Traffic will be shaped to the configured APN-AMBR value. Previously, data carried on non-GBR bearers was policed at the configured APN-AMBR rate. APN-AMBR policing dropped the data that did not match the configured APN-AMBR. With APN-AMBR traffic shaping, non-GBR data that does not match the configured APN-AMBR rate will be buffered. When enough memory tokens are available, the data will be transmitted. In addition, operators still have the option to allow operators to drop the data when the buffer limit is reached.

Command Changes

apn-ambr

The shape and transmit-when-buffer-full keywords are now available in APN Configuration Mode for traffic shaping on the GGSN, P-GW and SAEGW.

configure
    context  context_name
        apn  apn_name
            apn-ambr rate-limit direction { downlink | uplink } | violate-action { shape |
            transmit-when-buffer-full ]
            [ default | no ] apn-ambr rate-limit direction { downlink | uplink }
        end

Notes:

• shape [ transmit-when-buffer-full ]: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.
The `token-replenishment-interval` keyword has been added to the `apn-ambr` command in APN Configuration Mode. This token replenishment interval is used for both APN AMBR traffic policing and traffic shaping. Operators have the option of using the default interval (100ms) or configuring a lower token replenishment interval of 10ms. Reducing the interval to 10ms helps reduce the queuing time required by the 100ms interval for a given packet size.

**configure context context_name apn apn_name apn-ambr rate-limit token-replenishment-interval duration_msecs end**

Notes:

- Where `token-replenishment-interval` is the time duration, in milliseconds, to be used for APN AMBR-based traffic policing and shaping.
- Valid entries are 10 or 100 milliseconds. The default is 100 milliseconds.

The `milliseconds` variable has been added to the `auto-readjust duration` keyword for the `apn-ambr` command in APN Configuration Mode. This variable allows operators to configure the `auto-readjust duration` in increments of 100 milliseconds.

**configure context context_name apn apn_name apn-ambr rate-limit direction { downlink | uplink } [ burst-size { auto-readjust duration milliseconds integer 100...900 } [ default | no ] apn-ambr rate-limit direction { downlink | uplink } end**

Notes:

- Where `milliseconds` is the time duration, in milliseconds, to be used for the `auto-readjust duration` function in APN AMBR-based traffic policing and shaping.
- Valid entries are from 100 to 900 milliseconds, in increments of 100 milliseconds. For example, 100, 200, 300 and so on.

The new `traffic shape` command has been added to Global Configuration Mode. This command enables operators to configure the maximum limit for data buffering during APN AMBR traffic shaping.

**configure traffic shape max-buffer-size sessmgr MBs subscriber MBs end**

Notes:

- `sessmgr MBs`: Specifies the amount of memory allocated towards buffering session manager instances during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The `sessmgr MBs` setting should be larger than the `subscriber MBs` setting.
• **subscriber MBs**: Specifies the amount of memory allocated towards buffering subscriber traffic during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The **subscriber MB** setting should be less than the **sessmgr MB** setting.

---

**Caution**

Standard size buffers (500, 2k, and 10k bytes) are used for buffering packets to avoid memory fragmentation. As a result, there may be additional memory overhead in the memory used for buffering. The buffer limit in the above configuration refers to actual effective bytes used to store packets. Use caution to use appropriate buffer limits, so that the system does not significantly affect the overall Session Manager memory requirement for sessions.

---

### Performance Indicator Changes

**show configuration verbose**

The output of this command has been enhanced to provide APN AMBR traffic shaping parameters for the GGSN, P-GW, and SAEGW, if configured.

- `apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape (if configured without the transmit-when-buffer-full option).`
- `apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape transmit-when-buffer-full (if configured with the transmit-when-buffer-full option).`

The output of this command has also been enhanced to show the **token-replenishment-interval** for APN AMBR traffic shaping and policing, if configured.

- `apn-ambr rate-limit token-replenishment-interval <milliseconds>`

The output of this command has also been enhanced to provide the maximum buffer size allocated for traffic shaping for both subscribers and the session manager.

- `traffic shape max-buffer-size sessmgr <no. of MB> subscriber <no. of MB>`

**show subscriber pgw-only/ggsn-only/saegw-only full all**

Command output for each of these commands has been enhanced to show APN AMBR traffic shaping configuration parameters and statistics.

- APN AMBR shaping:
- Token replenishment interval(ms):
- Downlink traffic-shaping: <Enabled or Disabled>
- APN-AMBR(bps):
- Buffer full action: <drop or transmit>
- Burst Size:
- Auto Readjust: <Enabled or Disabled>
• Auto Readjust Duration (ms):
• Peak Burst size (bytes):
• Guaranteed burst size (bytes):
• Queued data (packets):
• Queued data (bytes):
• Drop count (packets):
• Drop count (bytes):
• Buffer Full Packets Fwd:
• Buffer Full Bytes Fwd:
• Packets Forwarded:
• Bytes Forwarded:
• Uplink traffic shaping: <Enabled or Disabled>
• APN-AMBR (bps):
• Buffer full action: <drop or transmit>
• Burst Size:
• Auto Readjust: <Enabled or Disabled>
• Auto Readjust Duration (ms):
• Peak Burst Size:
• Guaranteed burst size (ms):
• Queued data (packets):
• Queued data (bytes):
• Drop count (packets):
• Drop count (bytes):
• Buffer Full Packets Fwd:
• Buffer Full Bytes Fwd:
• Packets Forwarded:
• Bytes Forwarded:

If APN AMBR traffic shaping is disabled, the following output appears:
• APN AMBR Shaping:
• Downlink traffic-shaping: Disabled
• Uplink traffic-shaping: Disabled
Virtual APN Selection Based On PDP-Type

CSCuo61924 - Virtual APN based on PDP type.

**Applicable Products:** GGSN, P-GW, SAEGW

**Feature Changes**

The current implementation of selection of virtual APN is based on various criteria and a call received on a selected APN can be forwarded to another APN based on the configured criteria. This feature enables the operator to select the Virtual APN on the basis of PDP-type and PDP-type for roamers. For this, PDP-type rules for PDP-types IPv4, IPv6, and IPv4v6 have been added to the existing Virtual APN rules. Also, **roaming mode-roaming** has been implemented as a secondary option to PDP type to enable the operator to select the Virtual APN on the basis on PDP-type for roamers.

**Previous Behavior:** Earlier, Virtual APN was selected on the basis on various factors such as IMSI and MSISDN. PDP-type and PDP-type for roamers were not the basis for selection.

**New Behavior:** Now, an existing CLI virtual-apn preference has been modified to enable the Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

**Command Changes**

```
virtual-apn preference
```

New keyword **pdp-type** has been added to the command virtual-apn preference to support Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

```
configure
c   context context_name
c     apn apn_name
         virtual-apn preference priority apn apn_name [ access-gw-address { ip_address | ip_address/mask } | bearer-access-service service_name | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | domain domain_name | mcc mcc_number mnc mnc_number | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | cc-behavior cc_behavior_value | msisdn-range from msisdn_range_from to msisdn_range_to | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } ] ] | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } | ] ]
```

**Notes:**

- **pdp-type** Configures pdp-type rule.
- **ipv4** Configures Virtual APN rule for ipv4 addresses.
- **ipv6** Configures Virtual APN rule for ipv6 addresses.
- **ipv4v6** Configures Virtual APN rule for ipv4v6 addresses.
Performance Indicator Changes

show apn <apn_name>

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

Virtual APN Configuration:
Preference Rule-Definition Selected-APN
1 PDP Type = ipv4 telenor.ipv4v6
2 PDP Type = ipv6 telenor.nat64
3 PDP Type = ipv4v6
Roaming mode = roaming telenor.nat64

show pgw-service stats all

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

Virtual APN Configuration:
Preference Rule-Definition Selected-APN
1 PDP Type = ipv4 telenor.ipv4v6
2 PDP Type = ipv6 telenor.nat64
3 PDP Type = ipv4v6
Roaming mode = roaming telenor.nat64

show saegw-service stats all function pgw

This command has been modified to include counters to indicate the number of PDNs setup and rejected for Virtual APNs selected on the basis of PDP-type at the service level. Modified output includes the following fields:

VAPNs Selected Based on Configured PDP-Type
IPv4: Setup: 8 Rejected: 5
IPv6: Setup: 8 Rejected: 5
IPv4v6: Setup: 8 Rejected: 5

Virtual APN Selection Based on CC-Behavior

CSCuu43329 - Virtual APN selection based on all 16 bits of charging characteristics.

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Virtual APN Selection feature enables an operator to select Virtual APN based on all 16 bits of Charging Characteristics for GGSN, P-GW, and SAEGW nodes. Earlier, virtual APN selection was possible only on the basis on 4 cc-profile bits. With this feature, now an operator can select a Virtual APN on the basis on 4 cc-profile bits and 12 cc-behavior bits or on the basis on complete 16 cc-behavior bits. This selection can be done with the help of a CLI.

Previous Behavior: Earlier, Virtual APN selection was possible on the basis of 4 cc-profile bits.
**New Behavior:** Now, Virtual APN selection can now be done on the basis of 4 cc-profile bits and 12 cc-behavior bits or complete 16 cc-behavior bits.

**Customer Impact:** Virtual APN can be selected based on all 16 bits of Charging Characteristics.

**Command Changes**

virtual-apn preference

New keywords `pre-rel-9.1-cc-behavior` and `cc-behavior` have been added to the command `virtual-apn preference` to support Virtual APN selection on the basis of all charging characteristics.

```
configure context context_name
  apn apn_name
    virtual-apn preference priority apn apn_name { access-gw-address { ip_address | ip_address/mask } } | bearer-access-service service_name | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | cc-behavior cc_behavior_value | [ rat-type { eutran | gan | hspa | utran | wlan } ] | domain domain_name | mcc mcc_number | mnc mnc_number | cc-profile cc_profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | cc-behavior cc_behavior_value | [ msin-range from msin_range_from to msin_range_to ] | [ rat-type { eutran | gan | geran | hspa | utran | wlan } ] | roaming-mode { home | roaming | visiting } ]
no virtual-apn preference priority
end
```

Notes:

- `pre-rel-9.1-cc-behavior cc_behavior_value` Specifies the behavior charging characteristics bits in 12 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x341, then 0x34 corresponds to B12-B5 [MSB] and 0x1 corresponds to B4-B1 [Least significant nibble] of CC behavior. `cc_behavior_value` must be a hex value in the range 0x0000 to 0xFFFF.

- `cc-behavior cc_behavior_value` Specifies the behavior charging characteristics bits in 16 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x3412, then 0x34 corresponds to B15-B8 [MSB] and 0x12 corresponds to B7-B0 [LSB] of charging char. `cc_behavior_value` must be a hex value in the range 0x0000 to 0xFFFF.

**Performance Indicator Changes**

show apn <apn_name>

The following fields have been added to the output of this command.
show config

The following fields have been added to the output of this command.

```
apn starent.ipv4
selection-mode sent-by-ms
accounting-mode gtpp
ip context-name pgw-gl
virtual-apn preference 1 apn cisco.ipv4 cc-profile 1
virtual-apn preference 2 apn cisco.ipv4 cc-profile 1 rat-type eutran
virtual-apn preference 3 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104
virtual-apn preference 4 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104 rat-type gan
virtual-apn preference 5 apn star.com cc-behavior 0x1204
virtual-apn preference 6 apn star.com cc-behavior 0x1204 rat-type gan
virtual-apn preference 7 apn abc2.com mcc 100 mnc 100 cc-profile 1
virtual-apn preference 8 apn pqr2.com mcc 100 mnc 100 cc-profile 2 pre-rel-9.1-cc-behavior 0x104
virtual-apn preference 9 apn star2.com mcc 100 mnc 100 cc-behavior 0x1204
exit
```
show sub saegw-only full all

The following fields have been added to the output of this command.
charging id: 16777216
Charging chars (hex): 0x341    Charging chars: flat

P-GW Enhancements for 19.1

This section identifies all of the P-GW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *P-GW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

---

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**GTP-C Load and Overload Control on P-GW**

CSCus68103 - 3GPP based GTP-C Load and Overload Control on P-GW

**Feature Changes**

In StarOS release 19.0, this feature was supported as lab quality only. In StarOS release 19.1, this feature is now supported as deploy quality.
For details on this feature, refer to *GTP-C Load and Overload Control on P-GW* in the *P-GW Enhancements for 19.0* section of this document.

---

**Important**

GTP-C Load and Overload Control is an optional license-controlled feature. Contact your Cisco account or service representative for licensing information.

---

**New trap in the SNMP MIBs Reference**

CSCur07170 - Add a log/trap for SERDES lane(s) marked down

**Feature Changes**

Added the starSerdesLanePermDown SNMP MIB alarm.

---

**P-GW Enhancements for 19.0**

This section identifies all of the P-GW enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *P-GW Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your P-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements
Adding Cause in the UBRsp and CBRsp

CSCut49047 - Adding cause in the UBRsp, CBRsp

Feature Changes

In case of roaming, it can be difficult for the HPLMN to determine the reason why a bearer establishment or modification has been refused by the VPLMN. This results in a loss of cost revenue during the time of debugging. A new cause value has been added which indicates if it is due to the MME that the bearer has not been established or modified. This new cause value has been named as "MME/SGSN refuses it due to VPLMN Policy" and has been added in the Create Bearer Response and Update Bearer Response.

"MME/SGSN refuses due to VPLMN policy" cause is used by the MME/SGSN in the VPLMN to indicate to the P-GW in the Create Bearer Response or Update Bearer Response that it does not allow the establishment or modification of the bearer due to VPLMN operator’s policy.

Performance Indicator Changes

eGTP-C Schema

The following fields have been added to the eGTP-C Schema.

- tun-recev-crebearrespdeneidRejDueToVplmnPolicy
- tun-recev-updbearrespdeneidRejDueToVplmnPolicy

APN Schema

The following fields have been added to the APN Schema.

- crebearrespdeneidRejDueToVplmnPolicy
- updbearrespdeneidRejDueToVplmnPolicy

show egtpc statistics verbose

The following fields have been added under the "Reject Statistics" header in the command show egtpc statistics verbose

- Reject due to VPLMN policy: 0
- Reject due to VPLMN policy: 1

The following fields have been added under the "Update Bearer Denied" header in the command show egtpc statistics verbose

- Reject due to VPLMN policy: 0
- Reject due to VPLMN policy: 0
The following fields have been added under the "APN QCI Stats" header in the command `show egtpc statistics verbose`

- `crebearspdeniedRejDueToVplmnPolicy`
- `updbearspdeniedRejDueToVplmnPolicy`

### Bulkstat Process Retries for Connection Attempt After Transfer Interval

CSCuu58335 - Unable to retrieve bulkstats server information

**Feature Changes**

**Previous Behavior:** When a bulkstat receiver failed to respond, the bulkstat process tried reconnecting with the receiver during every server poll (30-second interval).

**New Behavior:** The bulkstat process no longer tries to reconnect on every server poll. Instead it will try to reconnect on expiry of the configurable bulkstat transfer-interval. The default transfer interval is 15 minutes. Bulkstat data collection continues during the configured transfer interval on receiver failures.

### eGTP-C Statistics

CSCuv69229 - show egtpc stats wrongly shows overload control info

**Feature Changes**

**Previous Behavior:** Having multiple services with an overload control profile configured led to the CLI command `show egtpc statistics` showing potentially inaccurate values for overload and load control. This problem was compounded further if there were multiple overload and load control profiles and they were associated with different services.

**New Behavior:** Load and overload statistics are now associated with a specific service and proper output is seen with the `show egtpc statistics egtp-service egtp_service_name` CLI command.

### Event-Based Idle Second Micro-Checkpoint Generation for P-GW

CSCut55276 - Support event based idle sec microcheck point generation

**Related CDETS ID** = CSCut82325

**Feature Changes**

To reduce the number of micro-checkpoints to peers for sessions moving from active to idle and idle to active, a new approach has been introduced using event-based micro-checkpoint generation.

This feature involves sending an idlesec micro-checkpoint from an active to standby chassis when the session state changes from active to idle or from idle to active. The micro-checkpoint carries information about the time when the session became active or idle. Upon receipt of the micro-checkpoint, the standby chassis updates the active/idle time. This process enables the active and standby chassis to be synchronized with respect to
when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event occurs, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not.

New configuration has been added per APN to send micro-checkpoints only when UE transitions from idle to active or active to idle.

**Previous Behavior:** Micro-checkpoints were configurable only with the `timeout idle` `micro-checkpoint-periodicity` option in the `timeout idle` command.

**New Behavior:** The `micro-checkpoint-deemed-idle` option is added to the `timeout idle` command to configure event-based sending of micro-checkpoints.

**Customer Impact:** More efficient sending of micro-checkpoints to the standby chassis along with an increase in SRP bandwidth.

### Command Changes

```
timeout idle
```

The new keyword `micro-checkpoint-deemed-idle` has been added to this command at the APN level for P-GW to configure the time duration, in seconds, after which a session is deemed idle or active and determines whether a micro-checkpoint must be sent.

```
configure
  context context_name
    apn apn_name
      timeout idle idle_dur [ micro-checkpoint-deemed-idle time_in_seconds ]
    micro-checkpoint-periodicity time_in_seconds
    { default | no } timeout idle
end
```

Notes:

- **micro-checkpoint-deemed-idle time_in_seconds:** Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis.

  The `micro-checkpoint-deemed-idle` setting should be less than the `timeout idle` setting.

  `time_in_seconds` must be an integer from 10 to 1000.

  Default: 180

- **default:** Indicates the timeout specified is to be returned to its default behavior.

- **no:** Disables the timeout idle functionality.

- Either the `micro-checkpoint-deemed-idle` or `micro-checkpoint-periodicity` value can be configured for idle time duration.

- Any change from `micro-checkpoint-deemed-idle` to `micro-checkpoint-periodicity`, or vice versa, requires removing the first configuration before adding the new configuration.
Performance Indicator Changes

show apn name \textit{apn\_name}

The following new field has been added to show idle timeout configuration at the APN level:

- idle seconds deemed idle checkpoint periodicity

show configuration

The output of this command has been enhanced to show the micro-checkpoint-deemed-idle setting:

- timeout idle <duration\_seconds> micro-checkpoint-deemed-idle <duration\_seconds>

Grep Option Removed from "clear subscriber" Command

CSCus03709 - Command \texttt{<b>clear subs</b>} with \texttt{grep} does not prompt for confirm

Feature Changes

Previous Behavior: Earlier, the command \texttt{clear subscriber} asked for a confirmation before cleaning the subscribers when \texttt{no autoconfirm} was set. Also, when \texttt{clear subscriber} command was given in conjunction with a |, the command cleared the subscribers without asking for confirmation, even when \texttt{no autoconfirm} was set. As a result, the subscribers were cleared without confirmation.

New Behavior: The | option has been removed and is no longer available. The command \texttt{clear subscriber} now always ask for a confirmation message when \texttt{no autoconfirm} is set.

Command Changes

clear subscriber

This command has been modified to remove the | option. The command now always prompts for a confirmation when \texttt{no autoconfirm} is set.

GTP-C Collision Handling on P-GW

CSCut47252, CSCut47278, CSCut47296, CSCut47347 - GTP-C Collision Handling on P-GW

Feature Changes

Three enhancements have been made to handle various GTP-C collision handling scenarios on the P-GW:

1. DBCmd/MBreq Collision Handling: The P-GW has been enhanced to allow operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW.
Previous Behavior: The MBReq message was aborted upon its collision with the DBCmd.

New Behavior: Now there are three CLI-controlled options to handle the collision between the DBCmd and MBReq messages:

- Queue the DBCmd message when the MBreq message is pending. The advantage of this option is that the DBCmd message is not lost for most of the collisions. It will remain on the P-GW until the MBRsp is sent out.
- Drop the DBCmd message when the MBreq message is pending. Note that with this option the S-GW must retry the DMCmd.
- Use pre-StarOS 19.0 behavior: abort the MBreq message and handle the DBCmd message. The advantage of this option is that it provides backward compatibility if the operator wants to retain pre-StarOS 19.0 functionality.

Customer Impact: More flexibility in handling DBCmd message and MBReq message collision scenario.

2. MBReq/CBreq Parallel Processing; Handling CBRsp: The P-GW has been enhanced to handle the following collision scenario:

Previous Behavior: When the Create Bearer Request (CBreq) message was pending at the P-GW, and if a Modify Bearer Request (MBReq) message was received at the P-GW, then the CBReq transaction was allowed to exist while the MBReq was in progress. If a CBRsp was subsequently received then it was dropped by the EGTPC layer.

New Behavior: The EGTPC layer queues the CBRsp message and feeds the CBRsp message to the P-GW session manager when the MBRsp is sent out.

Customer Impact: No retransmission of CBRsp messages from the MME.

3. Handling UBRsp when Transaction is Suspended: The P-GW has been enhanced to handle this collision scenario.

Previous Behavior: The P-GW/S-GW dropped the Update Bearer Response (UBRsp) if the Update Bearer Request (UBReq) transaction was suspended.

New Behavior: When the P-GW/S-GW receives an UBRsp message, then the P-GW/S-GW handles the UBRsp message for the suspended transaction.

Customer Impact: The UBRsp message will be buffered until the MBRsp message is sent out.

Command Changes

collision-handling dbcmd-over-mbreq

This new CLI command in EGTP Service Configuration Mode allows operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW.

configure
  context context_name
    egtp-service egtp_service_name
      collision-handling dbcmd-over-mbreq { drop | queue }
      { default | no } collision-handling dbcmd-over-mbreq
  end

Notes:
Performance Indicator Changes

show configuration

The output of this command has been enhanced to show the collision handling setting for the DBcmd message when the MBreq message is pending.

- collision-handling dbcmd-over-mbreq queue
- no collision-handling dbcmd-over-mbreq queue

show egtp-service all

The output of this command has been enhanced to show the collision handling setting for the DBcmd message when the MBreq message is pending.

- Collision handling:
  - DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort MBreq and handle DBcmd>.

GTP-C Load and Overload Control on P-GW

CSCus68103 - 3GPP based GTP-C Load and Overload Control on P-GW

Feature Changes

This feature is currently supported as lab quality only.

Important

R12 GTP-C Load and Overload Control on the P-GW has been enhanced with the following features:

- **Self-Protection Behavior**: Applies to Overload Control only. Enables the operator to configure APN names and EARP priority level values for self-protection mode so that incoming request messages for emergency packet data node (PDN) connections and/or configured EARP priority values are not rejected even if the system is under self-protection mode.

- **Publishing/Handling of Load/Overload Control Profile Information**: The operator can enable/disable the publishing of Load or Overload control information towards roaming partners. By default, publishing of load control information is enabled for home PLMN(s) and disabled for foreign PLMN(s). EGTPC categorizes each peer as belonging to either the home or visited PLMN, and uses this information to publish load/overload control information to a peer based on the configuration. To help support this
enhancement, operators can now configure up to 512 PLMN IDs in S-GW Service Configuration Mode using the `plmn id` command.

- **Message Prioritization:** *Applies to Overload Control only.* In the R12 GTP-C Load Overload control feature, it is possible to apply message throttling, (when a peer indicates it is overloaded), based on message priority. To apply message prioritization it is necessary to configure the percentage of two groups of messages that each node (P-GW or ePDG) is expected to generate. The operator now can define the expected number of messages as a percentage for each message group.

- **Addition of Granular Statistics:** Granular level statistics at the EGTP service and peer levels have been added to provide more detailed information on R12 GTP-C Load/Overload Control feature performance.

### Command Changes

#### load-control-handling

This new command has been added to GTPC Load Control Profile Configuration Mode. It enables or disables the handling of load control information provided to the MME and S-GW.

```
configure
  gtpc-load-control-profile profile_name
    load-control-handling { home | visited }
    no load-control-handling { home | visited }
    default load-control-handling
end
```

Notes:

- **home:** Enables the handling of load control information for the home PLMN.
- **visited:** Enables the handling of load control information for the visited PLMN.
- **default:** Returns load control handling to its default behavior (enabled).

#### load-control-publishing

This new command has been added to GTPC Load Control Profile Configuration Mode. It enables or disables the publishing of load control information towards the home or visited PLMN.

```
configure
  gtpc-load-control-profile profile_name
    load-control-publishing { home | visited }
    no load-control-publishing { home | visited }
    default load-control-publishing
end
```

Notes:

- **home:** Enables the publishing of load control information towards the home PLMN.
- **visited:** Enables the publishing of load control information towards the visited PLMN.
- **default:** Returns load control handling to its default behavior (enabled).
message-prioritization

This new command has been added to GTPC Overload Control Profile Configuration Mode. It configures the priority percentage to be given to each of two specific message groups.

configure
gtpc-overload-control-profile  profile_name
  message-prioritization group1 percentage group2 percentage
  no message-prioritization
  default message-prioritization
end

Notes:

- **group1** specifies the message priority percentage for the following messages:
  - Update Bearer Request message for default bearer generated from P-GW ingress
  - Update Bearer Request message for dedicated bearer generated from P-GW ingress
  - Handoff Create Session Request message generated from ePDG egress.

- **group2** specifies the message priority percentage for the following messages:
  - Create Bearer Request message for default bearer generated from P-GW ingress
  - PDN connection requested Create Session Request message from ePDG egress

- The total percentage for the message groups should equal 100%.
- **group1** messages will have the highest priority (1) and are dropped last. **group2** messages will have the lowest priority (2) and are dropped first.
- **default** returns the group message priority settings to their default value. The default for each group is 50%.
- The default behavior for this command is enabled. To disable the command use the **no** option.

overload-control-handling

This new command in GTPC Overload Control Profile Configuration Mode enables or disables the handling of overload control information for the home or visited PLMN.

overload-control-handling
gtpc-overload-control-profile  profile_name
  overload-control-handling { home | visited }
  no overload-control-handling { home | visited }
end

Notes:

- **home**: Specifies that the handling of overload control information is enabled for the home PLMN.
- **visited**: Specifies that the handling of overload control information is enabled for the visited PLMN.
overload-control-publishing

This new command in GTPC Overload Control Profile Configuration Mode enables or disables the publishing of overload control information towards the home or visited PLMN.

configure
gtpc-overload-control-profile profile_name
  overload-control-publishing { home | visited }
  no overload-control-publishing { home | visited }
end

Notes:

- **home**: Specifies that overload control information will be published towards the home PLMN.
- **visited**: Specifies that overload control information will be published towards the visited PLMN.

self-protection-behavior

This new command in GTPC Overload Control Profile Configuration Mode configures self-protection-behavior for configured APNs or EARP values.

configure
gtpc-overload-control-profile profile_name
  [ no ] self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude }
end

Notes:

- **apn**: Configures up to three APN names to be allowed under self-protection behavior.
- **earp**: Configures up to three EARP priority level values so that incoming request messages for the configured evolved ARP priority values are not rejected even if the system is under self-protection mode.
- **no**: Disables the specified options.

Performance Indicator Changes

show configuration

The output of this command has been enhanced to provide additional details on self-protection configuration settings.

- no self-protection-behavior earp exclude
- no self-protection-behavior apn exclude
- self-protection-behavior earp <n n> exclude
- self-protection-behavior apn <n n> exclude

The output of this command has also been enhanced to show the configuration settings for overload and load control publishing and handling.

- overload-control-handling <home or visited>
• overload-control-publishing <home or visited>
• load-control-handling <home or visited>
• load-control-publishing <home or visited>

The output of this command has been enhanced to show the message prioritization configuration settings:

• message-prioritization group1 <n> group2 <n>
• no message-prioritization

**show gtpc-load-control-profile full all**

The output of this command has been enhanced to indicate how load control handling and load control publishing are configured.

• Load control information Handling:
  • Homer: <Enabled/Disabled>
  • Visitor: <Enabled/Disabled>

• Load control information Publishing:
  • Homer: <Enabled/Disabled>
  • Visitor: <Enabled/Disabled>

**show gtpc-overload-control-profile full all**

The output of this command has been enhanced to indicate how overload self-protection behavior, load control handling, load control publishing, and load control message prioritization are configured.

• Self-Protection Behavior:
  • Exclude EARP: <Disabled> or <n n>
  • Exclude APN: <Disabled> or <n n>

• Overload control information Handling:
  • Homer: <Enabled/Disabled>
  • Visitor: <Enabled/Disabled>

• Overload control information Publishing:
  • Homer: <Enabled/Disabled>
  • Visitor: <Enabled/Disabled>

• Message Prioritization
  • Group1: <0...100 or n/a>
show egtpc statistics egtp-service <egtp-service name>

The output of this command has been enhanced to provide detailed granular statistics for load and overload control profile statistics that have been transmitted (TX) and received (RX). Statistics are provided on a per egtp-service basis.

Load Control Information
No of times Load Control info TX:
   Accepted:
      Homer:
      Non Homer:
   Ignored:
      Homer:
      Non Homer:
      No config:
   Wrong Sequence Number:
   Current Load Factor:
   Sequence Number:
Overload Control Information:
No of times Overload Control info TX
   Accepted
      Homer:
      Non Homer:
   Ignored:
      Homer:
      Non Homer:
      No config
   Wrong Sequence Number:
   Current Overload Factor:
   Current Overload Reduction Metric
   Sequence Number:
   Validity Period(Secs):
No of times Overload ThresholdReached
Number of Messages Throttled:
   Message group 1:
   Message group 2:
   Self Protection:
Number of Messages Accepted in Self Protection:
   APN level:
   EARP level

Load Control Information
No of times Load Control info RX:
   Accepted:
      Homer:
      Non Homer:
   Ignored:
      Homer:
      Non Homer:
      No config:
   Wrong Sequence Number:
   Current Load Factor:
   Sequence Number:
Overload Control Information:
No of times Overload Control info RX
   Accepted
      Homer:
      Non Homer:
   Ignored:
      Homer:
      Non Homer:
      No config
   Wrong Sequence Number:
   Current Overload Factor:
   Current Overload Reduction Metric
   Sequence Number:
**Validity Period (Secs):**
No of times Overload Threshold Reached
Number of Messages Throttled:
  Message group 1:
  Message group 2:
Self Protection:
Number of Messages Accepted in Self Protection:
  APN level:
  EARP level:

**IMSI/IMEI Available in System Event Logs of Type Error and Critical**

CSCuu51587, CSCut68271 - Inclusion of IMSI/IMEI in logs

**Applicable Products:** GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

**Previous Behavior:** The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all system event logs of type error and critical.

**New Behavior:** The GGSN/P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available.

---

**Important**

Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.

---

**Table 4: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details**

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format &quot;[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d&quot;</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s&quot;</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Ran out of session handles&quot;</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td><strong>Modified Events</strong></td>
<td></td>
</tr>
<tr>
<td>139001</td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td>191006</td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td>10034</td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s&quot;. For example &quot;[IMSI -112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td>12668</td>
<td>Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot;</td>
</tr>
<tr>
<td>12774</td>
<td>Represents pgw_purge_invalid_crr in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot;</td>
</tr>
<tr>
<td>12855</td>
<td>Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td>12857</td>
<td>Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%lu&gt;.&quot;</td>
</tr>
<tr>
<td>12858</td>
<td>Represents ncqos_nrxx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%lu&gt;.&quot;</td>
</tr>
<tr>
<td>12859</td>
<td>Represents ncqos_nrxx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%lu&gt;: pf_id_bitmap 0x%x and tft_opcode: %d&quot;</td>
</tr>
<tr>
<td>12860</td>
<td>Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%lu&gt; rejected, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12861</td>
<td>Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%lu&gt;, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12862</td>
<td>Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state: &lt;%s&gt;.[event:&lt;%s&gt;]&quot;</td>
</tr>
<tr>
<td>11830</td>
<td>Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
<tr>
<td>11832</td>
<td>Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GRV bearers to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0x%x&gt; not found.&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>12960</td>
<td>Represents gtp_pdp_type_mismatch in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN %s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>11282</td>
<td>Represents pcc_intf_error_info in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents collision_error in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d&quot;</td>
</tr>
<tr>
<td>11917</td>
<td>Represents rcvd_invalid_bearer_binding_req_from_acs in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr %d: Received invalid bearer binding request from ACS.&quot;</td>
</tr>
<tr>
<td>11978</td>
<td>Represents saegw_uid_error in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11994</td>
<td>Represents unwanted_pcc_intf_setup_req error in format &quot;[IMSI &lt;IMSI&gt;] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface &quot;</td>
</tr>
<tr>
<td>140005</td>
<td>Represents ue_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled UE event %s in state %s&quot;</td>
</tr>
<tr>
<td>140006</td>
<td>Represents pdn_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled PDN event %s in state %s&quot;</td>
</tr>
<tr>
<td>140007</td>
<td>Represents epsb_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled EPSB event %s in state %s&quot;</td>
</tr>
<tr>
<td>10726</td>
<td>Represents saegwdrv_generic_error &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
</tbody>
</table>

**Command Changes**

**logging**

The **include-ueid** keyword has been added to the **logging** command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```plaintext
configure
logging include-ueid
no logging include-ueid
end
```
Performance Indicator Changes

The output of this command has been enhanced to indicate if the `logging` command is enabled with the `include-ueid` keyword.

- logging include-ueid
- no logging include-ueid

Inclusion of Sender F-TEID in DSReq

CSCut49046 - support: CR-1419, Inclusion of senderfteeid in DSReq

Feature Changes

P-GW wrongly deleted PDN connection upon receiving Delete Session Request message from the old S-GW, which is not the current serving S-GW for the PDN connection. This lead to hung sessions on the new S-GW. To overcome this problem, S-GW includes sender’s F-TEID for S5/S8 interface also, so that P-GW compares it with the received Sender's F-TEID earlier in the Create Session Request or Modify Bearer Request message.

Previous Behavior: Earlier, in DSReq at S5/S8 interface S-GW would not send its own FTEID.

New Behavior: Now, sender's FTEID is included in the Delete Session Request message also for S5/S8 interface, so that compares it with the received Sender's F-TEID earlier in the Create Session Request or Modify Bearer Request message.

IPMS Configuration Update During VPN-ctrl Start

CSCuu56803 - [SysTest] vpnctrl over mem usage during longevity

Feature Changes

During unplanned MIO switchover, VPN-ctrl restarts and IPMS-config is updated to all clients in non-blocking call, causing too many memory allocations.

Previous Behavior: In the absence of the IPMS-config at SCT, configuration was broadcast to all the clients by IPMS-ctrl (part of VPN-ctrl) while VPN-ctrl kick started.

New Behavior: In the absence of the IPMS-config at SCT, configuration is not broadcast to all the clients by IPMS-ctrl (part of VPN-ctrl) while VPN-ctrl kick starts.

Customer Impact: During unplanned MIO switchover, VPN-ctrl would not go to warn state.

Log Cause Values Corrected

CSCut96856 - Difference in Cause values during DBReq/MBReq collision
Feature Changes

Cause value displayed in eGTP-C log during DBReq/MBReq collision is not consistent with cause displayed in mon pro for same eGTP-C message.

**Previous Behavior:** Log used to print cause sent by application.

**New Behavior:** Log prints cause sent by application, but if it is not proper a cause from PDU is printed instead.

**Customer Impact:** Ease of debugging increased.

LTE to 3G Handover

CSCuu88011 - Seg fault in "egtpc_handle_del_bearer_cmd_req_evt" during LTE to 3G HO

Feature Changes

**Previous Behavior:** In case of collapsed call when LTE to 3G HO takes place, call on S-GW was aborted internally.

**New Behavior:** In case of collapsed call when LTE to 3G HO takes place, call on S-GW aborted after DSReq is received from MME.

Maintain Session Uniqueness

CSCus87417, CSCut99086 - PGW: Maintain Session Uniqueness

Feature Changes

When the MME is reselected by the UE or when the MME reselects a different P-GW during timeout scenarios, it is possible that the old PDN connection request is still being processed in the network and the session created by the new PDN connection request is overwritten by the stale procedure.

New IEs TimeStamp and MWT (MaxWaitTime) have been added in CSReq and forwarded on S6b/Gx/Gy interfaces in order to maintain session uniqueness at P-GW.

**Previous Behavior:** These IEs were not present and in certain scenarios there were stale sessions in P-GW.

**New Behavior:** Using these new IEs, now session uniqueness can be maintained on P-GW.

**Customer Impact:** In the following scenario, stale session won't be present on P-GW.

The P-GW is still processing the session creation but the S-GW times out due to timer configurations and notifies the MME with Create Session Failure (Cause #100: Remote Peer Not Responding). MME reselects an alternate P-GW in this case, but the original P-GW still continues to process the session. In certain scenarios, the original P-GW can overwrite the Gx session on the PCRF that is created by the newly selected P-GW. In this case, the new P-GW session is the valid session and original P-GW session is invalid as far as the UE, MME, and S-GW are concerned. The same can occur with the AAA session as well based on timing. This results in PCRF having invalid session information and the user plane works fine anchored on the second P-GW, but the Rx and Gx signaling fails as this terminates via original P-GW.

This results in VoLTE calls failing after SIP signaling between UE and P-CSCF.
To solve the problem, TimeStamp and MWT IE have been incorporated to be transmitted from MME and shared across the network nodes.

**Command Changes**

**message-timestamp-drift**

This new command allows drift time configuration to take care of NTP drift issues.

```
configure
  context context_name
  pgw-service service_name
    message-timestamp-drift time_in_seconds
    { default | no } message-timestamp-drift
end
```

Notes:

- **message-timestamp-drift time_in_seconds**: Configures the drift time from the message timestamp, in seconds, up to which P-GW will consider processing the message timestamp and max-wait-time (MWT) IEs.

  If the create-time from MME is off from the currenttime by configured-drift-duration, then this could lead to a high NTP drift and session uniqueness falls back to using currenttime toward Diameter servers.

  If the timestamp received in CSReq is significantly off (more than configured drift), then P-GW will not take action based on MWT and received timestamp and will transparently pass it to all AAA/Gx/Gy interfaces.

  When received drift is less than configured limit, P-GW will reject the call if "MWT + ReceivedTimeStamp > CurrentTimeStampAtPGW" condition is met. Otherwise, P-GW will forward the timestamp and MWT to AAA/Gx/Gy interfaces.

  **time_in_seconds** must be an integer from 0 to 1000.

  Default: 180

- **default**: Sets drift time to 180 seconds.

  If P-GW detects drift less than 180 seconds, it will check for condition "MWT + ReceivedTime > CurrentTimeAtPGW" and based on that P-GW will reject the call. If this condition is not met, it will transparently forward MWT and timestamp to AAA/Gx/Gy interfaces.

- **no**: Disables message timestamp drift. MWT and received timestamp will not be passed on to all AAA/Gx/Gy interfaces.

- Drift time configuration under P-GW service shall be used by the associated LMA service.

**Performance Indicator Changes**

**LMA Schema**

The following new counters have been added to show the total number of binding update deny messages due to newer sessions detected:
The following new fields have been added to show the number of PBA failures due to newer sessions detected:

- Update Denied - Unspecified Reason
  - Newer Session detected by AAA
  - Newer Session detected by PCRF
  - Newer Session detected by PCS

**"Newcall policy reject" Enhancement for Releasing Existing Calls**

CSCuu21036 - Newcall policy reject enhancement for releasing existing calls

**Applicable Products:** GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

If the newcall policy is set to **reject release-existing-session** and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

**Important**

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Command Changes**

**newcall policy**

The keyword **release-existing-session** has been added to this command to reject and release existing IMSI/IMEI session(s) when newcall arrives.

```
newcall policy pgw-service { all | apn name apn_name | name service_name } reject [ release-existing-session ]
no newcall policy pgw-service { all | apn name apn_name | name service_name }
```

**Notes:**

- **reject release-existing-session:** All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Disabled by default.
Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions.

**Performance Indicator Changes**

*show egtpc statistics verbose*

The following new field has been added to indicate such calls released:

- NewCall Reject Existing Sessions Released

**Newcall Policy Retained After Demux Migration**

CSCuu51916 - Newcall policy not working after demux PSC migration

**Feature Changes**

**Previous Behavior:** Newcall policy not working after demux migration.

**New Behavior:** Newcall policy configuration will be retained after demux migration.

**P-GW Overcharging Protection**

CSCut49056 - P-GW should use only one of indIE or Pvt exten for overcharging

**Feature Changes**

P-GW should send only required IE in the MBRsp message for Overcharging Protection.

**Previous Behavior:**

- Overcharging protection configuration in EGTPC service was used by EGTPC P-GW ingress along with Overcharging Protection CLI present in P-GW service.
- While doing network upgrade, some of the S-GW supported indication IE in the MBReq message and some of the IEs supported private extension in the MBReq message. P-GW always sent both the IEs in the CSRsp and for all MBRsp message.

**New Behavior:**

- Overcharging Protection configuration in EGTPC service is not used by EGTPC P-GW ingress. CLI command "gtpc private-extension overcharge-protection" in egtp-service is now obsolete.
- On S5/S8 interface, while doing network upgrade, some of the S-GW now supports indication IE in the MBReq message and some of the IEs support private extension in the MBReq message. P-GW will not send both the IEs always in the CSRsp and MBRsp. Only for TAU/RAU/handover with S-GW relocation procedures based on CSReq and MBReq, P-GW may send both IEs or one of IE in CSRsp and MBRsp.
• For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW does not have indication or private extension IE with Overcharging Protection information.

Removal of APN-AMBR from the Modify Bearer Response

CSCut49045 - support CR-1392(3gpp 29.274): Removal of APN-AMBR in the MBR

Feature Changes

To support CR-1392 (3gpp 29.274) during GnGp handover, APN-AMBR IE has been removed from Modify Bearer Response. A node compliant to this release of the specification will not include APN-AMBR IE in Modify Bearer Response. A new CLI has been introduced, which when enabled sends MBRsp with APN-AMBR during GnGp HO to sync with old behavior.

Previous Behavior: During GnGp handover if PCRF changes APN-AMBR value in CCA-U, then MBRsp is sent with APN-AMBR IE.

New Behavior: Now, during GnGp handover, if PCRF changes APN-AMBR value in the CCA-U, then MBRsp does not include APN-AMBR. However, UBRRes is triggered to send updated APN-AMBR.

Command Changes

egtp

The new keyword gngp-modify-bearer-rsp-with-apn-ambr enables sending MBRsp with APN-AMBR during GnGp HO to sync with old behavior. By default, this CLI is disabled.

configure
context context_name
  pgw-service <pgw-service-name>:
    [ default | no ] egtp gngp-modify-bearer-rsp-with-apn-ambr
end

Notes:


• default: Disables the new keyword. MBRsp should not have APN-AMBR, but UBRReq should be triggered to send updated APN-AMBR.

• no: Disables this functionality. MBRsp should not have APN-AMBR, but UBRReq should be triggered to send updated APN-AMBR.

Performance Indicator Changes

show pgw-service all

The following field has been added in the output of this command.

• EGTP GnGp Modify bearer res with APN-AMBR: Enabled /Disabled
RTT Support Expanded to Include PMIPv6 (S2a)

CSCut82602 - RTT support to be expanded to include PMIPv6 (S2a)

Related CDETS ID = CSCut82619

Feature Changes

Previous Behavior: For eHRPD, RTT messages were not generated even if configuration was enabled.

New Behavior: For eHRPD, RTT messages are generated if configuration is enabled.

Performance Indicator Changes

System Schema

The following counters have been added for RTT messages:

- sess-pgw-total-pmipv6-event-records
- sess-pgw-total-pba-event-records
- sess-pgw-total-bra-event-records

show event-record statistics pgw

The following new fields have been added for RTT messages:

- PMIPv6 Event Records
  - PBU-PBA
  - BRI-BRA/Timeouts

Setting of HI bit in the CSReq

CSCut64771 - CR 1493. Setting of hi bit in the CSReq

Feature Changes

Previous Behavior: If HI bit in indication IE was not set and UE context was present with different RAT, then this CS request was treated as handoff CS request.

New Behavior: Now, if "Trusted WLAN Mode Indication" IE is present, then it is post-release-12 UE and HI bit in indication IE is used as coming from the network.

If "Trusted WLAN Mode Indication" IE is not present, then it is pre-release-12 UE and CS request is considered as handoff CS request if UE context is present with different RAT.
Syslogging of Reject Events

CSCuu21047 - Inclusion of IMSI in EGTPC logs for reject events

**Applicable Products**: GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

**Previous Behavior**: The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all eGTP-C system event logs of type error and critical.

**New Behavior**: The P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the eGTP-C event log details for the system event logs of type error and critical, if available. If the IMSI is not available, the P-GW/SAEGW/S-GW will make the best effort to obtain the IMEI.

**Command Changes**

```
logging

The **include-uid** keyword has been added to the **logging** command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
c
```
configure

  logging include-uid
  no logging include-uid

  end

```

**Performance Indicator Changes**

```
show configuration

The output of this command has been enhanced to indicate if the **logging** command is enabled with the **include-uid** keyword.

  • logging include-uid
  • no logging include-uid
```
PSF Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from PSF in StarOS 19 software releases.

- PSF Enhancements for 19.0, page 325

PSF Enhancements for 19.0

This section identifies all of the PSF enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the PSF Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Support for Client and Server Port in Access Ruledefs

CSCut79532 - Client port and Server port support in FW access ruledefs

Applicable Products: GGSN, HA, IPSG, P-GW, PDSN

Feature Changes

In this release, the Firewall Access Ruledefs support TCP/UDP client port and server port configurations in addition to TCP/UDP source port, destination port and either port configurations that are already supported.

Previous Behavior: ECS allows TCP/UDP port-based rules to be configured only as "src-port" and "dst-port". Support to configure direction based rules was not provided.

New Behavior: TCP/UDP client port and server port support is provided for Firewall Access Ruledefs to simplify rule line configurations. When a Firewall//NAT rule match is performed, for an uplink packet, the destination port in the packet must be considered as server port and rule match must be done accordingly.
Similarly the source port of an uplink packet must be considered as the client port. For a downlink packet, the source port must be considered as the server port and the destination port as the client port. The new CLI commands added to support client/server port configurations are configured in the ACS Ruledef Configuration mode and Firewall-and-NAT Access Ruledef Configuration mode.

**Command Changes**

**tcp client-port**

This new command configures an access ruledef to analyze user traffic based on client TCP port.

```
configure
  active-charging service service_name
  access-ruledef access_ruledef_name
    [ no ] tcp client-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } }
end
```

**tcp client-port**

This command allows you to define rule expressions to match client port number in TCP headers.

```
configure
  active-charging service service_name
  ruledef ruledef_name
    [ no ] tcp client-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } }
end
```

**tcp server-port**

This command configures an access ruledef to analyze user traffic based on server TCP port.

```
configure
  active-charging service service_name
  access-ruledef access_ruledef_name
    [ no ] tcp server-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } }
end
```

**tcp server-port**

This command allows you to define rule expressions to match server port number in TCP headers.

```
configure
  active-charging service service_name
  ruledef ruledef_name
    [ no ] tcp server-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name } }
end
```
udp client-port

This command configures an access ruledef to analyze user traffic based on client UDP port.

```plaintext
configure
  active-charging service service_name
  access-ruledef access_ruledef_name
    [ no ] udp client-port { operator port_number | { !range | range } { start_range to end_range } }
    port-map port_map_name }
end
```

udp client-port

This command allows you to define rule expressions to match client port number in UDP headers.

```plaintext
configure
  active-charging service service_name
    ruledef ruledef_name
    [ no ] udp client-port { operator port_number | { !range | range } { start_range to end_range } }
    port-map port_map_name }
end
```

udp server-port

This command configures an access ruledef to analyze user traffic based on server UDP port.

```plaintext
configure
  active-charging service service_name
    access-ruledef access_ruledef_name
    [ no ] udp server-port { operator port_number | { !range | range } { start_range to end_range } }
    port-map port_map_name }
end
```

udp server-port

This command allows you to define rule expressions to match server port number in UDP headers.

```plaintext
configure
  active-charging service service_name
    ruledef ruledef_name
    [ no ] udp server-port { operator port_number | { !range | range } { start_range to end_range } }
    port-map port_map_name }
end
```

Performance Indicator Changes

show active-charging ruledef firewall

This command is enhanced to display the TCP/UDP client port and server port configurations.
Support for Client and Server Port in Access Ruledefs
SAEGW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from SAEGW in StarOS 19 software releases.

The following points to changes made in this document to correct omissions or technical errors made in previously published Release Change Reference. In content for:

- SAEGW Enhancements for 19.0:
  - CSCut88293 - SAEGW S2a support. Included is a feature description, command changes, bulk statistic schema changes, and performance indicator changes.

- SAEGW Enhancements for 19.6.6, page 329
- SAEGW Enhancements for 19.5, page 331
- SAEGW Enhancements for 19.4.x, page 332
- SAEGW Enhancements for 19.4, page 334
- SAEGW Enhancements for 19.3, page 348
- SAEGW Enhancements for 19.2, page 348
- SAEGW Enhancements for 19.1, page 358
- SAEGW Enhancements for 19.0, page 358

SAEGW Enhancements for 19.6.6

This section identifies all of the SAEGW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SAEGW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

## Configuration for HTTP Packets with Partial Headers

**Applicable Products:** SAEGW

### Feature Changes

**Previous Behavior:** Earlier, when HTTP packets with partial headers were received, HTTP analyzer went in a "wait" state until the partial header was completed in subsequent packets. The packets received in such a state were not sent for rule matching.

**New Behavior:** With this change, a new CLI command has been introduced to allow the operator to configure a packet limit until which the analyzer can remain in the "wait" state. The operator can either continue or terminate the flow when the configured limit is reached.

**Customer Impact:** In case of HTTP flows where only a partial header has been received, a change in rule-match behavior may be seen.

### Command Changes

A new CLI command has been added to the ACS Rulebase Configuration Mode to configure the maximum number of packets in which the partial HTTP header should get completed.

```
configure
  active-charging service ecs_service_name
  rulebase rulebase_name
    [ no ] flow http max-packets-for-header-completion <10...50> action { continue | terminate }
end
```

**Notes:**

- **http:** Specifies the HTTP flow.
max-packets-for-header-completion: Specifies the maximum number of packets to be considered for header complete state.

action: Specifies the Action for HTTP flows.
continue: Continue flow in partial state.
terminate: Terminates the flow.

Usage: This command sets the maximum number of packets in which partial HTTP header gets completed. If the configured packet limit is reached, the flow can either be continued or terminated.

HTTP Version Check Not Done in HTTP Analyzer

Applicable Products: SAEGW

Feature Changes

An issue was seen with the HTTP analyzer that passes invalid HTTP version packets and does not flag HTTP errors against any Layer7 rules.

Previous Behavior: Invalid HTTP version packet was not flagged as HTTP error.

New Behavior: With this release, invalid HTTP version packet is flagged as HTTP error.

Customer Impact: This change in behavior prevents the ability of rogue subscribers to bypass policies by spoofing the HTTP header version.

SAEGW Enhancements for 19.5

This section identifies all of the SAEGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the SAEGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.
Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Packet With Unexpected GTP Version

CSCuz86464 - Packet with unexpected GTP version: Behavior change.

Applicable Products: P-GW, SAEGW, S-GW

Packet With Unexpected GTP Version

Old Behavior: Earlier, if GTP-v2 received messages with version v1, v0, or above v2 sent a response messages stating "version not supported".

New Behavior: Now, if GTP-v2 received messages with v1 or v0, messages would be silently discarded. However, if the version is above v2, GTP-v2 sends a response message stating "version not supported".

Impact on Customers: Since the v0 and v1 messages are silently discarded, peer may not see any response and retry the same.

SAEGW Enhancements for 19.4.x

This section identifies all of the SAEGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the SAEGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.
Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Handling of DHCPv6 Unicast Messages

CSCvd10605 - DHCP relay from UE to external DHCP server - in R17 PGW forwards the message, in R19 PGW inter

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Handling of DHCPv6 unicast messages has been modified with this release.

Previous Behavior: All the DHCPv6 messages originating from UE (access side) with destination port number as 547 were consumed by the DHCPv6 server running on the box. These messages included DHCPv6 messages sent to unicast, multicast, or both unicast and multicast destination address with destination port number = 547. Other DHCPv6 messages with destination port number != 547 were sent to Gi interface as is, that is without any processing.

New Behavior: Following is the behavior when the dhcpv6-client-unicast CLI command under DHCP Client Profile Configuration Mode is:

- Disabled (default behavior) – The P-GW only consumes DHCPv6 message received from UE which has destination address as multicast address (FF02::1:2) and port number as 547. This behavior is compliant as per RFC 3315. All other messages are forwarded to Gi interface as it is, without any processing. To proxy the unicast messages, operators should configure dhcp-client-profile with enable dhcpv6-client-unicast CLI command.

- Enabled – The P-GW consumes DHCPv6 messages received from UE which has any destination address (unicast, multicast, or both unicast and multicast) and port number as 547. These messages are proxied to the external DHCPv6 server with the configured unicast address in DHCPv6-Service. The messages which do not satisfy this condition are forwarded as it is, without any processing, to Gi interface.
Customer Impact: Changes in DHCPv6 signaling for unicast packets.

SAEGW Enhancements for 19.4

This section identifies all of the SAEGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the SAEGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

Feature Description

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into the following three features:
IPv6 Prefix Delegation from the RADIUS Server

**Important**

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the delegated prefix from the RADIUS server to the UE or the CPE.

To enable the prefix delegation from the RADIUS server, first configure the APN on the P-GW. See Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96

**How It Works**

This section describes functionality of the prefix delegation from the RADIUS server.

During initial authentication process, RADIUS AAA can authorize Framed-IPv6-Address and Delegated-IPv6-Prefix AVP. Prior to the introduction of this feature Cisco P-GW was able to process only Framed-IPv6-Address AVP. This AVP was treated as Default-Prefix for the attaching UE. P-GW used to allocate 64-bit Interface-ID and the combined 128-bit address. The 64-bit default-prefix, derived from Framed-IPv6-Address AVP, and locally generated 64-bit Interface-ID was sent to the UE during this initial attachment. This 64-bit default-prefix was then associated with the default bearer/PDN for the UE and is considered as the UE's IPv6 address.

With the introduction of this feature, P-GW is able to process Delegated-IPv6-Prefix AVP along with Framed-IPv6-Address. Delegated-IPv6-Prefix AVP is used to designate the Delegated Prefix of prefix length 48/52/56 bits. This AVP is treated differently than Framed-IPv6-Address. P-GW communicates this delegated prefix to the UE only using DHCPv6 message handshake SOLICIT/ADVERTISE/REQUEST/RESPONSE. Delegated-IPv6-Prefix is not associated with the default bearer and it is not considered as the UE IPv6 address.

1. Configure the APN on the P-GW, to enable the prefix delegation from the RADIUS server. For the configuration steps, see Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 96.

2. Configure APN on the P-GW for the prefix delegation. RADIUS server may send delegated prefix in the Access-Accept message independent of the APN configuration on the P-GW. Based on the APN configuration and presence of delegate prefix in the Access-Accept message, the following combinations are possible. The PDN setup is rejected if:

   - The RADIUS server has not sent Delegated Prefix in the Access-Accept message
   - The `pd-alloc-method` in the APN configuration is `no-dynamic`

The following table lists all possible combination of the APN configuration and presence of delegated prefix in the Access-Accept message:
### Table 5: Mapping of APN Configuration and RADIUS Message

<table>
<thead>
<tr>
<th>pd-alloc-method in APN Configuration</th>
<th>Delegated-IPv6-Prefix in Access-Accept RADIUS Message</th>
<th>PDN State</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-dynamic</td>
<td>Yes</td>
<td>PDN is set up if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The delegated prefix is successfully allocated after level1 and level2 validations are done</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Validation with the static pool, as mentioned in step 3, is successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If validation fails, PDN is not set up.</td>
</tr>
<tr>
<td>no-dynamic</td>
<td>No</td>
<td>PDN is not set up.</td>
</tr>
<tr>
<td>local/dhcpv6-proxy</td>
<td>Yes</td>
<td>Delegated-IPv6-Prefix in Access-Accept RADIUS message is discarded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDN is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delegate prefix is allocated to the UE, on receiving SOLICIT message, based on the configured pd-alloc-method in the APN.</td>
</tr>
<tr>
<td>local/dhcpv6-proxy</td>
<td>No</td>
<td>PDN is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delegated prefix is allocated to the UE, on receiving SOLICIT message, based on the configured pd-alloc-method in the APN.</td>
</tr>
</tbody>
</table>

3 The P-GW then performs the following two level validation for the prefix length received in Access-Accept RADIUS message:

**Level 1**: Prefix length must be only one of the supported values, such as, 48 / 52 / 56. For any other length, delegate prefix is rejected and PDN is not set up.

**Level 2**: If level 1 validation is passed, the prefix length is compared with the prefix-delegation-len configured in the APN using the CLI command, `ipv6 address prefix-delegation-len`.

If there is a mismatch, delegate prefix is rejected and PDN is not set up.

**Important**

Level2 validation is not done if prefix-delegation-len is not configured in the APN.

4 Only if the above two level validation is successful, the received delegate prefix is validated against the static ipv6 prefix pool configured in the destination context. If validation with the static pool is successful, then the delegate prefix is stored on the P-GW. If validation with the static pool fails, the delegate prefix is rejected and PDN is not set up.
After the PDN is set up, the UE or the CPE sends a delegated prefix request by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix, which it had stored earlier, in the DHCPv6 ADVERTISE message to the UE.

Next, the UE sends the DHCPv6 REQUEST message to the P-GW and the P-GW sends the DHCPv6 REPLY message to the UE, which completes the DHCPv6 handshake.

When the DHCPv6 RELEASE message is received from the UE, P-GW blocks data from any sources IP address from the delegated prefix pool. The delegated prefix is not released to the static ipv6 prefix pool from which it was allocated. If the DHCPv6 SOLICIT message is received again from the UE, the same delegate prefix is sent to the UE. The P-GW starts passing the data from the source address part of the said delegated prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests delegated prefix release by sending DHCPv6 RELEASE REQUEST message to the P-GW.

The DHCPv6 RELEASE REPLY message is not sent to the UE and no message is sent to the RADIUS server if:

- The delegated prefix is released when validity time configured in the DHCPv6 service expires
- When the PDN is cleared

Release triggered reason can be checked from the DHCPv6 statistics (output of the CLI command `show dhcpv6 statistics`), which are as follows:

```
Session Release Reasons: (dhcp-prefix-delegation)
PDNs Released: 3  Lease Exp Policy: 0
UE Initiated Release: 1  Other Reasons: 0
```

When the PDN is cleared, the delegate prefix is released to the static ipv6 prefix pool from which it was allocated.

**Configuring APN to Enable Prefix Delegation From RADIUS Server**

Use the following syntax to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the RADIUS Server.

```
config
context context_name
  apn apn_name
    ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic] allow-prefix-delegation
    pd-alloc-method no-dynamic
      ipv6 address prefix-delegation-len [48 | 52 | 56]
end
```

Notes:

- **dhcpv6-proxy**: Configures the IPv6 address from DHCP server for the APN.
- **dhcpv6-proxy**: Configures the IPv6 address from DHCP server for the APN.
- **local**: Configures the IPv6 address from the local pool configured.
- **no-dynamic**: Configures the IPv6 address as indicated by the authentication server.
- **allow-prefix-delegation**: Configures the APN to allow DHCPv6 prefix-delegation.
- **ipv6 address prefix-delegation-len**: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.
Verifying Prefix Delegation from the RADIUS Server
To verify the Prefix Delegation from the RADIUS Server, use the following show commands.

show dhcpv6 statistics

When APN is configured to receive Delegated Prefix from Radius Server, the sessions statistics is visible under CLI command output of `show dhcpv6 statistics` and displays the following output:

```
DHCPv6 Session Stats:
  Total Current: 0
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 0
  Local PD: 0
  Total Setup: 5
    DHCP Proxy: 0
    DHCP Server: 0
    DHCP PD: 0
    Radius PD: 1
    Local PD: 4
  Total Released: 5
    DHCP Proxy: 0
    DHCP Server: 0
    DHCP PD: 0
    Radius PD: 1
    Local PD: 4
```

Notes:
- The total current counter is incremented while sending request reply message to the UE.
- The total current counter is decremented while sending release reply message to the UE (in case of UE initiated release) in the following two cases:
  - on valid life timer expiry
  - when PDN is cleared
- The total current counter may be incremented/decremented multiple times during a PDN connection.
- The total setup counter is incremented multiple times during the PDN connection lifetime. For example, every-time when the SOLICIT message is processed, the PD is successfully allocated to the UE.
- The total release counter is incremented multiple times during a PDN connection lifetime. For example, everytime when the PD is released when DHCPv6 RELEASE message is processed from the UE and/or PD is released due to VALID lifetime timer expiry event. Along with this Session Release Reasons: (dhcp-prefix-delegation) counters are also incremented to the corresponding release reasons.
  - Hence in case of delegate prefix allocation from the RADIUS server, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all

This command displays the following output:

```
IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

show sub pgw-only full all
This command displays the following output:

```
IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56  Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

show sub saegw-only full all

This command displays the following output:

```
IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56  Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

### IPv6 Prefix Delegation from the Local Pool

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request the delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the prefix delegation from the local pool to the UE or the CPE.

To enable the prefix delegation from the local pool, first configure the APN on the P-GW. See Configuring APN for Private Pool Name, on page 99 and Configuring Prefix Delegation on Destination Context, on page 100.

#### How It Works

This section describes the functionality of the prefix delegation from the local pool.

1. Configure APN on the GGSN/P-GW/SAE-GW to enable the prefix delegation from the local pool. For configuration steps, see Configuring APN for Private Pool Name, on page 99.

2. Once the APN is configured, configure the pool on destination context. See Configuring Prefix Delegation on Destination Context, on page 100.

3. The PDN is first set up with default ipv6 prefix of length 64.

4. Once the PDN is set up, User Equipment (UE) or a Customer Premises Equipment (CPE) can request delegated prefix by sending DHCPv6 SOLICIT message to P-GW.

5. The P-GW then performs the following two level validation for the prefix length:

   **Level 1:** The prefix length requested in DHCPv6 SOLICIT message must be only one of the supported values, 48 / 52 / 56. For any other length, the SOLICIT is silently dropped at P-GW.

   **Level 2:** If level 1 validation is successful, then the following validation is done. If prefix-delegation-len is configured in the APN, then delegate prefix allocation of this length is attempted from the local private pool. If prefix-delegation-len is not configured in the APN, then delegate prefix allocation of length requested in SOLICIT message is attempted from the local private pool.
The requested length for the delegate prefix must match with the prefix-length configured for the private pool. The requested prefix length is as configured in the APN as ipv6 address prefix-delegation-len 52. If it is not configured in the APN, it may also be from the SOLICIT message. Configure the prefix length for the private pool by using the CLI command, `ipv6 pool ipv6-private prefix 5001::/1/48 prefix-length 52 private 0`. Only when these lengths match, delegated prefix allocation from the local pool is successful.

6 The UE or a CPE can request the delegated prefix by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix allocated from the local pool, in the DHCPv6 ADVERTISE message to the UE.

7 Next, the UE sends the DHCPv6 REQUEST message to the P-GW. The P-GW sends the DHCPv6 REPLY message to the UE, which completed the DHCPv6 handshake.
If the delegated prefix allocation from the local pool fails, the DHCPv6 SOLICIT message is silently dropped at the P-GW.

8 When the UE sends the DHCPv6 RELEASE message, the delegated prefix is released to the ipv6 prefix pool.
DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests prefix delegation released by sending DHCPv6 RELEASE REQUEST message to the P-GW.
DHCPv6 RELEASE REPLY message is not sent to UE if:
- The prefix delegation is released when validity time configured in the DHCPv6 service expires
- The PDN is cleared

If DHCPv6 SOLICIT message is received again from the UE, a new delegated prefix is allocated from the local pool and sent to the UE.

**Configuring APN to Enable Prefix Delegation From Local Pool**

**Configuration Overview**

To enable prefix delegation from a local pool, perform the following steps:

**Step 1** Configure the private pool name in the APN configuration mode, to be used for delegate prefix allocation.

**Step 2** Configure the APN to enable or disable IPv6 prefix delegation or default prefix delegation from the local pool.

Configuring APN for Private Pool Name

Use the following steps to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the local pool:

```plaintext
config
 context context_name
 apn apn_name
 ipv6 address delegate-prefix-pool pool_name
```
no ipv6 address delegate-prefix-pool
end

cfg
  context context_name
    apn apn_name
      ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic] allow-prefix-delegation
    pd.alloc-method local
      ipv6 address delegate-prefix-pool pool_name
      ipv6 address prefix-delegation-len [48 | 52 | 56]
  end

Notes:

• **delegate-prefix-pool**: Configures a pool of IPv6 address delegated prefix.
  *pool_name*: Name of the pool with IPv6 address delegated prefix.

• **no**: Disables the pool of IPv6 address delegated prefix.

• **dhcpv6-proxy**: Configures the IPv6 address from the DHCP server for the APN.

• **local**: Configures the IPv6 address from the local pool configured.

• **allow-prefix-delegation**: Configures the APN to allow DHCPv6 prefix-delegation.

• **ipv6 address prefix-delegation-len**: Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Configuring Prefix Delegation on Destination Context

Use the following configuration to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the Local Pool:

cfg
  context context_name
    ipv6 pool ipv6-private prefix 5001::1/48 prefix-length [48 | 52 | 56] private 0
  end

Notes:

• **ipv6 pool**: Modifies the current context's IP address pools by adding, updating, or deleting a pool. This command also resizes an existing IP pool.

---

**Important**

The ipv6 prefix pool must be of the type `private`.

**Verifying Prefix Delegation from the Local Pool**

To verify the Prefix Delegation from the local pool, use the following show commands.

show dhcpv6 statistics

When APN is configured to receive Delegated Prefix from the local pool, the sessions statistics is visible under CLI command output of **show dhcpv6 statistics** and displays the following output:

```
DHCPv6 Session Stats:
  Total Current: 0
  DHCP Proxy: 0
  DHCP Server: 0
  DHCP PD: 0
  Radius PD: 0
```
IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

Local PD: 0
Total Setup: 5
DHCP Proxy: 0
DHCP Server: 0
DHCP PD: 0
Radius PD: 1
Local PD: 4

Total Released: 5
DHCP Proxy: 0
DHCP Server: 0
DHCP PD: 0
Radius PD: 1
Local PD: 4

Notes: In case of delegate prefix allocation from local pool, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

show sub pgw-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

show sub saegw-only full all
The output of this command has been modified to display the following:

IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local

IPv6 Interface ID from the RADIUS Server
This feature allows the RADIUS/AAA Server to send an Interface-ID to the GGSN/P-GW/SAEGW service, in the Access-Accept message. This interface-id is used by these services and is communicated to the UE or the CPE. In this case, the GGSN/P-GW/SAEGW do not allocate a local interface-id. If the RADIUS/AAA server do not send an interface-id, then GGSN/P-GW/SAEGW allocate an interface-id locally and send it to the UE.

show apn statistics
Following CLI command can be used to see the total current active counter for Interface-ID allocation.

IP address allocation statistics:
Total IPv6 Interface IDs allocated:
AAA provided: 1
Locally Generated: 2
Limitations

Following are the limitations of the IPv6 Prefix Delegation feature:

• RADIUS ACCOUNTING messages do not support delegated prefix.

• Zero PL in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.

• NULL PD prefix in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.

• For PDN type v4v6, the dhcpv6-proxy method of allocation for the default prefix is not supported.

• The UE-requested Delegated Prefix in SOLICIT message is not supported. If the UE sends SOLICIT message requesting Delegated Prefix, it is rejected.

• One PD prefix per PDN is supported; multiple PD-prefixes per PDN are not supported.

• P-GW and GGSN do not support local-based and RADIUS-based allocation of both DHCPv6 prefix delegation and framed prefix delegation from the same pool. Hence the allocation is done from separate pools. Framed prefix received in the access-accept message is not part of the delegated prefix range.

Correction to GTPV2 Cause Source Being Incorrectly Set as S-GW

CSCux82063 - GTPv2 Cause Source incorrectly set as SGW of CC 64 in CSResp message

Applicable Products: SAEGW

Feature Changes

Consider the following scenario:

1. An SAEGW service is configured on the StarOS.
2. The S-GW ingress interface receives a Create Session Request with the Handover Indication Flag set.
3. The S-GW, being associated with the SAEGW service, checks with the SAEGW session manager for the presence or absence of a session on the P-GW without forwarding the PDU to the P-GW.
4. The session is not found and a Create Session Response is sent out with Cause Code 'Context NotFound'.

Even though the reject message is sent out by the S-GW, the message is logically rejected by the P-GW. Since there is a configured SAEGW service, the StarOS does not need to originate the message from the P-GW to save resources. External to the StarOS, the expectation is that the Cause Source IE (OI Flag) would indicate the presence or absence of the session at the P-GW.

Previous Behavior: The Cause Source IE (OI Flag) was not set, and therefore indicated that the reject originated from the S-GW.

New Behavior: The Cause Source IE is set and correctly indicates that the reject originates from the P-GW.

Customer Impact: This change was requested by a specific operator since their MME is expecting a set flag if a session is absent at the P-GW. If other operators' MMEs expect different behavior, then the issue is with the MME, according to the standards.
ECS Rules Written for IP Protocol

CSCuy14480 - ECS rules written for IP protocol 132 are not hit

Applicable Products: GGSN, P-GW, SAE-GW

Feature Changes

Previous Behavior: Earlier, SCTP downlink traffic passed through the default bearer instead of dedicated bearer, when the received packet was matched with the packet filter, which was configured in either of the following ways:

- Only source port or destination port was configured
- IP Address and port was configured

However, when the packet filter was configured for source and destination IP address, and the packet filter matched with the received packet, traffic passed through the dedicated bearer.

New Behavior: Now, SCTP downlink traffic passes through the dedicated when the received packet is matched with the packet filter, which was configured in either of the following ways:

- Source and destination IP address
- Only source port or destination port was configured
- IP Address and port was configured

P-GW Anchored and Co-located PDNs Incorrect Counters

CSCuy47807- Incorrect counters- PGW-anchored and Collocated PDNs by Operational Mode

Applicable Products: SAEGW

Feature Changes

Previous Behavior: There was a discrepancy in the CLI output of the command `show saegw-service statistics all`. The PGW-Anchor PDNS (Active) were pegged much higher than expected and the co-located PDNs (Active) were pegged much lower than expected. In addition to this, the 'Setup' and 'Release' stats were undervalued. This was observed because, the co-located stats were not pegged in the inter-tech handoff cases and the formula for setup/release statistics did not account for inter-tech handoff scenario. Statistics following under the following types were impacted during these cases.

- PDNs by PDN-Type and Operational-mode
- PDNs By Operational-Mode
- Bearers By Operational-Mode

New Behavior: Stats related issues in inter-tech handover cases are fixed and the above stats are now pegged appropriately.
SPGW Incorrectly Sending UDPv6 Packets

CSCuy78988 - SPGW incorrectly sending UDPv6 packets with 0x0 checksum against RFC2460

Applicable Products: GGSN, P-GW, SAEGW, S-GW

Feature Changes

Previous Behavior: Earlier, if the result of the UDPv6 checksum calculation is zero, GW used to send the same, which effectively disables checksum for that packet. This was not compliant with the RFC2460, which suggests the checksum value to be set to 0xFFFF if derived calculation is zero.

New Behavior: After the fix, the checksum value is set to 0xFFFF if the result checksum calculation is ZERO and the compliance is met.

Impact on customer: Packet drops might be seen at peer, which does not support of handling packet with 0xFFFF checksum as suggested by the RFC.

P-GW to Initiate CRA IE in UBReq Immediately

CSCuy95645 - PGW to initiate CRA IE in UBReq immediately

Applicable Products: P-GW, SAEGW

Feature Changes

For activating location reporting for a UE over Gx, RAR from PCRF was sent with the event trigger "USER_LOCATION_CHANGE". On receiving this event trigger, P-GW should typically send CRA IE with "Start Reporting " towards the MME to enable the Location-Change reporting for the UE in an MME.

Earlier, P-GW was not initiating Update Bearer Request procedure explicitly to inform only CRA IE and was relying on any other procedure like QoS change happening at same time or in future. This resulted in delay in updating required action at the MME. After this feature change, P-GW would immediately initiate Update Bearer Request, even for updating only CRA IE, if there are no other changes detected in RAR received with ULI_LOCATION_CHANGE event trigger. If there are other changes detected in RAR, CRA IE would be combined with Update Bearer Request initiated for the same.

Previous Behavior: Earlier, P-GW initiated update Bearer procedure was not triggered when the ULI event trigger was received from a RAR than a CCA-U.

New Behavior: Now, P-GW initiated update bearer procedure for CRA IE is triggered, if RAR is received with the ULI trigger.

IPv4v6 PDN Rejection

CSCuz51684 - IPv6 pdn rejected if UE req v6 addr n Access-Accept has Framed Prefix

Applicable Products: P-GW, SAEGW
Feature Changes

IPv4 or IPv6 PDN were rejected, when the UE requests IPv4 or IPv6 static address when the CLI command `ipv6 address alloc-method no-dynamic` was configured under the APN. However, IPv4v6 PDN was accepted when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` was configured.

**Old Behavior:** Earlier, IPv4v6 PDN was accepted when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` was configured.

**New Behavior:** Now, IPv4v6 PDN is rejected when the UE requested static IPv6 address when the CLI command `ipv6 address alloc-method no-dynamic` is configured.

L2TP Password Behavior Parity Between P-GW and GGSN

**Applicable Products:** P-GW, SAEGW

**Feature Changes**

GGSN L2TP call received from the UE without PCO IE in CSReq is successful. However, P-GW/SAEGW fails PPP authentication for a L2TP call if PCO IE is not received or PCO IE is received without authentication information in the Create Session Request. As a result the call is rejected.

A new keyword has been added to the existing CLI command `PPP` at the APN level. This CLI command allows L2TP P-GW/SAEGW call's PPP authentication to be successful even if:

- PCO IE is not received in CSReq
- PCO IE is not received
- PCO IE is received without authentication information in the Create Session Request.

**Old behavior:** Earlier, P-GW/SAEGW failed PPP authentication for a L2TP call if PCO IE was not received or PCO IE was received without authentication information in the Create Session Request. As a result, the call was rejected.

**New behavior:** A new CLI keyword has been added to the existing CLI command `PPP` at the APN level. When this CLI command is enabled, P-GW/SAEGW allows PPP authentication for a L2TP call even if:

- PCO IE is not received
- PCO IE is received without the authentication information in the Create Session Request.

As a result, the call is successful.

When the CLI command is disabled, P-GW/SAEGW fails PPP authentication information in the Create Session Request. As a result, the call is rejected.

**Impact on the Customer:** Successful P-GW/SAEGW L2tp calls can be established even if PCO IE is not received or PCO IE is received without authentication information in Create Session Request.
Command Changes

l2tp allow-auth-without-pco

A new keyword has been added to the existing CLI command PPP at the APN level. This command allows L2TP P-GW/SAEGW call's PPP authentication to be successful even if:

- The PCO IE is not received in CSReq
- The PCO IE is not received
- The PCO IE is received without authentication information in the Create Session Request.

```
configure
  context context_name
    apn apn_name
      ppp l2tp allow-auth-without-pco
      { default | no } ppp l2tp allow-auth-without-pco
    end
```

Notes:

- **l2tp**: Configures PPP L2TP specific parameters
- **allow-auth-without-pco**: allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request.
- **Default Behavior**: P-GW does not allow PPP authentication for a L2TP call to go through successfully when PCO IE is not received in Create Session Request.

Performance Indicator Changes

```
show apn <apn_name> | all
```

This command has been modified to display the following fields:

- ppp keep alive period: 32
- ppp mtu: 1500
- ppp auth without pco for l2tp: Enabled
- ppp auth without pco for l2tp: Disabled

```
show config verbose output
```

If the CLI command `ppp l2tp allow-auth-without-pco` is configured, the output of this command is modified to display the following:

- `ppp l2tp allow-auth-without-pco`

If `no ppp l2tp allow-auth-without-pco` or `default ppp l2tp allow-auth-without-pco` or `no configuration` is done, there is no change in the output of this show command.
show apn <apn_name>

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

<table>
<thead>
<tr>
<th>Preference Rule-Definition</th>
<th>Selected-APN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PDP Type = ipv4 telenor.ipv4v6</td>
</tr>
<tr>
<td>2</td>
<td>PDP Type = ipv6 telenor.nat64</td>
</tr>
<tr>
<td>3</td>
<td>PDP Type = ipv4v6</td>
</tr>
<tr>
<td>Roaming mode = roaming telenor.nat64</td>
<td></td>
</tr>
</tbody>
</table>

Retaining Old IMEI Values

CSCuz67967 - Logging when GTPC TEID reuse with different IMEI in MBR

**Applicable Products**: P-GW, SAEGW

**Feature Changes**

For a PDN session, P-GW receives MBReq with IMEI value which is different from old IMEI value.

**Old behavior**: On receiving MBReq with different IMEI value, P-GW replaces old IMEI information with the new IMEI value and start using the new IMEI information on all interfaces. This impacts the P-GW CDRs generated for that PDN session. P-GW CDRs generated before the MBReq uses the old IMEI value and P-GW CDRs generated after the MBReq uses the new IMEI value, which is wrong and has impact on billing and revenue loss for the customer.

**New behavior**: If, P-GW receives MBReq with IMEI value which is different from old IMEI value, P-GW ignores the new IMEI value received as part of MBReq and retains the old IMEI information. Hence, PGW-CDRs generated before or after MBReq now use the old IMEI value. As a result, there is no impact on billing.

SAEGW Enhancements for 19.3

There are no SAEGW enhancements for this release.

SAEGW Enhancements for 19.2

This section identifies all of the SAEGW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SAEGW Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

### Enforcing Throttling to Avoid Overusage

CSCuw83987 - GW does not enforce throttling causing over usage

#### Feature Changes

The fix implemented for CSCuw89387 has resulted in a behavior change.

Consider the following scenario:

1. A P-GW has an APN-AMBR value of a/b.
2. A RAR then is received with an APN-AMBR value of x/y.
3. A UBRq request is sent out, and the UBRsp is received with a Temp failure.
4. Now a second RAR is received with an APN-AMBR value of a/b.

**Previous Behavior:** Only one UBRq is sent out with the value of x/y.

**New Behavior:** The UBRq started in step 3 is suppressed and no UBRq is generated.

**Customer Impact:** No UBRq is generated. The PCRF and P-GW will be in sync with the APN-AMBR value as 'a/b'.

### License Control for Standardized PMIP Protocol Support for NEMO

CSCux14378, CSCux18618 - License Control for standardized PMIP Protocol Support for NEMO

Standardized PMIP Protocol Support for NEMO is now a license-controlled feature.

Contact your Cisco account or support representative for detailed licensing information.
**Feature Changes**

The fix implemented for CSCuw89387 has resulted in a behavior change.

Consider the following scenario:

1. A P-GW has an APN-AMBR value of a/b.
2. A RAR then is received with an APN-AMBR value of x/y.
3. A UBR req request is sent out, and the UBRsp is received with a Temp failure.
4. Now a second RAR is received with an APN-AMBR value of a/b.

**Previous Behavior:** Only one UBR req is sent out with the value of x/y.

**New Behavior:** The UBR req started in step 3 is suppressed and no UBR req is generated.

**Customer Impact:** No UBR req is generated. The PCRF and P-GW will be in sync with the APN-AMBR value as 'a/b'.

---

**Traffic Shaping at the APN-AMBR Data Rate Level**

CSCuw23766 - Traffic Shaping; CSCuw33511 - Reduce Policing bucket interval from 100 ms to 10 ms.

**Applicable Products:** GGSN, P-GW, SAEGW

---

**Feature Changes**

❄️ **Important**

In StarOS release 19.2, this feature is supported as lab quality only. With release 19.2.1, this feature is now available as fully qualified Deploy Quality.

❄️ **Important**

Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Traffic Shaping is a rate limiting method similar to Traffic Policing, but provides a buffer facility for packets exceeding the configured limit. Once packets exceed the data-rate, the packet is queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data, the system can be configured to either drop the packets or retain it for the next scheduled traffic session.

Traffic will be shaped to the configured APN-AMBR value. Previously, data carried on non-GBR bearers was policed at the configured APN-AMBR rate. APN-AMBR policing dropped the data that did not match the configured APN-AMBR. With APN-AMBR traffic shaping, non-GBR data that does not match the configured APN-AMBR rate will be buffered. When enough memory tokens are available, the data will be transmitted. In addition, operators still have the option to allow operators to drop the data when the buffer limit is reached.
Command Changes

apn-ambr

The **shape** and **transmit-when-buffer-full** keywords are now available in *APN Configuration Mode* for traffic shaping on the GGSN, P-GW and SAEGW.

```
configure
  context context_name
  apn apn_name
    apn-ambr rate-limit direction { downlink | uplink } | violate-action { shape |
    transmit-when-buffer-full } |
    | default | no | apn-ambr rate-limit direction { downlink | uplink }
end
```

Notes:

- **shape [transmit-when-buffer-full]**: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.

apn-ambr

The **token-replenishment-interval** keyword has been added to the **apn-ambr** command in *APN Configuration Mode*. This token replenishment interval is used for both APN AMBR traffic policing and traffic shaping. Operators have the option of using the default interval (100ms) or configuring a lower token replenishment interval of 10ms. Reducing the interval to 10ms helps reduce the queuing time required by the 100ms interval for a given packet size.

```
configure
  context context_name
  apn apn_name
    apn-ambr rate-limit token-replenishment-interval duration_msecs
end
```

Notes:

- Where **token-replenishment-interval** is the time duration, in milliseconds, to be used for APN AMBR-based traffic policing and shaping.
- Valid entries are 10 or 100 milliseconds. The default is 100 milliseconds.

apn-ambr

The **milliseconds** variable has been added to the **auto-readjust duration** keyword for the **apn-ambr** command in *APN Configuration Mode*. This variable allows operators to configure the **auto-readjust duration** in increments of 100 milliseconds.

```
configure
  context context_name
  apn apn_name
    apn-ambr rate-limit direction { downlink | uplink } | burst-size { auto-readjust duration milliseconds integer 100...900} |
    | default | no | apn-ambr rate-limit direction { downlink | uplink }
end
```

Notes:
Where **milliseconds** is the time duration, in milliseconds, to be used for the **auto-readjust duration** function in APN AMBR-based traffic policing and shaping.

- Valid entries are from 100 to 900 milliseconds, in increments of 100 milliseconds. For example, 100, 200, 300 and so on.

### Traffic Shape

The new **traffic shape** command has been added to **Global Configuration Mode**. This command enables operators to configure the maximum limit for data buffering during APN AMBR traffic shaping.

```
configure
  traffic shape max-buffer-size sessmgr  MBs subscriber MBs
end
```

**Notes:**

- **sessmgr MBs**: Specifies the amount of memory allocated towards buffering session manager instances during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The **sessmgr MBs** setting should be larger than the **subscriber MBs** setting.

- **subscriber MBs**: Specifies the amount of memory allocated towards buffering subscriber traffic during APN AMBR traffic shaping. Valid entries are from 1 to 100 MB. The **subscriber MB** setting should be less than the **sessmgr MB** setting.

**Caution**

Standard size buffers (500, 2k, and 10k bytes) are used for buffering packets to avoid memory fragmentation. As a result, there may be additional memory overhead in the memory used for buffering. The buffer limit in the above configuration refers to actual effective bytes used to store packets. Use caution to use appropriate buffer limits, so that the system does not significantly affect the overall Session Manager memory requirement for sessions.

### Performance Indicator Changes

#### show configuration verbose

The output of this command has been enhanced to provide APN AMBR traffic shaping parameters for the GGSN, P-GW, and SAEGW, if configured.

- apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape (if configured without the **transmit-when-buffer-full** option).

- apn-ambr rate-limit direction uplink burst-size auto-readjust duration <secs> violate-action shape transmit-when-buffer-full (if configured with the **transmit-when-buffer-full** option).

The output of this command has also been enhanced to show the **token-replenishment-interval** for APN AMBR traffic shaping and policing, if configured.

- **apn-ambr rate-limit token-replenishment-interval <milliseconds>**

The output of this command has also been enhanced to provide the maximum buffer size allocated for traffic shaping for both subscribers and the session manager.
• traffic shape max-buffer-size sessmgr <no. of MB> subscriber <no. of MB>

**show subscriber pgw-only/ggsn-only/saegw-only full all**

Command output for each of these commands has been enhanced to show APN AMBR traffic shaping configuration parameters and statistics.

- APN AMBR shaping:
- Token replenishment interval (ms):
- Downlink traffic-shaping: <Enabled or Disabled>
- APN-AMBR (bps):
- Buffer full action: <drop or transmit>
- Burst Size:
- Auto Readjust: <Enabled or Disabled>
- Auto Readjust Duration (ms):
- Peak Burst size (bytes):
- Guaranteed burst size (bytes):
- Queued data (packets):
- Queued data (bytes):
- Drop count (packets):
- Drop count (bytes):
- Buffer Full Packets Fwd:
- Buffer Full Bytes Fwd:
- Packets Forwarded:
- Bytes Forwarded:
- Uplink traffic shaping: <Enabled or Disabled>
- APN-AMBR (bps):
- Buffer full action: <drop or transmit>
- Burst Size:
- Auto Readjust: <Enabled or Disabled>
- Auto Readjust Duration (ms):
- Peak Burst Size:
- Guaranteed burst size (ms):
- Queued data (packets):
- Queued data (bytes):
- Drop count (packets):
Virtual APN Selection Based on CC-Behavior

CSCuu43329 - Virtual APN selection based on all 16 bits of charging characteristics.

**Applicable Products:** GGSN, P-GW, SAEGW

### Feature Changes

Virtual APN Selection feature enables an operator to select Virtual APN based on all 16 bits of Charging Characteristics for GGSN, P-GW, and SAEGW nodes. Earlier, virtual APN selection was possible only on the basis on 4 cc-profile bits. With this feature, now an operator can select a Virtual APN on the basis on 4 cc-profile bits and 12 cc-behavior bits or on the basis on complete 16 cc-behavior bits. This selection can be done with the help of a CLI.

**Previous Behavior:** Earlier, Virtual APN selection was possible on the basis of 4 cc-profile bits.

**New Behavior:** Now, Virtual APN selection can now be done on the basis of 4 cc-profile bits and 12 cc-behavior bits or complete 16 cc-behavior bits.

**Customer Impact:** Virtual APN can be selected based on all 16 bits of Charging Characteristics.

### Command Changes

**virtual-apn preference**

New keywords **pre-rel-9.1-cc-behavior** and **cc-behavior** have been added to the command **virtual-apn preference** to support Virtual APN selection on the basis of all charging characteristics.
cc_behavior_value | msin-range from msin_range_from to msin_range_to | rat-type { eutran | gan | geran | hspa | utran | wlan } | msisdn-range from msisdn_start_range to msisdn_to_range | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } ]

Notes:

• pre-rel-9.1-cc-behavior cc_behavior_value Specifies the behavior charging characteristics bits in 12 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x341, then 0x34 corresponds to B12-B5 [MSB] and 0x1 corresponds to B4-B1 [Least significant nibble] of CC behavior). cc_behavior_value must be a hex value in the range 0x0000 to 0xFFFF.

• cc_behavior cc_behavior_value Specifies the behavior charging characteristics bits in 16 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x3412, then 0x34 corresponds to B15-B8 [MSB] and 0x12 corresponds to B7-B0 [LSB] of charging char) cc_behavior_value must be a hex value in the range 0x0000 to 0xFFFF.

Performance Indicator Changes

show apn <apn_name>

The following fields have been added to the output of this command.

Virtual APN Configuration:
Preference | Rule-Definition | Selected-APN
--- | --- | ---
1 | CC Profile Index = 1 | cisco.ipv4
2 | CC Profile Index = 2, RAT Type = gan | intershat2
3 | CC Profile Index = 2 | cisco.ipv4
4 | CC Profile Index = 3 | cisco.ipv4
5 | CC Behavior Bits = 0x3412 | gan
6 | CC Behavior Bits = 0x104 | cisco.ipv4
7 | IMSI-MCC = 100, IMSI-MNC = 100 | cisco.ipv4
8 | IMSI-MCC = 100, IMSI-MNC = 100 | cisco.ipv4
9 | CC Profile Index = 2 | cisco.ipv4
10 | CC Behavior Bits = 0x341 | cisco.ipv4
11 | CC Behavior Bits = 0x104 | cisco.ipv4
12 | CC Behavior Bits = 0x104 | cisco.ipv4
13 | CC Behavior Bits = 0x1204 | cisco.ipv4

show config

The following fields have been added to the output of this command.
apn starent.ipv4
selection-mode sent-by-ms
accounting-mode gtp
ip context-name pgw-gi
virtual-apn preference 1 apn cisco.ipv4 cc-profile 1
virtual-apn preference 2 apn cisco.ipv4 cc-profile 1 rat-type eutran
virtual-apn preference 3 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104
virtual-apn preference 4 apn pqr.com cc-profile 2 pre-rel-9.1-cc-behavior 0x104 rat-type
gan
virtual-apn preference 5 apn star.com cc-behavior 0x1204
virtual-apn preference 6 apn star.com cc-behavior 0x1204 rat-type gan
virtual-apn preference 7 apn abc2.com mcc 100 mnc 100 cc-profile 1
virtual-apn preference 8 apn pqr2.com mcc 100 mnc 100 cc-profile 2 pre-rel-9.1-cc-behavior
Virtual APN Selection Based On PDP-Type

CSCuo61924 - Virtual APN based on PDP type.

**Applicable Products:** GGSN, P-GW, and SAEGW

**Feature Changes**

The current implementation of selection of virtual APN is based on various criteria and a call received on a selected APN can be forwarded to another APN based on the configured criteria. This feature enables the operator to select the Virtual APN on the basis of PDP-type and PDP-type for roamers. For this, PDP-type rules for PDP-types IPv4, IPv6, and IPv4v6 have been added to the existing Virtual APN rules. Also, roaming
**mode-roaming** has been implemented as a secondary option to PDP type enable the operator to select the Virtual APN on the basis on PDP-type for roamers.

**Previous Behavior:** Earlier, Virtual APN was selected on the basis on various factors such as IMSI and MSISDN. PDP-type and PDP-type for roamers were not the basis for selection.

**New Behavior:** Now, an existing CLI virtual-apn preference has been modified to enable the Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

### Command Changes

**virtual-apn preference**

New keyword **pdp-type** has been added to the command **virtual-apn preference** to support Virtual APN selection on the basis of PDP-type and PDP-type for roamers.

```bash
configure
c   context context_name
   apn apn_name
       virtual-apn preference priority apn apn_name | access-gw-address { ip_address | ip_address/mask } | bearer-access-service service_name | cc-profile cc_profile_index [ pre-rel-9.1-cc-behavior cc_behavior_value ] | rat-type { eutran | gan | geran | hspa | utran | wlan } | cc-behavior cc_behavior_value | rat-type { eutran | gan | geran | hspa | utran | wlan } | domain domain_name | IPv4 | IPv6 | mcc mcc_number mcc_number cc-profile cc-profile_index | pre-rel-9.1-cc-behavior cc_behavior_value | msin-range from msin_range_from to msin_range_to | rat-type { eutran | gan | geran | hspa | utran | wlan } | mscn-range from mscn_start_range to mscn_to_range | rat-type { eutran | gan | geran | hspa | utran | wlan } | pdp-type { ipv4 | ipv6 | ipv4v6 } | roaming-mode { roaming } | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } | no virtual-apn preference priority
end
```

**Notes:**

- **pdp-type** Configures pdp-type rule.
- **ipv4** Configures Virtual APN rule for ipv4 addresses.
- **ipv6** Configures Virtual APN rule for ipv6 addresses.
- **ipv4v6** Configures Virtual APN rule for ipv4v6 addresses.
- **roaming-mode { home | roaming | visiting }** Supports separate PDP context or PDN connection processing for roaming subscribers.

### Performance Indicator Changes

**show apn <apn_name>**

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

<table>
<thead>
<tr>
<th>Virtual APN Configuration</th>
<th>Selected-APN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference Rule-Definition</td>
<td></td>
</tr>
<tr>
<td>1 PDP Type = ipv4 telenor.ipv4v6</td>
<td></td>
</tr>
<tr>
<td>2 PDP Type = ipv6 telenor.ipv6v4v6</td>
<td></td>
</tr>
</tbody>
</table>
3  PDP Type = ipv4v6
Roaming mode = roaming telenor.nat64

show pgw-service stats all

This command displays the virtual-apn configuration based on pdp-type and pdp-type along with roaming-mode. The output of this command has been modified to display the following fields:

Virtual APN Configuration:
Preference Rule-Definition Selected-APN
1  PDP Type = ipv4 telenor.ipv4v6
2  PDP Type = ipv6 telenor.nat64
3  PDP Type = ipv4v6
Roaming mode = roaming telenor.nat64

show saegw-service stats all function pgw

This command has been modified to include counters to indicate the number of PDNs setup and rejected for Virtual APNs selected on the basis of PDP-type at the service level. Modified output includes the following fields:

VAPNs Selected Based on Configured PDP-Type
IPv4: Setup: 8  Rejected: 5
IPv6: Setup: 8  Rejected: 5
IPv4v6: Setup: 8  Rejected: 5

SAEGW Enhancements for 19.1

There are no SAEGW enhancements for StarOS release 19.1.

SAEGW Enhancements for 19.0

This section identifies all of the SAEGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the SAEGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SAEGW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
• MVG Enhancements
• NAT Enhancements
• SNMP MIB Enhancements
• System and Platform Enhancements

**IMSI Added to Error Logs**

CSCut68271 - IMSI not included in Error Logs

**Feature Changes**

**Previous Behavior:** When enabled, the following system error logs did not include the international mobile station identifier (IMSI) in the log details:

- gtpc 47595 error
- sessmgr 11826 error
- sessmgr 11831 error

**New Behavior:** The above error logs now contain the IMSI in the log details.

**IMSI/IMEI Available in System Event Logs of Type Error and Critical**

CSCuu51587, CSCut68271 - Inclusion of IMSI/IMEI in logs

**Applicable Products** = GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

**Previous Behavior:** The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all system event logs of type error and critical.

**New Behavior:** The GGSN/P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available.

---

**Important**

Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.
### Table 6: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format &quot;[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d&quot;</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Recover call from CRR failed for callid:0x%x reason=%s&quot;</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Ran out of session handles&quot;</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td><strong>Modified Events</strong></td>
<td></td>
</tr>
<tr>
<td>139001</td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td>191006</td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td>10034</td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s&quot;. For example &quot;[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td>12668</td>
<td>Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot;</td>
</tr>
<tr>
<td>12774</td>
<td>Represents pgw_purge_invalid_crr in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot;</td>
</tr>
<tr>
<td>12855</td>
<td>Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td>12857</td>
<td>Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>12858</td>
<td>Represents ncqos_nrxx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>12859</td>
<td>Represents ncqos_nrxx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%u&gt;: pf_id_bitmap 0x%x and tft_opcode: %d&quot;</td>
</tr>
<tr>
<td>12860</td>
<td>Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12861</td>
<td>Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td>12862</td>
<td>Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state state:&lt;%s&gt;, [event:&lt;%s&gt;]&quot;</td>
</tr>
<tr>
<td>11830</td>
<td>Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
<tr>
<td>11832</td>
<td>Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Call line has no non-GBR bearer to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0x%x&gt; not found.&quot;</td>
</tr>
<tr>
<td>12960</td>
<td>Represents gtp_pdp_type_mismatch in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN %s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>11282</td>
<td>Represents pcc_inf_err_info in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents collision_error in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d&quot;</td>
</tr>
<tr>
<td>11917</td>
<td>Represents rcvd_invalid_bearer_binding_req_from_acs in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr %d: Received invalid bearer binding request from ACS.&quot;</td>
</tr>
<tr>
<td>11978</td>
<td>Represents saegw_uid_error in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11994</td>
<td>Represents unwanted_pcc_inf_setup_req_error in format &quot;[IMSI &lt;IMSI&gt;] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface.&quot;</td>
</tr>
<tr>
<td>140005</td>
<td>Represents ue_fsmIllegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled UE event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>140006</td>
<td>Represents pdn_fsmIllegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled PDN event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
</tbody>
</table>
Command Changes

logging

The `include-ueid` keyword has been added to the `logging` command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
configure
  logging include-ueid
  no logging include-ueid
end
```

Performance Indicator Changes

show configuration

The output of this command has been enhanced to indicate if the `logging` command is enabled with the `include-ueid` keyword.

- `logging include-ueid`
- `no logging include-ueid`

"Newcall policy reject" Enhancement for Releasing Existing Calls

CSCuu21036 - Newcall policy reject enhancement for releasing existing calls

Applicable Products = GGSN, P-GW, SAEGW, S-GW

Feature Changes

If the newcall policy is set to `reject release-existing-session` and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).
Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Command Changes**

**newcall policy**

The keyword `release-existing-session` has been added to this command to reject and release existing IMSI/IMEI session(s) when newcall arrives.

```
newcall policy saegw-service { all | name service_name } reject [ release-existing-session ]
no newcall policy saegw-service { all | name service_name }
```

Notes:

- `reject release-existing-session`: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Disabled by default.

Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions.

**Performance Indicator Changes**

**show egtpc statistics verbose**

The following new field has been added to indicate such calls released:

- NewCall Reject Existing Sessions Released

**Support for S2a Standard-Based Call Flow on the SAEGW**

CSCut88293 - SAEGW S2a support

**Feature Changes**

This feature extends the support for Wifi to LTE handovers using Make and Break for the SAEGW service on the S2a interface. Multi-PDN handovers are also supported for SAEGW as part of this feature. This feature supports the use of WiFi/LTE handovers for the P-GW as a part of an SAEGW service, as well as handovers for Multi-PDN calls. So, the SAEGW now supports WiFi (S2a)/LTE handoffs using Make and Break.
Command Changes

interface-type interface-pgw-ingress

The existing s2a option is available in the interface-type interface-pgw-ingress command in eGTP Service Configuration Mode to provide GTP-based S2b interface support on the SAEGW.

```config
context  ingress_context_name
egtp-service  egtp_service_name
  interface-type interface-pgw-ingress  s2a
end
```

Disable S2a interface support by entering the following existing commands:

```config
context  ingress_context_name
egtp-service  egtp_service_name
  interface-type interface-pgw-ingress
end
```

Performance Indicator Changes

SAEGW Schema

The following bulk statistics have been added to the SAEGW schema for this feature:

- pgw-handoverstat-ltetos2agtpat
- pgw-handoverstat-ltetos2agtpsucc
- pgw-handoverstat-ltetos2agtpfail
- pgw-handoverstat-s2agtpolteatt
- pgw-handoverstat-s2agtpoltesucc
- pgw-handoverstat-s2agtpoltefail

```
show saegw-service statistics all
```

This command provides information on subscribers connected over the S2b interface via all configured SAEGW services.

- VPN Name:
- Subscribers Total:
- Active:
- S6b Assume Positive
- PDNs Total:
- Active:
• Released:
• Setup:
... 
• PDNs by PDN-Type and Operational-mode:
  • Colocated PDNs:
    • IPv4 PDNs:
      • Active:
      • Released:
      • Setup:
      ... 
      • Bearers Total:
        • Active:
        • Released:
        • Setup:
        • Bearers by Operational-Mode:
          • SGW-Anchored Bearers:
            • Active:
          • PGW-Anchored Bearers:
            • Active:
          • GGSN-Anchored Bearers:
            • Active:
          • SGW-PGW Collocated Bearers:
            • Active
          ... 
• Data Statistics Per PDN-Type
• IPv4 PDNs
• Uplink:
  • Total Pkts:
  • Total Bytes:
• Downlink:
  • Total Pkts:
  • Total Bytes:
show saegw-service statistics all function pgw

The output of this command has been enhanced to provide detailed PDN, handover and data statistics for S2a subscribers per P-GW function.

- Subscribers Total:
  - Active:
  - S6b Assume Positive:
  - PDNs By PDN-Type:
    - IPv4 PDNs:
      - Active:
      - Setup:
      - Released:
      - ...
  - Bearers Total:
    - Active:
    - Setup:
    - Released:
    - Rejected:
    - ...
    - S2bGTP-to-LTE handover
      - Attempted:
      - Succeeded:
      - Failed:
      - LTE-to-S2bGTP handover:
        - Attempted:
        - Succeeded:
        - Failed:
        - S2aGTP-to-LTE handover:
          - Attempted:
          - Succeeded:
          - Failed:
          - LTE-to-S2aGTP handover:
            - Attempted:
            - Succeeded:
• Failed:
• Data Statistics per Interface:
  • S5U/S8U/S2bU/Gn/Gp Total Data Statistics
• Uplink:
  • Total Pkts:
  • Std QCI(Non-GBR):
  • Std QCI(GBR):
• Downlink:
  • Total Pkts:
  • Std QCI(Non-GBR):
  • Std QCI(GBR):
  •

```shell
show session subsystem facility sessmgr service-type pgw-ingress debug-info verbose
```

Command output has been enhanced to provide detailed Session Manager, User data, WLAN data, WLAN connection, and Interface type statistics for subscribers connected via the S2a interface.

• (n) Session Managers
• Total calls arrived
• Total calls rejected
• Total calls connected
• Total calls failed
• Total calls disconnected
• Total handoffs
• Total renewals
• ...
• User Data statistics
• Data octets from User:
  • SIP Data octets:
  • MIP Data octets:
• Data octets from User:
  • SIP Data octets:
  • MIP Data octets:
• Data Octets to User:
  • SIP Data octets:
• MIP Data octets:
  • Data packets from User:
  • Data packets to User:
  • ...
• WLAN Data Statistics
  • packets to User:
  • octets to User:
  • packets from User:
  • octets from User:
  • ...
• Interface Type Statistics PGW Only:
  • LTE S5/S8 Connection Statistics
    • Total Sessions
    • Total calls arrived
    • Total calls connected
    • Total calls disconnected
  • S2bGTP Connection Statistics
    • Total Sessions
    • Total calls arrived
    • Total calls connected
    • Total calls disconnected
  • S2aGTP Connection Statistics
    • Total sessions
    • Total calls arrived
    • Total calls connected
    • Total calls disconnected
    • ...
• Number of PGW Services:
  • ...
• S2bGTP Data Statistics
  • Packets to User
  • Octets to User
  • Packets from User
• Octets from User
• Packets from User dropped (S2b to LTE HO)
• Packets to User dropped (S2b to LTE HO)
• S2aGTP Data Statistics
• Packets to User
• Octets from User
• Packets from User
• Octets from User
• Packets from User dropped (S2a to LTE HO)
• Packets to User dropped (S2a to LTE HO)

show subscribers saegw-only full all

The output of this command has been enhanced to provide detailed subscriber and S2a interface information for subscribers connected over the S2a interface.

• Username
• SAEGW Call mode:
• Subscriber Type:
• Status:
• State:
• Bearer State:
• Connect Time
• ...
• S2B interface
• pgw c-addr:
• pgw u-addr:
• pgw c-teid
• pgw u-teid
• ePdg c-addr:
• ePdg u-addr
• ePdg c-teid
• ePdg u-teid
• S2a interface
• pgw c-addr
• pgw u-addr
- pgw c-teid
- pgw u-teid
- cgw c-addr
- cgw u-addr
- cgw c-teid
- cgw u-teid
- input pkts
- input bytes
- input bytes dropped
- input pkts dropped
- output pkts
- output bytes
- output bytes dropped
- output pkts dropped

**show subscribers saegw-only interface-type S2aGTP**

The output of this command has been enhanced to provide subscriber information for subscribers connected via the S2a interface:

- CALLID
- IMSI/IMEI
- EBI v IP
- APN
- TIME-IDLE
- Total subscribers matching specified criteria:

**show subscribers summary pgw-address**

This command shows active and dormant statistics for subscribers connected via the S2a interface via a given P-GW IP address.

- Total Subscribers:
- Active:
- Dormant:
- LAPI Devices
- pdsn-simple-ipv4:
show subscribers summary interface-type S2aGTP

This command shows interface-specific access statistics for subscribers connected via the S2a interface.

- Total Subscribers:
- Active:
- Dormant:
- LAPI Devices:
- psdn-simple-ipv4:
- psdn-simple-ipv6:
S-GW Collision Handling Enhancement

CSCuu19566 - S-GW Collision Handling

Feature Changes

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The S-GW has been enhanced to process collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification (DDN) message with Create Bearer Request or Update Bearer Request.
Previous Behavior:

1. Whenever a Create Bearer Request (CBReq) and Modify Bearer Request (MBReq) [Inter MME/Inter RAT (with or without ULI change)] were detected at the S-GW ingress interface, the S-GW rejected the current CBReq and would send a failure message to the P-GW. The S-GW would then handle the incoming MBReq.

2. Whenever an Update Bearer Request (UBReq) and MBReq [Inter MME/Inter RAT (with or without ULI change)] were detected at the S-GW ingress interface, the S-GW rejected the current UBReq and would send a failure message to the P-GW. The S-GW would then handle the incoming MBReq.

3. Whenever a Downlink Data Notification (DDN) was ongoing, the S-GW rejected the incoming Create Bearer Request (CBReq) or Update Bearer Request (UBReq) and a failure message was sent to the P-GW.

New Behavior:

1. An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change)] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.

2. An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change)] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.

3. The Downlink Data Notification (DDN) message transaction is dis-associated from bearers. So Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

Customer Impact: No S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.

Performance Indicator Changes

show egtp statistics verbose

The output of this command has been enhanced to provide information on GTPv2 message collisions at the S-GW ingress interface, including:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5).

- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.

- **New Proc (Msg Type)**: The new procedure and message type.

- **Action**: The pre-defined action taken to handle the collision. The action can be one of:

  - **No Collision Detected**
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old**: Abort the original message handling and processes the new message.
  - **Reject New**: The new message is rejected, and the original (old) message is processed.
• Silent Drop New: Drop the new incoming message, and the old message is processed.

• Parallel Hndl: Both the original (old) and new messages are handled in parallel.

• Buffer New: The new message is buffered and processed once the original (old) message processing is done.

• Counter: The number of times each collision type has occurred.

---

![Image](image1.png)

**Important**

The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

---

**Standardized PMIP Protocol Support for NEMO on the ASR 5500**

CSCuu29938 - PMIPv6/LMA support for IPv4 prefix delegation on ASR5500

**Feature Changes**

![Image](image2.png)

**Important**

Use of NEMO requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The Network Mobility (NEMO) solution allows the dynamic advertisement of remote IPv4 networks to a NEMO Home Agent (HA) and Local Mobility Anchor (LMA) function on the enterprise gateway, which in turn propagates those networks to the enterprise. The remote networks behind a MR (Mobile Router) become routeable within the enterprise network, which permits the enterprise to establish communication between IP devices behind a mobile router and IP devices on the Enterprise VPN network in any initiated direction. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Prior to StarOS release 19.0, the NEMO solution for an SAEGW running on the ASR 5500 used the MIPv4 protocol-based proprietary solution between the MR and the NEMO HA service. In StarOS release 19.0, support has been added for the standardized PMIPv6 protocol between the NEMO and an SAEGW running on the ASR 5500.

PMIPv6 and PMIP are standardized by IETF and specified in RFC 5213.

This enhancement provides the capability to transmit data to and from devices (with IPv6 addresses) behind the wireless gateway (router, firewall, or switch) at the operator's location. This allows the operator to interact from allowable private and public networks to devices behind the gateway without managed hardware, end user software clients, or through having to manage large complex meshed encrypted tunnels.

**Important**

The IPv6 transmission between MAG and LMA for NEMO is not supported.
Command Changes

permission

The nemo keyword has been added to the permission command in APN Configuration Mode. It authorizes the user(s) for the NEMO service.

configure
case context context_name
  apn apn_name
  permission nemo
end

Performance Indicator Changes

show subscribers all

The output of this command has been enhanced to provide information on subscribers using the PMIPv6 protocol between the MAG client and the LMA service. Information includes:

- Call Type (vcccc)
- CALLID
- MSID
- USERNAME
- IP
- TIME-IDLE

show subscribers debug-info <pmipv6call_call_id>

The output of this command has been enhanced to provide information on subscribers using the PMIPv6 protocol between the MAG client and the LMA service. Information includes:

- Total Prefix
- All active prefixes
- Peer Callid
- VRF Detail
- Multi-VRF Enabled <Yes/No>
- Sessmgr Npu Flow Details

show lma session full all

The output of this command has been enhanced to provide information on subscribers using the PMIPv6 protocol between the MAG client and the LMA service. Information includes:
Syslogging of Reject Events

CSCuu21047 - Inclusion of IMSI in EGTPC logs for reject events

**Applicable Products** = GGSN, P-GW, SAEGW, S-GW

**Feature Changes**

**Previous Behavior:** The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all eGTP-C system event logs of type error and critical.

**New Behavior:** The P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the eGTP-C event log details for the system event logs of type error and critical, if available. If the IMSI is not available, the P-GW/SAEGW/S-GW will make the best effort to obtain the IMEI.

**Command Changes**

`logging`

The `include-ueid` keyword has been added to the `logging` command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
configure
  logging include-ueid
  no logging include-ueid
end
```

**Performance Indicator Changes**

`show configuration`

The output of this command has been enhanced to indicate if the `logging` command is enabled with the `include-ueid` keyword.

- logging include-ueid
- no logging include-ueid
SaMOG Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from SaMOG in StarOS 19 software releases.

- SaMOG Enhancements for 19.3, page 377
- SaMOG Enhancements for 19.0, page 381

SaMOG Enhancements for 19.3

This section identifies all of the SaMOG enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SaMOG Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SaMOG.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
IPv6 Transport Support Using EoGRE Access Type

CSCuV74182 - [SaMOG] - IPv6 Transport Interface support for EoGRE Access-Type

Feature Changes
With this release, the SaMOG Gateway supports IPv6 transport between the WLC/Access Point (AP) and the SaMOG gateway for trusted Wi-Fi subscribers using the EoGRE access type. This enables SaMOG Gateway to support a rapidly increasing number of subscribers accessing the internet via mobile devices, and technologically advanced (example, Internet of Things) internet-enabled devices (sensors, machine-readable identifiers) that demand high network address assignments.

The access side peers (WLC/AP) and SaMOG communicate over an IPv6 transport, and the data travels over the tunnel between IPv6 endpoints.

Command Changes

bind

Use the `ipv4-address` and `ipv6-address` keywords to configure the CGW service with IPv6 bind addresses. This enables IPv6 transport between the WLC and SaMOG for the EoGRE interface.

configure
  context context_name
    cgw-service cgw_service_name
      bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv6_address ] }
      no bind { ipv4-address [ ipv6-address ] | ipv6-address [ ipv4-address ] }
    end

Notes:

• `ipv4_address` must be an IPv4 address expressed in dotted-decimal notation.
• `ipv6_address` must be an IPv6 address expressed in colon (or double-colon) notation.
• IPv4 and/or IPv6 address(es) can be bound to the CGW service.
• The CGW service is started even when one of the address is bound.
• Both addresses (IPv4/IPv6) can be bound to the CGW service using either one command, or two separate commands.
• When a second address is configured, the service restarts and existing sessions are lost for the other bind address.
DHCPv6 Service Configuration

Use the `bind` and `dhcppv6-server` commands under the DHCPv6 Service Configuration Mode to enable SaMOG to receive DHCPv6 messages from the UE, and respond with the address assigned by the P-GW.

```
configure
countext context_name
dhcpv6-service dhcpv6_service_name
  bind address ipv6_address [port port_number]
nobind address
dhcpv6-server
  server ipv6_address
end
```

Notes:

- Once the DHCPv6 Service IPv6 bind address is configured, associate the DHCPv6 service with the SaMOG Service using the `associate` command under the SaMOG Service Configuration Mode.

Performance Indicator Changes

SaMOG Schema

The following bulk statistics counters are introduced in support of this feature:

- `cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv4-pkts`
- `cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv4-bytes`
- `cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv6-pkts`
- `cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv6-bytes`
- `cgw-sessstat-eogre-tunnel-data-receive-drop-errors`
- `cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv4-pkts`
- `cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv4-bytes`
- `cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv6-pkts`
- `cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv6-bytes`

The following bulk statistics counters are modified to support this feature:

<table>
<thead>
<tr>
<th>Counters in Earlier Releases</th>
<th>Modified Counters in Current Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-pkts</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv4-pkts</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv6-pkts</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv6-pkts</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-bytes</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv4-bytes</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv6-bytes</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv6-bytes</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-pkts</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv4-pkts</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-bytes</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv4-bytes</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv6-pkts</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-pkts</code></td>
</tr>
<tr>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv6-bytes</code></td>
<td><code>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-bytes</code></td>
</tr>
</tbody>
</table>
### Modified Counters in Current Release

<table>
<thead>
<tr>
<th>Counters in Earlier Releases</th>
<th>Modified Counters in Current Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-pkts</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv4-bytes</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv6-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-bytes</td>
</tr>
</tbody>
</table>

**show cgw-service all**

The output of this command is modified to display the following fields:

- Bind IPv4 Address
- Bind IPv6 Address

**show subscribers samog-only full**

The output of this command is modified to display the following field under the *CGW Subscriber Info* section:

- care-of-addr

**show samog-service all**

The output of this command is modified to display the following field:

- Associated DHCPv6 service

**show samog-service statistics**

The output of this command is modified to display the following fields:

**EoGRE Data Statistics:**

- Tunnel Data Received:
  - Total Packets
  - IPv6 EoGRE(IPv4)
  - IPv4 EoGRE(IPv6)
  - Total Bytes
  - IPv6 EoGRE(IPv4)
  - IPv4 EoGRE(IPv6)

- Tunnel Data Sent:
  - Total Packets
  - IPv6 EoGRE(IPv4)
SaMOG Enhancements for 19.0

This section identifies all of the SaMOG enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SaMOG Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

### Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SaMOG.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**SaMOG Inter-chassis Session Recovery**

CSCug95464 - ICSR support on SaMOG GW
Feature Changes

With this release, SaMOG can support inter-chassis session recovery (ICSR) configurations on the ASR 5x00 and virtualized platforms. SaMOG is now capable of providing chassis-level and geographic-level redundancy and can recover fully created sessions in the event of a chassis failure.

IPv6 Transport Support Using PMIPv6 Access Type

CSCut52257 - IPv6 Support on Control Interface on Access side for SaMOG

Feature Changes

Important

This feature is currently supported as lab quality only.

With this release, the SaMOG Gateway supports IPv6 transport between the WLC/Access Point (AP) and the SaMOG gateway for trusted Wi-Fi subscribers using the PMIPv6 access type. This enables SaMOG Gateway to support a rapidly increasing number of subscribers accessing the internet via mobile devices, and technologically advanced (example, Internet of Things) internet-enabled devices (sensors, machine-readable identifiers) that demand high network address assignments.

The access side peers (WLC/AP) and SaMOG communicate over an IPv6 transport, and the data travels over the tunnel between IPv6 endpoints.

Command Changes

bind (CGW Service Configuration Mode)

Use the \texttt{ipv6-address} keyword in the \texttt{bind} command under the CGW Service Configuration Mode to enable IPv6 transport between the WLC and SaMOG for PMIPv6 access type.

Important

In this release, when both IPv6 and IPv4 addresses are configured for PMIPv6 access type, only IPv6 address is considered.

\begin{verbatim}
configure
  context context_name
  cgw-service cgw_service_name
    bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
    no bind { ipv4-address [ ipv6-address ] | ipv6-address [ ipv4-address ] }
  end
\end{verbatim}

- \texttt{ipv4_address} must be an IPv4 address expressed in dotted-decimal notation.
- \texttt{ipv6_address} must be an IPv6 address expressed in colon (or double-colon) notation.
- IPv4 and/or IPv6 address(es) can be bound to the CGW service.
• The CGW service is started even when one of the address is bound.
• Both addresses (IPv4/IPv6) can be bound to the CGW service using either one command, or two separate commands.

**bind (MRME Service Configuration Mode)**

The `bind` command configures IP address(es) to be used as a connection point to establish SaMOG sessions for handling authentication and accounting messages.

With this release, the `address` keyword is deprecated and replaced with the `ipv4-address` and `ipv6-address` keywords to configure MRME service with IPv6 bind addresses. This enables IPv6 transport between the WLC and SaMOG for the RADIUS interface.

```
configure context context_name
  mrme-service mrme_service_name
    bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
    no bind { ipv4-address [ ipv6-address ] | ipv6-address [ ipv4-address ] }
end
```

Notes:

• `ipv4_address` must be an IPv4 address expressed in dotted-decimal notation.
• `ipv6_address` must be an IPv6 address expressed in colon (or double-colon) notation.
• IPv4 and/or IPv6 address(es) can be bound to the MRME service.
• The MRME service is started even when one of the address is bound.
• Both addresses (IPv4/IPv6) can be bound to the MRME service using either one command, or two separate commands.
• When a second address is configured, the service restarts and existing sessions are lost for the other bind address.

**Performance Indicator Changes**

**SaMOG Schema**

The following bulk statistics counters are introduced in support of this feature:

• cgw-tdr-ipv6greipv6-pkts
• cgw-tdr-ipv6greipv4-pkts
• cgw-tdr-ipv6greipv6-bytes
• cgw-tdr-ipv6greipv4-bytes
• cgw-tds-ipv6greipv4-pkts
• cgw-tds-ipv6greipv6-pkts
• cgw-tds-ipv6greipv4-bytes
• cgw-tds-ipv6greipv6-bytes
• cgw-tds-ipv6greipv6-bytes

The following bulk statistics counters are modified to support this feature:

<table>
<thead>
<tr>
<th>Counters in Release 18 and Earlier</th>
<th>Modified Counters in Current Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>cgw-tdr-ipv4gre-pkts</td>
<td>cgw-tdr-ipv4greipv4-pkts</td>
</tr>
<tr>
<td>cgw-tdr-ipv6gre-pkts</td>
<td>cgw-tdr-ipv4greipv6-pkts</td>
</tr>
<tr>
<td>cgw-tdr-ipv4gre-bytes</td>
<td>cgw-tdr-ipv4greipv4-bytes</td>
</tr>
<tr>
<td>cgw-tdr-ipv6gre-bytes</td>
<td>cgw-tdr-ipv4greipv6-bytes</td>
</tr>
<tr>
<td>cgw-tds-ipv4gre-pkts</td>
<td>cgw-tds-ipv4greipv4-pkts</td>
</tr>
<tr>
<td>cgw-tds-ipv6gre-pkts</td>
<td>cgw-tds-ipv4greipv6-pkts</td>
</tr>
<tr>
<td>cgw-tds-ipv4gre-bytes</td>
<td>cgw-tds-ipv4greipv4-bytes</td>
</tr>
<tr>
<td>cgw-tds-ipv6gre-bytes</td>
<td>cgw-tds-ipv4greipv6-bytes</td>
</tr>
</tbody>
</table>

**show mrme-service**

The output of this command is modified to display the following fields. These statistics are also displayed in the output of the `show cgw-service` command.

• Bind IPv4 Address
• Bind IPv6 Address

**show samog-service**

The output of this command is modified to display the following field:

• Associated DHCPv6 service

**show samog-service statistics**

The output of this command is modified to display the following fields under the `PMIPv6 Data Statistics` section:

• Tunnel Data Received
  • Total Packets
    • IPv6 GRE (IPv4)
    • IPv4 GRE (IPv6)
  • Total Bytes
• IPv6 GRE (IPv4)
• IPv4 GRE (IPv6)

• Tunnel Data Sent
  • Total Packets
    • IPv6 GRE (IPv4)
    • IPv4 GRE (IPv6)
  • Total Bytes
    • IPv6 GRE (IPv4)
    • IPv4 GRE (IPv6)

show subscribers samog-only full
The output of this command is modified to display the following fields:
  • MRME Subscriber Info
    • RadClient address: <IPv6_address>
    • CC-Profile
      • Dynamic Auth Details
        • Server IP: <IPv6_address>

• CGW Subscriber Info
  • care-of-addr

show twan-profile all
The output of this command is modified to display the following fields:
  • Radius Client List
    • IPv6 Address
  • Access-Type Client List
    • IPv6 Address
HTTPS Redirection for SaMOG Web Authorization

CSCut84129 - HTTPS Redirection Support on SaMOG

Feature Changes

With this release, SaMOG is qualified to redirect subscribers (on non-UICC devices) accessing an HTTPS website to an external web portal for authentication. SaMOG performs HTTPS redirection using configured Layer 4 redirection rules (ACLs). The web portal performs SSL handshakes and redirects at the HTTP application level.
SecGW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from SecGW in StarOS 19 software releases.

- SecGW Enhancements for 19.0, page 387

SecGW Enhancements for 19.0

This section identifies all of the SecGW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the SecGW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

L3-ICSR Enhancement

CSCuq23595 - Stale RRI and SRI routes on standby cause traffic outage and rekey failure

Feature Changes

Previous Behavior: Only onePK was used for adding L3 routes by using ip sri-route or ipv6 sri-route and ip rri-route or ipv6 rri-route CLI commands.

New Behavior: With this enhancement, Border Gateway Protocol (BGP) is introduced to propagate the additional routes (RRI 2nd-leg routes). Also, ip sri-route and ipv6 sri-route configurations are deprecated and not supported in 19.0 and later releases.

No other CLI commands are added or modified as part of this enhancement. Only CLI command usage and restrictions are changed for ip rri-route and ipv6 rri-route. Both of these commands will use a loopback address as the network address instead of a dummy-ip for L3 mode.
RRI and SRI Inserted Under the Particular VRF Table

CSCut88426 - VRF aware RRI

Feature Changes

With this feature, Reverse Route Injection (RRI) is inserted under the particular VRF table for clear and encrypted traffic to work under Virtual Routing and Forwarding (VRF).

The existing `ip rri` or `ipv6 rri` and `ip rri-route` or `ipv6 rri-route` CLI commands can be used to configure the RRI related configuration.

A single RRI route configurations is allowed per context, and one interface is always mapped to a specific VRF name. For example, the below configuration is incorrect because the interface is mapped to two different VRF names (`clear5`, `clear4`):

```
 ip rri-route network-model 13 3.3.3.3 5.5.5.5 interface clear vrf clear5
 ip rri 5.5.5.5 interface clear vrf clear4
```

SecGW to Send the DNS Server IP Address to the Peer

CSCut88425 - DNS to AP feature

Feature Changes

This feature allows the SecGW to send the dns-server ip-address to the peer in Auth response message.

Command Changes

dns-server

This is a new command introduced under WSG-Service Configuration Mode.

```
configure
 context context_name
   wsg-service service_name
     dns-server primary { ipv4_address | ipv6_address } [ secondary { ipv4_address | ipv6_address } ]
 ]
   no dns-server primary { ipv4_address | ipv6_address }
 end
```

Notes:

- Use this command to configure an IPv4 or IPv6 address of a DNS server. The same CLI command can be configured twice, at the most, with different IP address type. However, both primary and secondary IP address should be of the same type (IPv4 or IPv6) for a CLI.
- This CLI command is effective only for the tunnels created with the local address pool.
- A new request will overwrite the existing entries of the same IP address type.
• The CLI command can be unconfigured using `no dns-server primary` command. There is no default behavior for this CLI command.

• The configured CLI command will be visible as a part of `show configuration` and `show wsg-service all` or `show wsg-service name` CLI commands.
SecGW to Send the DNS Server IP Address to the Peer
CHAPTER 22

SGSN Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from the SGSN in StarOS 19 software releases.

- SGSN Enhancements for 19.6, page 391
- SGSN Enhancements for 19.5, page 395
- SGSN Enhancements for 19.4, page 398
- SGSN Enhancements for 19.3, page 411
- SGSN Enhancements for 19.2, page 415
- SGSN Enhancements for 19.0, page 424

SGSN Enhancements for 19.6

This section identifies all of the SGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SGSN.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
• Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
• MVG Enhancements
• NAT Enhancements
• SNPP MIB Enhancements
• System and Platform Enhancements

EPC ARP and Gn-Gp ARP Parameter Mapping in S4-SGSN

CSCvc54409 - [S4-SGSN]"QoS gn-arp" CLI Should Be Applicable In Israu and SRNS

Feature Changes

Previous Behavior: The command `qos gn-arp high-priority priority medium-priority priority` under the call control profile ensures proper QoS parameter mapping between the S4-SGSN and EPC UEs, SGWs and PGWs. It maps the EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) parameters which are used during S4-SGSN to Gn SGSN call handovers. Consider an Inter-SGSN RAU or SRNS scenario where the high-priority and medium-priority values are configured using the `qos gn-gp` command, it is observed that the S4-SGSN does not map the values to the configured values during new Inter-SGSN RAU and SRNS call flows, instead the S4-SGSN incorrectly uses the default values of medium priority and high priority. The S4-SGSN should map the EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) parameters configured under the call-control-profile. The default values must be used only when no specific values are configured for high and medium priority.

New Behavior: The S4-SGSN now maps EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) parameters configured using the command `qos gn-arp high-priority priority medium-priority priority` under the call control profile for New SGSN RAU and New SRNS call flows.

Customer Impact: The customer has more control over pre-release ARP to EPC ARP parameter mapping in new SGSN RAU and new SRNS call flows.

ISRAUs Over GTPv2 for Roaming Subscribers Restricted

CSCuy87278- Wrong service selection during RAU when S3 and Gn are both configured

Feature Changes

Previous Behavior: The S4-SGSN uses GTPv2 by default and allows new Inter SGSN RAUs over GTPv2 for all subscribers. The S4-SGSN allows ISRAUs over GTPv2 even if the subscriber’s call-control-profile is configured explicitly with Gn interface as the S4-SGSN does not check for core network interface configured for a specific subscriber before allowing GTPv2. The inbound ISRAUs over GTPv2 interface has to be restricted for roaming subscribers. Currently there is no mechanism in the S4-SGSN for to implement this restriction. Access to S4 interface or GTPv2 should be limited only to home subscribers.
A short-term solution for the above mentioned issue was provided through CSCvb34803 (in release 19.3.10) wherein the new ISRAU over GTPv2 was rejected for roaming subscribers, if the `sgsn core-nw-interface gn` command has been configured in the roaming subscribers call-control-profile. The command `sgsn core-nw-interface gn` under the call control profile enables operators to select the Gn interface or the S4 interface for EPC capable UEs and non-EPC capable UEs on the S4-SGSN. The configuration of the CLI command `sgsn core-nw-interface gn` was used to decide whether to reject/honor the RAU request upon context response received via GTPv2. The table below displays the actions based on the configuration:

<table>
<thead>
<tr>
<th>Interface</th>
<th><code>sgsn-core-nw-interface gn</code></th>
<th><code>sgsn-core-nw-interface s4</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPv1 protocol</td>
<td>Proceed with call</td>
<td>Proceed with call</td>
</tr>
<tr>
<td>GTPv2 protocol</td>
<td>RAU reject</td>
<td>Proceed with call</td>
</tr>
</tbody>
</table>

**New Behavior:** As part of this release instead of rejecting ISRAU over GTPv2 for roaming subscribers as described above, RAU will fall back to GTPv1 and will be processed. The command `sgsn core-nw-interface gn` under the call control profile enables operators to select the Gn interface or the S4 interface for EPC capable UEs and non-EPC capable UEs on the S4-SGSN. The command `sgsn core-nw-interface gn` has to be configured in the roaming subscribers call-control-profile to implement the restriction on ISRAU over GTPv2 for roaming subscribers. When the EGTP context response is received from the peer during inbound ISRAU over GTPv2, a new check is introduced where the `sgsn core-nw-interface gn` command configuration is verified. If the subscriber's call-control profile is configured to use Gn interface alone, then EGTP context ACK with failure cause will be sent to peer and RAU will fall back to GTPv1. The failure cause value sent in EGTP context ACK message to peer is `EGTP_CAUSE_USER_AUTHENTICATION_FAILED`. The table below displays the actions based on the configuration:

<table>
<thead>
<tr>
<th>Interface</th>
<th><code>sgsn-core-nw-interface gn</code></th>
<th><code>sgsn-core-nw-interface s4</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPv1 protocol</td>
<td>Proceed with call</td>
<td>Proceed with call</td>
</tr>
<tr>
<td>GTPv2 protocol</td>
<td>RAU fall back to GTPv1 and proceed with call</td>
<td>Proceed with call</td>
</tr>
</tbody>
</table>

This is applicable for both 2G and 3G scenarios.

**Performance Changes**

The following new statistics are added to the `show gmm-sm statistics verbose` command to provide information on the number of new ISRAUs by roaming subscribers that have been restricted over GTPv2 and fall back to GTPv1:

- **Inbound Inter-RAU Fallback Statistics:** Is displayed under the Miscellaneous Statistics section of `show gmm-sm statistics verbose` command. The following counter is listed as a part of Inbound Inter RAU Fallback Statistics:

  - **3G-Inbound Inter SGSN RAU Fallback to GTPV1:** This counter displays the number of 3G in-bound ISRAUs for which GTPv2 is restricted and RAU has succeeded over GTPv1. This counter is pegged during 3G in-bound ISRAU, when the S4-SGSN sends EGTP context Ack with failure
cause to the peer as the subscriber’s call-control profile has `sgsn core-nw-interface gn` configuration and initiates a GTPv1 context request for a subscriber.

- **Inter-RAU Inbound Fallback to GTPV1**: This counter displays the number of 2G in-bound ISRAUs for which GTPv2 is restricted and RAU has succeeded over GTPv1. This counter is pegged during 2G in-bound ISRAU, when the S4-SGSN sends EGTP context ACK with failure cause to the peer as the subscriber’s call-control profile has `sgsn core-nw-interface gn` configuration and initiates a GTPv1 context request for a subscriber. This counter is listed under the GPRS FSM Miscellaneous Statistics section of `show gmm-sm statistics verbose` command.

## Processing of RAU Request On Context Response Received via GTPv2

CSCvb34803 - Short term fix for rejecting the Israu's for roamers

### Feature Changes

**Important**

This behavior change is applicable from release 19.3.10 onwards.

**Previous Behavior**: Consider the scenario, where a roaming subscriber registered on a node (S4 supporting node) with a PLMN using Gn path is performing an ISRAU on another node (S4 supporting node) in the same PLMN. The ISRAU on the second node is rejected after obtaining the IMSI of the subscriber from the peer node. The new ISRAU has to be restricted over GTPv2 (on S4-SGSN) for roamers and fallback to GTPv1 after sending context ack failure to the peer sgsn. Currently, the new ISRAU over GTPv2 is allowed for roamers even if the command `sgsn core-nw-interface gn` is configured in roamers call-control-profile.

**New Behavior**: A short-term solution for the above mentioned issue is provided where in the new ISRAU over GTPv2 is rejected for roamers, if `sgsn core-nw-interface gn` command is configured in roamers call-control-profile. The command `sgsn-core-nw-interface` under the call control profile enables operators to select the Gn interface or the S4 interface for EPC capable UEs and non-EPC capable UEs on the S4-SGSN.

The configuration of the CLI command `sgsn-core-nw-interface` will be used to decide whether to reject/honor the RAU request upon context response received via GTPv2. The following table displays the actions based on the configuration:

<table>
<thead>
<tr>
<th>Interface</th>
<th>sgsn-core-nw-interface gn</th>
<th>sgsn-core-nw-interface s4</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPv1</td>
<td>Proceed with call</td>
<td>Proceed with call</td>
</tr>
<tr>
<td>GTPv2</td>
<td>RAU Reject</td>
<td>Proceed with call</td>
</tr>
</tbody>
</table>

A more comprehensive solution for the above mentioned issue will be provided in a future release. The CLI command `sgsn core-nw-interface gn` will be used and instead of RAU reject, the RAU falls back to GTPv1 and the call will be processed.
Purge Request on RAU Timer Expiry During 2G/3G to 4G TAU

CSCvb40275 - [S4 SGSN] After IRAT to MME SGSN clears subscriber without HSS MS Purge

Feature Changes

- **Important** This behavior change is applicable to 19.3.10 and later releases.

In the case of TAU from S4-SGSN to MME, the SGSN clears the subscriber database without sending MS purge to HSS/HLR. It is expected that the subscriber remains in PMM detached state in the S4-SGSN after the TAU to MME. If the S4-SGSN decides to clear the subscriber completely (purge the cache), then it should send a MS purge message to HSS/HLR.

The MME should set the Single-Registration-Indication flag in the Notify request during 4G attach (using mapped GUTI from PTMSI) so that the registration at the HLR is cleared.

**Previous Behavior:**

1. During 3G/2G to 4G TAU from SGSN, the subscriber was cleared after RAU timer expiry without notifying HSS.

2. During 4G attach with mapped GUTI, Single-Registration-Indication flag was not set in Notify request if ULR was not initiated for the attach.

**New Behavior:**

1. Sending purge request on RAU timer expiry during S4-SGSN to MME TAU is mandated. The purge request is sent to notify HSS that subscriber database is cleared at SGSN.

- **Important** Purge request will be sent only if context request received from MME is GTPv2.

2. Single-Registration-Indication flag is set in Notify request during 4G attach using mapped GUTI from PTMSI. If this flag is set, then the HSS sends CLR to SGSN.

- **Important** This flag will be set only if ULR is not sent or if initial-attach indicator is not set in ULR.

SGSN Enhancements for 19.5

This section identifies all of the SGSN enhancements included in this release:

- **Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.

- **Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.
Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.

---

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

Enhancement for Extended Usage of Configured Static SGSN Address

CSCva55357 - Peer-SGSN selection using nri based selection for 3g and 2g

Feature Changes

Previous Behavior: The Static SGSN address configured through the CLI command `sgsn-address` under the Call Control Profile configuration mode is used for inter-SGSN RAUs only if the RAI in the RAU request is local to the SGSN (that is, if the RAI is configured in this SGSN). If the RAI is not configured in the SGSN, a DNS query is sent out.

New Behavior: A new CLI keyword `nri-for-inter-pool-address` is introduced in the command `peer-nri-length` under the Call Control Profile configuration mode, when this keyword is enabled the static `sgsn-address` configured through the command `sgsn-address` is used for inter-pool Attaches/RAUs if the NRI value configured in the CLI command `sgsn-address` matches the NRI value calculated from the PTMSI received in attach/RAU message.

Customer Impact: DNS query is avoided in the above mentioned scenarios.

Feature Description

The static SGSN address configured in the CLI `sgsn-address` under call-control-profile is used for the inter-SGSN RAUs only if the RAI in the RAU request is local to the SGSN (that is, if the RAI is configured in this SGSN). If the RAI is not configured in the SGSN, DNS query is sent out to fetch peer-sgsn address.

With this feature enhancement the static address configured from the CLI `sgsn-address` will be used for inter-pool scenarios as well. A new CLI keyword `nri-for-inter-pool-address` is introduced in the command
**peer-nri-length** under the call-control-profile configuration mode, when this keyword is enabled the static SGSN address configured in the command **sgsn-address** is used for inter-pool Attaches/RAUs if the NRI value configured in the CLI **sgsn-address** matches the NRI value calculated from the PTMSI received in the attach/RAU message. If the keyword **nri-for-inter-pool-address** is not enabled, a DNS query is sent out to fetch the peer-sgsn address.

This enhancement is applicable for both 2G and 3G scenarios. The primary advantage of this enhancement is that the DNS query for inter-pool 3G or 2G Attach/RAU scenarios is avoided.

---

**Configuring the SGSN-NRI Feature**

The command **peer-nri-length** under the Call Control Profile configuration mode is enhanced with a new keyword **nri-for-inter-pool-address** as a part of this feature enhancement. If this new keyword is configured and if the NRI value derived from the PTMSI received in the RAU request matches the NRI value configured in the CLI command **sgsn-address nri nri-value prefer local address ipv4 addr interface name** the static sgsn-address configured in the above CLI will be used to initiate context request. Otherwise, a DNS query will be initiated to fetch the peer-sgsn address.

```config
   call-control-profile cc_profile_name
      peer-nri-length length [rai-fqdn-fallback] [nri-for-inter-pool-address]
      remove peer-nri-length rai-fqdn-fallback nri-for-inter-pool-address
   exit
```

**Notes:**

- The keyword **nri-for-inter-pool-address** is not enabled by default. This keyword is used to enable NRI-only based static peer-sgsn address configuration for inter-pool.
- The keyword **remove** deletes the existing configuration.

**Sample Configuration:**

```config
   call-control-profile cc1
      peer-nri-length / nri-for-inter-pool-address
   exit
```

**Verifying the Configuration**

The **show call-control-profile full** command is used to verify the configuration of this feature. The following field is displayed as either true or false depending on whether **nri-for-inter-pool-address** is enabled or not:

- NRI-only based static sgsn-address for inter-pool Attach/RAU

---

**Monitoring and Troubleshooting the SGSN-NRI Feature**

This section provides information on how to monitor the SGSN-NRI Feature.

**Show Command(s) and/or Outputs**

This section provides information regarding show commands and/or their outputs in support of the SGSN-NRI feature:
**show gmm-sm statistics verbose**

The following new parameter is added to this show command to display the statistics for this feature:

- **NRI-based local addr resolution for Foreign PTMSI Attach/ISRAU**: This counter tracks the number of times local address resolution is done using NRI-based CLI over DNS query.

**show call-control-profile full name**

The following new counter is added to this show command; it is displayed as either TRUE or FALSE. It is displayed as TRUE when the feature is enabled and FALSE when the feature is disabled:

- NRI-only based static sgsn-address for inter-pool Attach/RAU

---

**SGSN Enhancements for 19.4**

This section identifies all of the SGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**APN-OI-Replacement for Gn-SGSN**

CSCuy29739 - SGSN - Gn-SGSN support of APN-OI-Replacement over Gr
Feature Description

Overview

Beginning with release 19.4, in compliance with 3GPP TS 29-003, decoding of the APN-OI-Replacement IE is supported by Cisco Gn-SGSNs using either a Gr MAP or an S6d Diameter interface.

The Gn-SGSN accepts the APN-OI-Replacement field included as part of the GPRS subscription. Typically, the field value, stored at the HLR/HSS as part of the subscription data, is a domain name for a specific GGSN. The value in the APN-OI-Replacement field is intended to replace the APN-OI (derived from the IMSI) during the GGSN selection process. The replacement results in the construction of a fully qualified domain name (FQDN) APN, for a preferred GGSN, to be used for DNS resolution.

Supported Functions

UE-Level

• The Gn-SGSN supports decoding of a UE-level APN-OI-Replacement IE from the HLR/HSS via either MAP or Diameter interface.
• The Gn-SGSN stores the UE-level APN-OI-Replacement value as a subscription database record.
• The Gn-SGSN uses the APN-OI-Replacement only for DNS translation in selection of a Home GGSN.
• The APN sent to other entities (GGSN/SGSN, CGF) is not affected by APN-OI replacement.

APN-Level

• The Gn-SGSN supports decoding of a APN-level APN-OI-Replacement IE from the HLR/HSS via either MAP or Diameter interface.
• The Gn-SGSN stores the APN-level APN-OI-Replacement value per APN as a subscription database record.
• The Gn-SGSN uses the APN-level APN-OI-Replacement, even when a UE-level APN-OI-Replacement is present, because the APN-level APN-OI-Replacement has higher priority.
• The Gn-SGSN uses the APN-OI-Replacement only for DNS translation while accessing Home GGSN.
• The APN sent to other entities (GGSN/SGSN, CGF) is not affected by APN-OI replacement.

Gn-SGSN

• The Gn-SGSN indicates APN-level and UE-level APN-OI replacements received in subscriptions as part of the output generated by the show subscriber gprs-only | sgsn-only full all command.
• The Gn-SGSN applies APN-level APN-OI-Replacement when both APN-level and UE-level APN-OI replacement are available for a PDP context.

Benefits

This feature makes it possible for the operator to use UE-level and/or APN-level APN-OI replacement to substitute an APN-OI per UE or per APN and then redirects the PDP session to a different GGSN.

This fully-compliant 3GPP functionality enables operators to differentiate service or customer UE and/or APN levels based on the HLR/HSS subscription.
Limitations

The Gn-SGSN does not handle EPS subscription. This means that even though the Gn-SGSN supports S6d, the APN-OI-Replacement in an EPS subscription is not applicable.

Related Product Support

Decoding of this AVP is supported by both the Cisco S4-SGSN and MME for EPS subscriptions.

License Information

This feature is enabled by default and does not require a feature license.

Configuration

Because this feature is 3GPP compliant and does not require enabling or configuration, there are no CLI commands or keywords specific to this feature.

How It Works

The Gn-SGSN supports decoding of the UE and/or APN level APN-OI-Replacement IE received in GPRS subscriptions on either the Gr interface or the S6d interface.

In accord with 3GPP TS 23.060:

- UE-level APN-OI-Replacement field values are conditionally stored as permanent data in the HSS/HLR and the SGSN.
- APN-level APN-OI-Replacement field values are conditionally stored as permanent data in the HSS and the SGSN.
- APN-level APN-OI-Replacement has the same role as UE-level APN-OI-Replacement. If both the APN-level APN-OI-Replacement and the UE-level APN-OI-Replacement are present, the APN-level APN-OI-Replacement has a higher priority than UE-level APN-OI-Replacement.

The format of the domain name used in the APN-OI-Replacement field (as defined in 3GPP TS 23.060 and 3GPP TS 23.401) is the same as the default APN-OI except that it may be preceded by one or more labels, each separated by a dot.

- Example 1: province1.mnc012.mcc345.gprs
- Example 2: ggsn-cluster-A.provinceB.mnc012.mcc345.gprs

The APN-OI-Replacement handling is case insensitive.

The APN constructed using the APN-OI-Replacement field is only used for DNS translation to locate the Home GGSN. DNS translation for other entities is unaffected.

Flow

1. During a 2G/3G Attach procedure, the Gn-SGSN receives an Insert Subscriber Data (ISD) during UGL/ULR from the HLR/HSS.

2. APN-OI-Replacement IE is present in the Subscription-Data AVP sent in an Insert-Subscriber-Data-Request (IDR) if the UE-level APN-OI-Replacement has been added or modified in the HSS.
APN-OI-Replacement IE is present in the GPRS-Subscription-Data sent in an Insert-Subscriber-Data (ISD) if the UE-level APN-OI-Replacement has been added or modified in the HLR.

3 APN-OI-Replacement IE is present in the PDP-Context AVP sent within an Insert-Subscriber-Data-Request (IDR) if the APN-level APN-OI-Replacement has been added or modified in the HSS.

APN-OI-Replacement IE is present in the PDP-Context IE in the GPRS-Data-List sent within an Insert-Subscriber-Data (ISD) if the APN-level APN-OI-Replacement has been added or modified in the HLR.

4 After receiving an APN-OI-Replacement from an HLR/HSS,
   • the Gn-SGSN decodes the IE,
   • the Gn-SGSN replaces the stored information (if any) with the received APN-OI-Replacement under the subscription dB record for the subscriber on the SGSN,
   • during activation of the PDP context, the Gn-SGSN presents this replacement APN-OI to be used for the DNS resolution to determine the GGSN.

5 The HLR (MAP) removes the UE-level APN-OI-Replacement by setting the "APN-OI-Replacement withdraw" bit of the Delete-Subscriber-Data (DSD), sent over Gr.

The HSS removes the UE-level APN-OI-Replacement by setting the "APN-OI-Replacement" bit of the Delete-Subscriber-Data-Request (DSR) flag field of S6d.

Monitoring and Troubleshooting

Monitor Protocol
Monitor Protocol functionality is supported for this feature and can be used by enabling MAP (55), Diameter (36), and DNS Client (70).

⚠️ Caution
Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. We recommend that you contact your Cisco Support Representative prior to using it for troubleshooting.

Output of “show” Commands
The Gn-SGSN displays received UE-level APN-OI-Replacements under GPRS subscriptions and APN-level APN-OI-Replacements under PDP subscription data of the output generated by the show subscriber [ gprs-only | sgsn-only ] full imsi imsi commands.

Quick Check
To quickly check for APN-OI-Replacement use the following grep command with either the gprs-only or the sgsn-only keyword:

\texttt{show subscribers gprs-only full imsi imsi | grep Repl}

The following illustrates the type of output generated by the above command. The first line is for UE-level replacement information and the second line illustrates APN-level replacement information:

\begin{verbatim}
APN OI Replacement : abc.ggg.mnc009.mcc262.gprs
APN OI Replacement: : ggg.mnc009.mcc262.gprs
\end{verbatim}
To generate the full output, use the same command without the `grep` option:

```
show subscribers gprs-only full imsi imsi
```

The following is a limited sample of the display that is generated. The entries for APN-OI-Replacement are in bold:

```
[local]asr5000# show subscribers sgsn-only full all
Username: 491740460103
  Access Type: sgsn
  Access Tech: WCDMA UTRAN
  callid: 01317b21
  msid: 262090426000193
  state: Connected
  connect time: Sun Apr 24 12:20:44 2016
  call duration: 00h00m11s
  idle time: 00h00m00s
  Imsimgr Instance: 1
  Temporary Imsimgr instance: 0
  Operator Policy Name: policy1

  EPS Subscription:
  None:

  GPRS Subscription:
    APN_OI_Replacement: abc.mnc009.mcc262.gprs

  PDP Subscription Data:
    PDP Context Id: 1
    APN: WAP98.TESTNETZ-VD2.DE
    APN_OI_Replacement: op1.mnc009.mcc262.gprs
    PDP Type: IPv4
    PDP Address Type: Dynamic
    Charging Characteristics: Normal Billing
    VPLMN Address Allowed: Not Allowed

  ...

The highlighted entry under the GPRS Subscription section lists the information for a UE-level APN-OI-Replacement.

The highlighted entry under the PDP Subscription Data section lists the information for an APN-level APN-OI-Replacement.

### Assertion Failure in Function

CSCuu751111 - Assertion Failure in Function: sn_gt_process_inv_local_event(3)

### Feature Changes

**Previous Behavior:** In earlier releases, the Modify PDP Context requests from the Mobile Station (MS) were processed when the requests were received during the GMM identification procedures for TMSI.

**New Behavior:** From release 19.4 onwards, the Modify PDP Context requests from the MS will be dropped when the requests are received during the GMM identification procedures for TMSI.

### Direct Tunnel Interface Selection

CSCuz20719 - Direct-tunnel cannot be distinguished between Gn or S12
**Feature Changes**

In this release, the SGSN has been provisioned to enable or disable Direct Tunnel separately to either the GGSN or the SGW.

**Previous Behavior:** The StarOS CLI command used to enable Direct Tunnel functionality is the same for both the Gn-SGSN's GTP-U interface towards a GGSN and the S4-SGSN's S12 interface towards an S-GW. There is no way to differentiate the services for Gn versus S4.

**New Behavior:** The new Direct Tunnel Interface Selection enhancement adds new CLI keywords to enable the operator to choose - to configure the SGSN to provide one of the following:

- only GTP-U interface towards GGSN
- only S12 interface towards an S-GW.

The CLI for this functionality requires the system to be loaded with the appropriate SGSN license and a Direct Tunnel license. There is no license specific to this functionality.

**Impact on Customer:** The customer will have greater control over the functionality configured for the Direct Tunnel.

**Command Changes**

Two new keyword filters, `to-ggsn` and `to-sgw`, have been added to the `direct-tunnel` command to enable the operator to select the interface the SGSN will use for its direct tunnel. Direct Tunnel is configured under the Call-Control Profile configuration mode.

```
configure
  call-control-profile profile_name
    direct-tunnel attempt-when-permitted [to-ggsn | to-sgw ]
  end
```

**Notes:**

1. Use the keyword `attempt-when-permitted` without a filter to enable both GTP-U towards the GGSN and S12 towards the SGW.
2. To remove the configuration for both DT interfaces, use the following command: `remove direct-tunnel`
3. Use the keyword `attempt-when-permitted` with the `to-ggsn` keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
4. To remove the configuration for the GTP-U interface, use the following command: `remove direct-tunnel to-ggsn`
5. Use the keyword `attempt-when-permitted` with the `to-sgw` keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
6. To remove the configuration for the S12 interface, use the following command: `remove direct-tunnel to-sgw`

---

**Important**

All three forms of the CLI function independently. This means that the configuration created with one command (for example: `direct-tunnel attempt-when-permitted to-sgw`) is not overwritten by the entry of one of the other commands (for example: `direct-tunnel attempt-when-permitted`). The existing configuration must be removed to disable the configuration and then the next configuration must be added.
Monitoring Changes

show call-control-profile

The **show call-control-profile full name** `<profile_name>` instructs the SGSN to display the current direct tunnel configuration - to GGSN, to SGW, or to both.

If DT for the SGSN has been configured with one of the keyword filters, for example the `to-ggsn` keyword filter, then the DT to the GGSN would not be restricted and the output would look similar to this example:

```
... Reuse of authentication triplets : Enabled
Re-Authentication : Disabled
Direct Tunnel to GGSN : Not Restricted
Direct Tunnel to SGW : Restricted
Super Charger : Disabled
P-CSCF Restoration : Disabled
...
```

show subscribers sgsn-only summary

The **show subscribers sgsn-only summary** command output displays many pieces of information, including the total number of PDPs activated with direct tunnel, or activated through Gn, or activated through S4.

```
[local]asr5000# show sub sgsn-only summary
Total Subscribers : 1 Total Connected Subscribers : 1
Total Idle Subscribers : 0 Total Detached Subscribers : 0
Total Subscribers using HLR : 0 Total Subscribers using HSS : 1
Total HSS subscribers sharing subscription-info : 0
Total Active Subscribers : 1 Total PDP ctxs : 2
Activated through Gn : 0 Activated through Gn : 0
Activated through S4 : 1 Activated through S4 : 2
pdp-type-ipv4 : 2 pdp-type-ipv4 : 0
pdp-type-ipv6 : 0 pdp-type-ipv4-ipv6 : 0
Total PDPs with direct tunnel : 2
Activated through Gn : 0
Activated through S4 : 2
Total LCS Subscribers : 0
Total LCS Sessions : 0
```

Disc-Reason Pegging for Same R-TLLI

CSCuz79951 - 2G SGSN starts rejecting sessions due to AAA resource exhaustion

Feature Changes

A new triggering function has been added for 'sgsn-implicit-detach(237)' disconnect reason.

**Previous Behavior:** If handling of Random-TLLI collision is enabled via the SGSN Global Configuration mode command `gmm-message attach-with-tlli-in-use discard-message [only-on-same-nsei]` and the 2G-SGSN rejects the Attach Request due to same Random-TLLI collision, the session disconnect reason was not pegged.

**New Behavior:** If handling of Random-TLLI collision is enabled via the SGSN Global Configuration mode command `gmm-message attach-with-tlli-in-use discard-message [only-on-same-nsei]` and the 2G-SGSN rejects the Attach Request due to same Random-TLLI collision, the 'sgsn-implicit-detach(237)' session disconnect reason is now pegged.
Excluding GMLC Address from UGL

CSCuy51007 - LCS SGSN - CLI to not send v_GMLC address in UGL

Feature Changes

Feature Change

Previous Behavior:
By default, the SGSN includes the GMLC address, configured in the MAP service, in all Update-GPRS-Location (UGL) messages going to the HLR. Some HLRs do not recognize the v_GMLC field or value when it arrives in the UGL, as a result, the HLRs reject the calls. This prevents roaming-in subscribers from using some networks where LCS is enabled.

New Behavior:
Beginning with Release 19.4, it is possible for the operator to configure the SGSN to exclude the GMLC address from the UGL messages sent to the HLR.

Command Changes

A new keyword, exclude-gmlc, added to the map command in the Call-Control Profile configuration mode, enables the operator to override default behavior and exclude the GMLC address (v_GMLC IE) from all UGL messages.

```
config
  call-control-profile profile_name
    map message update-gprs-location exclude-gmlc
  end
```

Notes:

- **exclude-gmlc** - This keyword configures the SGSN to exclude the GMLC address in the Update-GPRS-Location (UGL) messages sent to the HLR.
- To re-enable the default behavior to include the GMLC address in the map message, enter the following configuration command:
  ```
  remove map message update-gprs-location exclude-gmlc
  ```
- For information about the other keywords available for the map command, refer to the Command Line Interface Reference.

IMSI Manager Broadcast Control

CSCux75750 - Control IMSIMGR to sessmgr broadcasting for unknown subscriber requests
**Feature Changes**

**Previous Behavior:** The IMSI Manager broadcasts requests to all Session Managers for unknown subscriber requests from HLR. When broadcasting for unknown requests is enabled, the IMSI Manager broadcasts all unknown requests to all active Session Managers to find the Session Manager instance hosting the subscriber. Broadcasting consumes a large portion of the IMSI Manager CPU capacity, especially if large numbers of broadcasts are performed in a short span of time. This may eventually lead the IMSI Manager to crash.

**New Behavior:** Broadcasting for unknown requests is enabled, the IMSI Manager broadcasts until the configured CPU threshold is reached. Once the threshold is reached, the IMSI Manager stops broadcasting and sends the unknown requests to any random Session Manager which in turn sends the response to the HLR. When the CPU threshold is not configured, the default IMSI Manager CPU threshold of 70% is applicable. Moreover, the broadcasting for unknown requests is disabled for first 60 mins after system reboot.

**Impact on Customer:** Unknown HLR requests will not be broadcasted when the IMSI Manager is overloaded.

**Feature Description**

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mapping maintained at IMSIMGR task is usually in sync with the mapping maintained at all session managers. But in some rare cases, there is a mismatch due to problems during the synchronization process. In such scenarios, the IMSIMGR task sends out a broadcast message to all session managers hoping that at least one of them will be hosting that session and could respond positively to this broadcast.

If none of the Session Managers respond with the mapping, the IMSI Manager considers it as request for an UNKNOWN (unregistered) subscriber and forwards it to a random Session Manager, which in turn sends an error response for the HLR request. The broadcasts from the IMSI Manager happen through a non-blocking vector call to all active Session Managers which can lead the IMSI Manager into a CPU overload condition considering the high number of session managers.

IMSI Manager broadcast control is implemented by the following:

- In IMSI Manager, broadcast disabling CPU threshold value defined; once the CPU utilization crosses this threshold, the IMSI Manager will not broadcast any unknown subscriber requests from HLR. Default value of this threshold is set as 50%. A CLI command is provided to optionally define the CPU threshold.

- In IMSI Manager, congestion threshold value of 70% is defined; once the CPU utilization crosses this threshold, the IMSI Manager will trigger congestion control action and will drop all unknown subscriber requests from HLR.

**Important**

This feature is enabled by default.

**How It Works**

**IMSI Manager Broadcast Control**

IMSI Manager broadcast control is applicable only to SGSN. The MAP requests from the HLR arrives at the IMSI Manager as the Link Manager cannot find the Session manager instance from IMSI in the request. The following MAP requests arrive at the IMSI Manager:
1. CANCEL LOCATION REQUEST
2. Standalone INSERT SUBSCRIPTION DATA (ISD)
3. Delete Subscriber Data (DSD)
4. Provide Subscriber Location (PSL)

The IMSI Manager looks for the Session manager id which hosts the IMSI in its mapping table. If the mapping does not exist, the requests are broadcasted to all active Session Managers for finding the session or mapping. If all the Session managers respond with negative response, the IMSI Manager sends the MAP request to a random Session manager which in turn responds with a Map User Error response with cause as "Unidentified Subscriber". Broadcasting of request consumes a huge amount of IMSI Manager CPU capacity, it is also observed that the most of the unknown requests received genuine unknown subscriber requests sent by HLR and the HLR is incorrectly sending these requests to the SGSN. To conserve the IMSI Manager CPU, broadcasting of these requests are avoided.

**IMSI Manager Broadcast Disabled During System Reboot**

After a system reboot, the subscribers are not yet registered in the system. During this period, if HLR sends ISD or Cancel Location Requests to the system in huge numbers, these requests are broadcasted thus leading to an IMSI Manager CPU overload condition. To conserve IMSI manager CPU, the IMSI Manager will not perform any broadcasting for the UNKNOWN MAP requests from HLR for first 60 minutes after reboot of the system. This SGSN feature is enabled by default and is not configurable. After 60 mins, the behavior as per the CLI configuration for IMSI manager broadcasting will be applied.

**Disabling Broadcast**

Broadcasting is stopped when the IMSI Manager is busy handling heavy traffic (that is, when IMSI Manager reaches a specific CPU threshold). All the IMSI Manager instances monitor their CPU usage and when the CPU threshold is reached, broadcasting is stopped until the CPU comes down below the threshold value. Instead of broadcasting to all Session Managers, the request is sent to any random Session Manager which in turn sends the response back to the originating node. This feature is enabled by default and the default CPU threshold for disabling broadcasting is 50%. The configured CPU threshold overrides this default value.

**Congestion Control**

In IMSI Manager, congestion is triggered when CPU crosses 70%; once the CPU utilization crosses this threshold, the IMSI Manager will trigger congestion control action and will silently drop all unknown subscriber requests from HLR. No responses will be sent to peer originating the requests.

---

**Note**

The thresholding application is a best effort at that instance and if the incoming rate of unknown messages is unusually high, a brief spike in the CPU usage of IMSIMGR task might occur.
Configuring IMSI Manager Broadcast Control

This section describes the configuration procedure for this feature. A new keyword is added to the command `task facility imsimgr` command under the global configuration mode to configure an IMSI Manager CPU threshold, once this threshold is reached the IMSI Manager stops broadcasting to conserve CPU.

```
config
  task facility imsimgr { avoid-sessmgr-broadcast { cpu_threshold percentage_value } | max integer_value |
  required-sessmgr no_sess_mgrs | sessmgr-sessions-threshold high-watermark high_value low-watermark low_value }
end
```

Notes:

- The keyword `cpu_threshold` specifies the CPU value of the IMSI Manager in percentage.
- The `percentage_value` is a percentage integer from 50 up to 70 %. The default value is 50%.

Examples

The following command is used to disable all IMSI Manager Broadcasts:

```
task facility imsimgr avoid-sessmgr-broadcast
```

The following command is used to disable broadcast after the IMSI Manager CPU reaches 60%:

```
task facility imsimgr avoid-sessmgr-broadcast cpu_threshold 60
```

Monitoring and Troubleshooting IMSI Manager Broadcast Control

New statistics are introduced as a part feature which can be viewed in the Debug mode. The operator can use these statistics to get the current status of broadcasting, which is either broadcasting is enabled or disabled.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs:

```
show demuxmgr statistics imsimgr all
```

- Total Unknown Subscriber Request Rx counters
- Insert Subscriber Data req
- Delete Subscriber Data req
- Cancel location req
- Other unknown req
- Imsimgr-Sessmgr Broadcast statistics for unknown Subscriber requests
- Broadcast Current status ( enabled/disabled and reason for disabling)
- Number of requests sent to Random smgr (after bcast failure rsp)
- Number of requests sent to Random smgr (broadcast disabled)
- Number of request dropped due to High CPU
Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics insimgr all. The show output is realigned for better readability. Unusual logs are added in IMSIMGR to print the IMSI of subscriber and the unknown request type received from the peer node. Debug logs are also provided to display the current CPU usage and the request types that are dropped.

**IMSI Manager Overload Control**

**Feature Description**

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mappings maintained for all registered subscribers are synchronous with the Session Managers.

When the incoming attach rate is high at the IMSIMGR in a short span of time, the CPU consumption is very high and affects the normal processing activities of the IMSI Manager. At times this can lead to an IMSI Manager crash. Overload control methods are devised through this feature enhancement to keep the IMSI Manager CPU under control.

---

**Important**

This feature is enabled by default.

**IMSI Manager Overload Control**

IMSI Manager Overload control is implemented on both SGSN and MME call flows. Attach rate throttling (network overload protection) is implemented in IMSI Manager to cap the rate at which new requests are accepted by SGSN and MME. This feature helps us process the incoming new subscriber requests (for example ATTACH/ISRAU) at a configured rate, therefore the HLR and other nodes are not overloaded. The SGSN and MME have separate pacing queues in the IMSI Manager to monitor the incoming rate of requests and have a separate network overload configuration as well.

For the SGSN, the following requests are paced using the pacing queues:

- Initial ATTACH (with IMSI, L-PTMSI, F-PTMSI)
- Inter-SGSN RAU
- Empty-CR requests

In the MME, new connections are setup for the following events:

- UE initiated initial Attach
- All types of attach – IMSI, local GUTI, foreign GUTI, mapped GUTI, emergency and so on.
- UE initiated Inter-CN node TAU request requiring context transfer from old MME/SGSN
- TAU request with foreign GUTI or mapped GUTI
- Peer SGSN/MME initiated forward relocation request via Gn/S10/S3
With this feature enhancement when the incoming attach rate is high, the pacing queue becomes full and the further requests are either dropped or forwarded to Session Manager. The Session Manager in turn sends the reject response based on the configuration. When network overload protection action is set as "reject", the IMSI Manager has to forward overflowing requests from the pacing queue to Session Manager through a messenger call to send back error response. The IMSI Manager spends more time on messenger read and write. The IMSI Manager CPU reaches high values when the incoming call rate is very high (both SGSN/MME) though the network overload protection is configured. To ensure that the IMSI Manager CPU is under control, the IMSI Manager reduces certain messenger activities on reaching the default CPU threshold of 70%. This threshold value is fixed and this feature is enabled by default. This value is currently non-configurable. The IMSI Manager drops the overflowing requests from the pacing queue when the CPU crosses 70% mark instead of rejecting the request. Every IMSI Manager instance monitors its CPU usage independently and actions are taken according to the CPU usage.

**Relationships to Other Features**

Attach throttling feature will have an impact due to this feature enhancement. Once the CPU reaches the threshold of 70%, the messages will be dropped (irrespective of configured action).

**Monitoring and Troubleshooting IMSI Manager Overload Control**

New statistics are introduced as a part of feature which can be viewed in the Debug mode. The operator can use these statistics to find the number of requests dropped due to overload.

**Show Command(s) and/or Outputs**

This section provides information regarding show commands and/or their outputs:

```
show demuxmgr statistics imsimgr all
```

These counters are available for both MME and SGSN separately.

- Requests dropped due to pacing queue with High Imsimgr CPU

Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics imsimgr all. The show output is realigned for better readability. Debug logs are also provided to display the current CPU usage.

**IMSI Manager Attach Rate Throttling Queue**

CSCuy08829 - imsimgr crash - Fatal Signal 6 Aborted PC: [0b001879/X] client_bounce()

**Feature Changes**

**Previous Behavior:** The MME and SGSN support network overload protection feature to throttle the incoming traffic to the specified rates. When the incoming pacing queue used for attach rate throttling is full, all further requests are either rejected or dropped based on the configured action.

**New Behavior:** When the incoming pacing queue used for attach rate throttling is full due to heavy traffic and the IMSI Manager CPU is higher than 70%, the IMSI Manager drops the requests even if the configured action is reject. Dropping the requests saves the IMSI Manager CPU time. The SGSN and MME have separate IMSI Manager queues for attach rate throttling and other actions that are taken independently based on the traffic and queue length.
**UPC Requests from GGSN**

CSCuy11739 - SessionManager restarts on failed assert:sn_gt_process_inv_local_event()

**Feature Changes**

**Previous Behavior:** The SGSN queued UPC Requests from the GGSN in cases where the RAB was preserved.

**New Behavior:** Now, the SGSN drops UPC Requests from the GGSN in cases where the RAB is already preserved.

**XID Requests Received during Ongoing Authentication**

CSCuu39329 - Sessmgr restarts: Segmentation fail at sessmgr_gprs_fsm_substate_initial

**Feature Changes**

**New Behavior:** There is a new counter, "XID Req rcvd-auth ongoing", displayed in the output generated by the `show gmm-sm statistics verbose` command. This counter tracks the number of XID Requests received during an Intra-RAU procedure while authentication is in progress.

**Stats Track Attach Rejects due to Same R-TLLI Collision**

CSCuz32230 / CSCuz34368 - Bulkstat to measure Random TLLI collision counter in CLI

**Feature Changes**

**New Behavior:** Two new bulk statistics have been added to the SGSN schema to track the number of times the SGSN rejects Attach Requests or Combined Attach Requests due to requests arriving, via GPRS service, at the same time with the same Random TLLI. Rejection is configured with the 'gmm-message' command in the SGSN Global Configuration mode.

- 2G-simple-attach-rej-randomtlli-collision
- 2G-combined-attach-rej-randomtlli-collision

**Change to Existing Statistics:** From Release 19.3 onwards, the SGSN schema's "2G-attach-rej-implicitly-detach" statistic responds to the following additional trigger:

- Based on settings for the SGSN Global Configuration `gmm-message` command, the SGSN rejects Attach Requests due to same Random TLLI collisions.

**SGSN Enhancements for 19.3**

This section identifies all of the SGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.
Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/ or fields in new or modified schema and/or show command output. For details, refer to the ASR 5x00 Statistics and Counters Reference for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your SGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

RTLLI Management for 2G M2M Devices

Feature Description

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

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

How It Works

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

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

**Configuring RTLLI Management**

No new commands or keywords have been added to the command line interface (CLI) in support of Fixed Random TLLI Management. Enabling / disabling this mechanism is integrated into existing CLI.

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

---

**Important**

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

---

**Verifying Both the RTLLI and the NSEI**

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

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

Notes:

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

**Verifying Only the RTLLI**

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

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

Notes:

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

**Verifying Configuration**

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

```
show configuration | grep gmm-mess
show configuration | grep old-
show configuration verbose | grep old-
```
Monitoring and Troubleshooting

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

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

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

Configured to Verify Both RTLLI and NSEI

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

```
[local]asr5000# show gbmgr all parser statistics all | grep use

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

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

Configured to Verify Only RTLLI

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

```
[local]asr5000# show gbmgr all parser statistics all | grep use

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

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

Verify Attach Rejects due to Same RTLLI

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

```
[local]asr5000#show gmm sm stats | grep Same random tlli collision

Same random tlli collision: 10
```

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

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

```
[local]asr5000# show bulkstats variables sgsn | grep colli
%2G-simple-attach-rej-randomtlli-collision% Int32 0 Counter
%2G-combined-attach-rej-randomtlli-collision% Int32 0 Counter
```
SGSN Enhancements for 19.2

This section identifies all of the SGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

**GTPU Error Indication Enhancement**

CSCuv52163 - Enhancement for GTPU Error Indication handling

*Important* With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

**Feature Description**

This enhancement provides a solution to avoid GTPU Path Failure when a burst of GTPU Error Indication occurs. This enhancement is applicable only for SGSN.

Consider the following scenario:
1 Following a kernel crash and Hardware Failure (Fabric corruption) in a Demux Card, the SGSN is unable to respond Echo Requests from the GGSN. This results in Path Failure detection by the GGSN and a large number of sessions are cleaned up.

2 But the sessions are still active at the SGSN in PSC3 Cards where Session Manager is running. The SGSN sends uplink data for these sessions and this triggers a flood of GTPU Error Indications (~6 to ~9 million) from the GGSN to SGSN.

3 Simultaneously a Demux card migration is triggered in the SGSN to recover from the kernel crash and Hardware Failure. After the migration is completed, the SGSN restarts the Path Management Echo Requests. But the GGSN had already started sending Echo requests as soon as the new sessions were set up at the GGSN. This difference in the restarting of the Echo requests from both ends on the path leads to delay in detecting path failure between the SGSN and GGSN if echo responses are not received for any reason.

4 Once the Demux card has recovered at SGSN, the following are observed:
   - A flood of GTPU Error Indication messages further result in packet drops at the SGSN
   - The Echo Request causing another path failure at the GGSN
   - Echo Response cause a path failure on the SGSN with delay as well as loss of GTPU Error Indications at SGSN

5 This delay in Path Failure results in another flood of GTPU Error Indications in response to SGSN uplink data for the active sessions, which were already cleaned up at the GGSN (those created after first path failure). This flood of GTPU Error Indications results in additional packet drops at the SGSN. The cycle of cleaning up sessions and setting up new sessions continues until the SGSN is restarted.

The issue is resolved by creating an additional midplane socket for GTPU Error Indications so that flood of GTPU Error Indication will not create any impact on Path Management. New midplane socket and flows have been introduced to avoid path management failure due to flood of GTPU Error Indication packets. GTPU Echo Request/Response will continue to be received at existing midplane sockets. A new path for GTPU Error Indication will prevent issues in Path Management towards GGSN or towards RNC and avoids un-wanted detection of path failures. This enhancement requires new flows to be installed at the NPU.

The following existing statistics are helpful in observing loss of packets and drop of GTPU Error Indication Packets:

   [local]asr5000# show sgtpu statistics
   Total Error Ind Rcvd: 0
   Rcvd from GGSN: 0
   Rcvd from RNC: 0
   Rcvd from GGSN through RNC: 0
   Rcvd from RNC through GGSN: 0

The following show commands are useful to verify the NPU related statistics:

   - To check the flow id range associated with sgtpcmgr, use the following command:
     For ASR55K: show npumgr flow range summary
   - To check whether flow corresponding to GTPU Error Indication is installed or not, use the following command:
     For ASR5K: [local]asr5000# show npu flow record min-flowid 11954243 max-flowid 11966018 slot 1 verbose
     For ASR55K: show npumgr flow statistics 5/1/0
Identity Procedure for Authentication Failure

CSCuv21382 - Authentication and Ciphering Failure - GSM authentication unacceptable

Important
With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

Feature Changes

Previous Behavior: By default, the SGSN did the following upon receipt of an authentication failure:

- During an Attach/RAU from a 3G subscriber, while authenticating the subscriber, on receiving authentication failure with cause "GSM Authentication Unacceptable", the SGSN would (1) send Authentication Reject if the authentication vectors were retrieved from the HLR or (2) would initiate SAIt toward the HLR if the authentication vectors were from the peer-SGSN and would then start authentication with the vectors from the HLR.

- During 2G ISRAU, on receiving authentication failure with cause "MAC failure", the SGSN would send Authentication Reject to the subscriber.

New Behavior: The new default behavior has the SGSN initiate the Identity Procedure upon receipt of the authentication failures noted in the above scenario because there is the possibility that the network might have used incorrect vectors to authenticate the MS/UE. Per 3GPP TS 24.008, the SGSN may trigger the identity procedure to get the IMSI from the subscriber and using that IMSI, the SGSN can fetch the correct authentication vectors from the HLR to authenticate the subscriber when the SGSN received authentication failures with the following causes:

- "GSM Authentication Unacceptable" in 3G
- "MAC Failure" in 2G

This behavior can be disabled with the configuration noted below.

Customer Impact: Fewer subscribers will lose network connectivity due to Authentication Rejects.

Command Changes

```
gmm perform-identity-on-auth-failure
```

This command is not new, but with Release 19.2, the default behavior has been extended to enable the SGSN to initiate the identity procedure on receiving authentication failures with either cause "MAC Failure" or cause "GSM Authentication Failure".

The following command sequence disables the SGSN's default behavior and causes the SGSN to perform the identity procedure upon receipt of an authentication failure:

```
config context context_name
    sgsn-service sgsn_svc_name
        no gmm perform-identity-on-auth-failure
end
```
Notes:

• If the default behavior has been disabled with the command sequence noted above, then to re-enable the identity procedure upon receipt of an authentication failure, re-enter the sequence but do not include the no prefix with the `gmm perform-identity-on-auth-failure` command.

Performance Indicator Changes

`show gmm-sm statistics verbose`

New with this release, the following statistics track the number of IMSI Identity Requests triggered in response to authentication failures of the types noted above.

The `show gmm-sm statistics verbose` command from the Exec mode will generate an output that includes the following:

```
IMSI-Identity-Req triggered due to auth failures:
  3G-GSM Auth Unacc:  0  2G-MAC failure:  0
  3G-MAC failure:  0
```

`show gmm-sm statistics`

The number of IMSI identity requests initiated by the SGSN are captured in the following counter. This counter is not new with this release.

```
Total-IMSI-Identity-Req
```

Target Access Restriction

CSCux33388 - InterSGSN 3G to 2G HO fails
CSCur41900 - Rollback Behavior in EPC during TAU/RAU Needs to be Corrected

Feature Changes

Target Access Restriction feature was added to the SGSN and MME in release 17.4. The purpose of this feature is to avoid rollback behavior that exists in RAU and TAs by checking target RAT Type IE present in the Context Request at the source node, and then rejecting the TAU/RAU based on the subscriber's ARD profile earlier in the cycle if the target RAT is restricted for the subscriber. Rollback behavior caused late TAU/RAU rejection, resulting in PDP/bearer deletion for the MME, PGW, and the SGSN, requiring the UE to reattach and reactivate lost PDP/bearer.

**Previous Behavior:** As a part of this functionality, the target access restriction feature instructs the source-SGSN or the source-MME to reject outbound RAU when the target access was restricted for the subscriber. Rejection was performed without checking "access-restriction-data no-check" in the call control profile configuration.

**New Behavior:** With release 17.6.1, a new command keyword `target-access-restriction` has been introduced to the call control profile configuration to control (enable/disable) target access restriction functionality. Target access restriction is now disabled by default on both the SGSN and the MME. Refer to the `Command Changes` section below for the command information to enable/disable this functionality.

The default behaviors for the SGSN and the MME now differ:
• **New Behavior for the MME only:** "target-access-restriction" keyword configuration will control the target access restriction feature for the MME without other consideration:

  - **No Rejection:** if "target-access-restriction" is *not enabled*, then the source-MME will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

  - **Rejection:** if "target-access-restriction" is *enabled*, then the source-MME will *reject* the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

• **New Behavior for the SGSN only:** "target-access-restriction" keyword configuration enables/disables the target access restriction feature. The SGSN also considers "access-restriction-data no-check" in the call control profile configuration prior to rejecting outbound RAU when target access restriction functionality is enabled. The SGSN's target access restriction behavior is dependent upon the SGSN's "access-restriction-data no-check" configuration:

  - **No Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

  - **Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will *ignore* the "target-access-restriction enabled" configuration and the source-SGSN will *reject* the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

---

**Command Changes for the MME**

`access-restriction-data`

With release 17.6.1, the MME has access to this command in the call-control-profile configuration mode. The new keyword `target-access-restriction` enables or disables rejection of the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

```plaintext
configure
call-control-profile ccprof_name
  access-restriction-data target-access-restriction
remove access-restriction-data [ target-access-restriction ]
end
```

**Notes:**

- Including the `target-access-restriction` keyword with the command enables the target access restriction feature.

- Including the `remove` command filter disables the target access restriction feature. Inclusion of the `target-access-restriction` keyword in the remove command is currently optional.
Command Changes for the SGSN

access-restriction-data

With release 17.6.1, the new keyword `target-access-restriction` enables or disables the Target Access Restriction feature.

```
configure
call-control-profile ccprof_name
  access-restriction-data [eutran-not-allowed | failure-code | no-check | target-access-restriction]
end
```

Notes:

- Including the `target-access-restriction` keyword with the command enables the target access restriction feature.
- With the target access restriction feature enabled, including the `no-check` keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- Including the `remove` command filter with the `target-access-restriction` keyword disables the target access restriction feature.
- With the target access restriction feature enabled, including the `remove` command filter with the `no-check` keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Performance Indicator Changes

show call-control-profile

The Target Access Restriction field will display in the output with Enabled or Disabled and it will appear similar to the following:

```
[local]test# show call-control-profile full name ccprof1
... Authentication Detach : Not configured
Regional Subscription Restriction Failure Code Value : 13
ARD-Checking : Enabled
ARD Failure Code : Disabled
Access Restriction Data : EUTRAN Allowed
Target Access Restriction : Enabled
Zone-Code Check : Enabled
... ...
```
show configuration verbose

The access-restriction-data target-access-restriction field displays in the output without the "remove" prefix to indicate it is Enabled or with the "remove" prefix to indicate the feature is Disabled. The output will appear similar to the following when the feature is enabled:

[llocal]test# show configuration verbose
...
call-control-profile ccpref1
   remove rau-inter ctxt-xfer-failure
   no subscriber-control-inactivity
   ...
   access-restriction-data target-access-restriction
   ...

UDPC2 Support for SGSN/MME

CSCuw02651 - MME MME Mgrs Scaling and new config support on different platforms

Important With Release 19.2.1, this feature is available as fully qualified Deploy Quality.

Feature Changes

The MME and SGSN now support the UDPC2 hardware. The maximum number of MME managers supported per chassis on ASR 5500 with DPC is 24, to support UDPC2 on ASR 5500 the maximum number of MME managers have been increased to 36. The CLI command task facility mmemgr per-sesscard-density { high
| normal } under the Global configuration mode is used to configure the density (number of MME managers) of MME managers per session card. The disadvantage of this command is it does not allow configuration of specific number of MME managers per card, but allows the operator to configure only high or normal density. This CLI is deprecated and new CLI commands are introduced to provide the operator with more flexibility to configure number of MME managers per active session cards (or per active session VM in case of VPC) and the total number of MME managers. The MME managers are now moved to Non-Demux card, therefore the number of managers depends on the number of session cards per chassis. The new CLI command enables the operator to spawn the maximum or desired number of MME managers even when the chassis is not fully loaded in the case of ASR 5K and ASR 5500 platforms. For VPC DI the operator can restrict max number of MME managers per chassis, if operator desires to scale with more session VMs without requiring additional MME managers.

In UDPC2, the number of Session Managers in ASR5500 is increased from 336 to 1008.

Note The StarOS does not support an ASR5500 deployment with mixed usage of DPC and DPC2 cards. All session cards in one ASR5500 have to be of the same type.

Note All product specific limits, capacity and performance, will remain same as compared to ASR5500 with DPC.
Command Changes

**task facility mmemgr per-sesscard-density { high | normal }**

This CLI command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid till release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command **task facility mmemgr per-sesscard-count count**.

```configure
task facility mmemgr per-sesscard-density { high | normal }
exit
```

**Notes:**

- This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.
- New commands are introduced to provide more flexibility to the operator to configure required number of MME managers per session card and to configure the desired number of MME managers per chassis.

**task facility mmemgr per-sesscard-count**

This CLI command is introduced to configure the desired number of MME managers per session card.

```configure
task facility mmemgr per-sesscard-count count
default task facility mmemgr per-sesscard-count
exit
```

**Notes:**

- The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to 6.
- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.
- This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.
- The keyword **default** resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured default number of MME managers per session card will be selected based on platform and card type. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>4</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>6</td>
</tr>
</tbody>
</table>
The keyword `per-sesscard-count count` is used to set the maximum number of MME managers per session card.

- The value of `count` is an integer with range 1 up to 6.

Listed below is the maximum number of MME managers allowed per session card based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>1</td>
</tr>
</tbody>
</table>

**task facility mmemgr max**

This CLI command is introduced to configure the desired number of MME managers per chassis.

```
configure
task facility mmemgr max value
default task facility mmemgr max
exit
```

Notes:

- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.
- The maximum number of MME managers that can be configured per chassis is varies based on the platform. However, the upper limit of MME managers per chassis is set to 36.
• This CLI is not configured by default. The keyword default resets the number of MME managers per chassis to the default values. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>36</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>1</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
</tbody>
</table>

• The keyword **max value** is used to set the maximum number of MME managers per chassis.
  * The maximum value is an integer with range 1 up to 36.

Listed below is the maximum number of MME managers allowed per chassis based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>36</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
</tbody>
</table>

**SGSN Enhancements for 19.0**

This section identifies all of the SGSN enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *SGSN Administration Guide* for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *ASR 5x00 Command Line Interface Reference* for this release.
Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *ASR 5x00 Statistics and Counters Reference* for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your SGSN.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

Cause Code Mapping of ESM #66 by SGSN and MME

CSCut50598 - 3GPP R11 new cause code '#66' Support

Feature Changes

This feature is developed to achieve compliance with Release 11 3GPP Technical Specifications. The Release 11 3GPP Technical Specification introduced a new ESM/SM cause code 'Requested APN not supported in current RAT and PLMN combination (cause code #66)'. This ESM/SM cause is used by the network to indicate that the procedure requested by the UE is rejected as the requested APN is not supported in the current RAT and PLMN. A UE which receives this cause will stop accessing the APN in the current RAT, but as soon as it enters another RAT type it will retry the APN.

In earlier releases, only cause code #27 and cause code #33 were supported. These codes were not sufficiently effective in restricting APN in a particular RAT. For example, UE which has received cause #27 (with timer = 24 hours) will stop retrying a PDN connection in every RAT for 24 hours. This is not the desired behavior in some cases APN cannot be restricted in a particular RAT. If the SGSN sends cause code #33 to the UE for an IMS APN, the UE/MS stops retrying the PDN connection for some time, but UE/MS will not automatically retry this APN in 4G, even though the APN is available there. The introduction of cause code #66 resolves this issue as the operator can block access to IMS APN in 2G/3G and can allow access in 4G.

This feature is applicable for both SGSN and MME.
**Important**

This is a 3GPP Release 11 compliance feature and will be applicable only to UEs capable of decoding ESM/SM cause code #66.

---

**Command Changes**

**restrict access-type**

The `restrict access-type` command under the APN profile configuration mode is used to configure PDP activation restriction on the basis of access type. A new command option `eps` for EPS networks is introduced for this feature. In earlier releases this command was supported only for GPRS and UMTS networks to perform QoS related restrictions. Now this command is also used to configure the APN not supported in particular RAT and PLMN combinations. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

```
configure apn-profile profile_name
  [no] restrict access-type { eps | { gprs | umts } | qos-class { background | conversational | interactive | streaming } } } } 
  default restrict access-type { eps | gprs | umts } 
end
```

Notes:

- This command is disabled by default.
- In earlier releases this command was applicable only for SGSN. It is now supported by MME also.
- If the operator does not include the optional QoS-Class keyword option, then complete APN restriction is enabled and QoS related restrictions have no impact as QoS restriction is a subset of a complete APN restriction.

**local-cause-code-mapping apn-not-supported-in-plmn-rat**

This command remaps the EMM/ESM/SM cause codes to operator-preferred codes in the Call Control Profile. These replacements codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

```
configure call-control-profile profile_name
  local-cause-code-mapping apn-not-supported-in-plmn-rat { emm-cause-code emm_cause_number
  esm-cause-code esm_cause_number | attach | tau } | esm-cause-code esm_cause_number esm-proc
  sm-cause-code sm_cause_number }
  remove local-cause-code-mapping apn-not-supported-in-plmn-rat | attach | esm-proc
  sm-cause-code | tau }
end
```

Notes:

- This mapping is not done by default.
• The keyword `apn-not-supported-in-plmn-rat` specifies that the configuration maps operator-preferred replacement cause codes when a call is rejected because the requested APN is not supported in current RAT and PLMN combination.

• `emm-cause-code emm_cause_number esm-cause-code esm_cause_number | attach | | tau |`

  * The keyword `emm-cause-code` configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.

  * `emm_cause_number` specifies the EMM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 2 through 111.

  * `esm-cause-code` configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.

  * `esm_cause_number` specifies the ESM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 8 through 112.

  * The `attach` keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.

  * The `tau` keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

• `esm-cause-code esm_cause_number esm-proc`

  * `esm-cause-code` configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

  * `esm_cause_number` specifies the ESM cause code replacement integer in the range 0 through 255.

  * The `esm-proc` keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

• `sm-cause-code sm_cause_number` specifies the SM cause code replacement value and this keyword is only for the SGSN’s call control profile.

**local-cause-code-mapping apn-not-supported-in-plmn-rat**

This command remaps use of the 3GPP Release 11 rejection code #66 to the the EMM/ESM cause codes preferred by the operator and records the remapping in the MME service configuration. These replacement codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

`configure`

  `context context_name`

  `mme-service service_name`

  `local-cause-code-mapping apn-not-supported-in-plmn-rat { emm-cause-code emm_cause_number esm-cause-code esm_cause_number | attach | | tau | |esm_cause_number esm-proc }`
default local-cause-code-mapping apn-not-supported-in-plmn-rat | attach | esm-proc | tau |
end

Notes:

• The keyword `apn-not-supported-in-plmn-rat` specifies that the cause codes to be used for a rejection due to the requested APN not being supported in the current RAT and PLMN combination are those that are mapped in the MME service configuration.

• `emm-cause-code` `emm_cause_number` `esm-cause-code` `esm_cause_number` | attach | | tau |
  * The keyword `emm-cause-code` configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.
    * `emm_cause_number` specifies the EMM code replacement integer in the range 0 through 255.

  * `esm-cause-code` configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.
    * `esm_cause_number` specifies the ESM code replacement integer in the range 0 through 255.

  * The `attach` keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.

  * The `tau` keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

• `esm-cause-code` `esm_cause_number` `esm-proc`
  * `esm-cause-code` configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.
    * `esm_cause_number` specifies the ESM cause code replacement integer in the range 0 through 255.

  * The `esm-proc` keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

Performance Indicator Changes

MME Schema

The following new statistics have been added to the MME schema to track MME support of the 3GPP Release 11 code for call rejections due to the APN not being supported under the PLMN / RAT combination:

• inter-node-srns-proc-fail-apn-not-supported
• inter-node-tau-proc-fail-apn-not-supported
• tai-esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
• tai-emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- attach-proc-fail-apn-not-sup-in-plmn-rat
- esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- emmdisc-apnnotsupinplmnrat

For descriptions of these variables, see *MME Schema Statistics* in the *Statistics and Counters Reference*.

**show configuration**

The following new parameters have been added to the show configuration command for this feature:

- restrict access-type umts/gprs/eps
- local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code <cause_number>
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code <cause_number> esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 32 esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 15 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau

**show apn-profile full**

The following new parameters have been added to the show apn-profile command for this feature:

- Service Restriction for Access Type UMTS
- Complete APN restricted
- Service Restriction for Access Type GPRS
- Complete APN restricted
- Service Restriction for Access Type EPS

**show call-control-profile full**

The following new parameters have been added to the show call-control-profile command for this feature:

- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination
- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Requested service option not subscribed (33)
- Cause Code Mapping
- APN not supported PLMN-RAT esm-proc: Operator Determined Barring (esm-8)
- APN not supported PLMN-RAT Attach: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
• APN not supported PLMN-RAT TAU: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)

**show gmm-sm statistics verbose**

The following new parameters are added to this show command to display the statistics for this feature:

• 3G-Pri-Actv-APN-Not-Sup-Rej
• 2G-Pri-Actv-APN-Not-Sup-Rej
• 3G-APN-Not-Supported-in-PLMN-RAT
• 2G-APN-Not-Supported-in-PLMN-RAT
• APN Not Supported in PLMN RAT combination Statistics
• 3G-Pdp-Dropped-During-New-SGSN-RAU
• 2G-Pdp-Dropped-During-New-SGSN-RAU
• 3G-Pdp-Dropped-During-New-SGSN-SRNS
• Pdp-Dropped-During-3G-To-2G-IRAT
• 3G-Actv-NRPCA-Reject
• Pdp-Dropped-During-2G-To-3G-IRAT
• APN not sup PLMN-RAT
• Inbound Inter node SRNS failure
• APN not sup in PLMN/RAT

**show mme-service name**

The following new parameters are added to this show command to display the statistics for this feature:

• APN not supported PLMN-RAT esm-proc : Requested APN not supported in current RAT and PLMN combination (esm-66)
• APN not supported PLMN-RAT Attach: ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
• APN not supported PLMN-RAT TAU: No Suitable Cells In tracking area (emm-15)

**EPC QoS Attributes**

CSCut64359 - for eARP and APN-AMBR and UE-AMBR QoS attributes on Gn-SGSN.

**Feature Changes**

The Gn-Gp SGSN now supports EPC QoS parameters during PDP Activation/Modification procedures. Support is added for Evolved-ARP, APN-AMBR and UE-AMBR QoS parameters. The purpose of adding
this support is to achieve end to end synchronization of QoS parameters during IRAT (3G/4G) mobility procedures. In previous releases it was observed that there is no synchronization between QoS parameters during TAU/RAU mobility from a 4G scenario to a 3G scenario or vice versa.

The EPC QoS attributes now supported Gn SGSN can be briefly described as below:

**Evolved-ARP (E-ARP):** Evolved allocation or retention priority specifies the relative importance of a Radio Access Bearers as compared to other Radio Access Bearers for allocation or retention of the Radio access bearer. The EPC uses Evolved ARP, which has priority level ranging from "1" up to "15". Additionally, evolved ARP comprises of pre-emption capability and pre-emption vulnerability. The preemption capability information defines whether a bearer with a lower priority level should be dropped to free up the required resources. The pre-emption vulnerability information indicates whether a bearer is applicable for such dropping by a preemption capable bearer with a higher priority value.

**APN-AMBR (per APN Aggregate Maximum Bit Rate):** The APN-AMBR limits the aggregate bit rate that can be provided across all Non- GBR PDP contexts of the same APN (for example, excess traffic may get discarded by a rate shaping function). Each of those Non-GBR PDP contexts can potentially utilize the entire APN AMBR (for example, when the other Non- GBR PDP contexts do not carry any traffic). The PGW enforces the APN AMBR in downlink. Enforcement of APN AMBR in uplink may be done in the UE and additionally in the PGW.

**UE-AMBR:** The UE AMBR limits the aggregate bit rate that can be provided across all Non-GBR PDP contexts of a UE (for example, excess traffic may get discarded by a rate shaping function). Each of the Non-GBR PDP contexts can potentially use the entire UE AMBR (for example, when the other Non-GBR PDP contexts do not carry any traffic). The GBR (real-time) PDP contexts are outside the scope of UE AMBR. The RAN enforces the UE AMBR in uplink and downlink.

With this feature enhancement the SGSN now supports the following functionalities:

1. EPC QoS parameters for Gn/Gp interface activated PDPs are supported.
2. The Gn-Gp SGSN reads the EPC QoS parameters from the HLR/HSS and the user.
3. The Gn-Gp SGSN now performs capping of the QoS parameters and sends the negotiated values towards the GGSN and RAN.

### Command Changes

epc-qos-params-in-gtpv1

This new command has been introduced in the QoS Profile configuration mode to enable or disable the SGSN to send EPC QoS parameters to GGSN.

```plaintext
configure
  quality-of-service-profile profile_name
    [remove] epc-qos-params-in-gtpv1 { eps-subscription | gprs-subscription }
end
```

Notes:

- This command is disabled by default.
- On enabling this command E-ARP and APN-AMBR parameters are included in the GTPV1 SM messages towards the GGSN
- If the keyword gprs-subscription is configured, E-ARP and APN-AMBR from the GPRS subscription are sent. The UE-AMBR value is read from the user (local capping).
class

New keywords are introduced in the `class` command under the QoS profile configuration mode to configure the E-ARP values.

```bash
configure
  quality-of-service-profile profile_name
  [remove] class { background | conversational | interactive | streaming } evolved-arp {
    preemption-capability capability_value | preemption-vulnerability vulnerability_value | priority-level level_value }
end
```

Notes:
- This command is disabled by default.
- Use the keyword `preemption-capability` to configure the preemption capability value. The value is configured as "0" or "1".
- Use the keyword `preemption-vulnerability` to configure the preemption capability value. The value is configured as "0" or "1".
- Use the keyword `priority-level` to configure the priority level of the E-ARP. The priority can be configured as any value in the range "1" up to "15".

prefer-as-cap

The existing command `prefer-as-cap` is used to instruct the SGSN to use either the local or subscription or both-subscription-and-local (lower of either the locally configured QoS bit rate or the subscription received from HLR/HSS) QoS configuration value as the capping value for the QoS parameters.

```bash
configure
  quality-of-service-profile profile_name
  prefer-as-cap [ both-subscription-and-local | subscription | local ]
end
```

override-arp-with-ggsn-arp

The existing command `[remove] override-arp-with-ggsn-arp` under the Call Control Profile is used to enable or disable the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

```bash
configure
  call-control-profile profile_name
  [remove] override-arp-with-ggsn-arp
end
```

Performance Indicator Changes

show quality-of-service-profile full all

The following parameter is displayed if `gprs-subscription` is selected in the `epc-qos-params-in-gtpv1` command:
• Sending of epc-qos-params to GGSN

show subscriber sgsn-only full all

The following new parameters are added to the show subscriber sgsn-only full all command:

• Evolved Allocation/Retention Priority
• Priority level
• Pre-emption Vulnerability
• Pre-emption Capability
• AMBR
• Negotiated APN-AMBR UL
• Negotiated APN-AMBR DL
• Max-Requested-Bandwidth-UL
• Max-Requested-Bandwidth-DL
• Applied UE-AMBR DL

IMSI Range Support Expanded

CSCuu50781 - IMSI-Range analysis limit reached in Cisco SGSN

Feature Changes

From release 19.0 onwards, the IMSI range supported has been enhanced to "2500" from "1000". The IMSI ranges configured must be unique, the SGSN selects the appropriate operator policy based on the IMSI range of the UE. The operator can verify the configured IMSI ranges and the associated operator policy by issuing the command "show config". The length of the description field in the imsi-range command under the SGSN Global Configuration mode has been reduced from a maximum of "100" alphanumeric characters to "50" alphanumeric characters. Reduction of the supported string size results in improvement of the boot up time.

Command Changes

imsi-range

This command is used to configure an IMSI range with an optional PLMN ID to associate with an Operator Policy.

configure
sgsn-global
    imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number [ operator-policy policy_name [ description description ] | plmnid plmn_id operator-policy policy_name [ description description ] ] | plmnid plmn_id } +
no imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number | plmnid plmn_id}
Notes:

- The length of the description field has been reduced from a maximum of "100" alphanumeric characters to "50" alphanumeric characters. Reduction of the supported string size results in improvement of the boot up time.

**Uplink Data Status IE in Service Request**

CSCuu03824 - Uplink data status IE in service req

**Feature Changes**

The Gn SGSN now supports processing of Uplink Data Status IE in Service Request; RABs are established for NSAPIs present in the Uplink Data Status IE. With this feature enhancement the RAB's are selectively established for NSAPIs which require uplink data transfer. In earlier releases RABs were established for all PDPs. Support has been added to decode Uplink Data Status IE in the Service Request. Performance improvement and reduced signaling are observed as RABs are established only for NSAPIs which require uplink data transfer.

A new CLI command has been provided under the Call Control Profile to enable or disable the feature. The user can configure the CLI to either ignore or process the Uplink Data Status IE in Service Request. This feature is enabled by default.

**Command Changes**

```
ignore-ul-data-status
```

This new CLI command under the Call Control Profile is used enable or disable processing of Uplink Data Status IE in Service Request.

```
configure
  call-control-profile profile_name
  [remove] ignore-ul-data-status
end
```

Notes:

- This feature is enabled by default, to disable the feature use the command `ignore-ul-data-status`
- To enable this feature use the command `remove ignore-ul-data-status`
- When this feature is enabled, RAB is established for NSAPIs present in the Uplink data status IE. RABs are not established if the NSAPI PDPs are not present in the SGSN. If the Uplink data Status IE contains NSAPI not known to the SGSN, the SGSN establishes all the RAB's. RAB's are not established if corresponding NSAPI is absent in the PDP-Context Status IE.
- When this feature is disabled, if Uplink data status IE is received in service request the SGSN ignores it and establishes RABs for all the PDPs.
Performance Indicator Changes

**show call-control-profile full**

The `show call-control-profile full` command is used to verify the configuration of this feature. The following field displays whether the Uplink Data Status IE is **Processed** or **Ignored**:

- Uplink data status IE in service request

**show gmm-sm statistics**

This `show` command is updated to display the number of RABs not re-established due to absence of NSAPI bit set in the Uplink Data Status IE. This field is also used as a measure to verify the reduction in radio signaling. The following new field is added to the `show` output:

- Rab-Not-Re-Estd-UL-Data-Stat
Uplink Data Status IE in Service Request
S-GW Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from Serving Gateway (S-GW) in StarOS 19 software releases.

- S-GW Enhancements for 19.6.6, page 437
- S-GW Enhancements for 19.5, page 438
- S-GW Enhancements for 19.4, page 439
- S-GW Enhancements for 19.3, page 440
- S-GW Enhancements for 19.2, page 441
- S-GW Enhancements for 19.1, page 443
- S-GW Enhancements for 19.0, page 445

S-GW Enhancements for 19.6.6

This section identifies all of the S-GW enhancements included in this release:

**Feature Changes** - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your S-GW.

- AAA Enhancements
- CF Enhancements
HTTP Injector Fraud When There Is No User-Agent in the HTTP

Applicable Products: S-GW

Feature Changes

Previous Behavior: The HTTP redirection was happening only for GET and POST methods.

New Behavior: All HTTP request packets which are charged by DCCA is redirected in case of Final Unit Indication (FUI) redirection.

Customer Impact: In case of FUI redirection, increase in the number of redirection might be seen.

S-GW Enhancements for 19.5

This section identifies all of the S-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your S-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
Packet With Unexpected GTP Version

CSCuz86464 - Packet with unexpected GTP version: Behavior change.

Applicable Products: P-GW, SAEGW, S-GW

Packet With Unexpected GTP Version

Old Behavior: Earlier, if GTP-v2 received messages with version v1, v0, or above v2 sent a response messages stating "version not supported".

New Behavior: Now, if GTP-v2 received messages with v1 or v0, messages would be silently discarded. However, if the version is above v2, GTP-v2 sends a response message stating "version not supported".

Impact on Customers: Since the v0 and v1 messages are silently discarded, peer may not see any response and retry the same.

S-GW Enhancements for 19.4

This section identifies all of the S-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your S-GW.

• AAA Enhancements
• CF Enhancements
• ECS Enhancements
• Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
S-GW Changes in Release 19

SPGW Incorrectly Sending UDPv6 Packets

CSCuy78988- SPGW incorrectly sending UDPv6 packets with 0x0 checksum against RFC2460

Applicable Products: GGSN, P-GW, SAEGW, S-GW

Feature Changes

Previous Behavior: Earlier, if the result of the UDPv6 checksum calculation is zero, GW used to send the same, which effectively disables checksum for that packet. This was not compliant with the RFC2460, which suggests the checksum value to be set to 0xFFFF if derived calculation is zero.

New Behavior: After the fix, the checksum value is set to 0xFFFF if the result checksum calculation is ZERO and the compliance is met.

Impact on customer: Packet drops might be seen at peer, which does not support of handling packet with 0xFFFF checksum as suggested by the RFC.

S-GW Enhancements for 19.3

This section identifies all of the S-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Important

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your S-GW.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
Correction for Unexpected Session Deletion on the S-GW

CDETS = CSCux10033 - Unexpected Session Deletion on S-GW

Applicable Products: S-GW

The fix implemented for CSCux10033 has resulted in a behavior change. Consider the following scenario:

- The `egtp cause-code temp-fail dbf-proc` CLI command is configured on the S-GW.
- A Modify Bearer Request (MBR) message is received by the S-GW from the MME.
- The Bearer context instance value is set to 1 under the MBR message.
- In response to this MBR, the P-GW sends a Delete Bearer Request message (DBR) to the S-GW.

This led to an unexpected event for the bearer at the S-GW, and the call was dropped.

Previous Behavior: The S-GW removed the bearer as soon as the MBR was received by changing the bearer state to 'disconnecting'.

New Behavior: The S-GW marks this bearer as an IDLE bearer but does not remove it. The S-GW waits for a Delete Bearer Command/Delete Bearer Response (DBC/DBR) message to delete the bearer as an expected scenario. The S-GW also permanently suspends this bearer by changing its state to drop data on idle at the session manager. Since this bearer is to be removed, the S-GW blocks any data level signaling. Thus, any new downlink data will not trigger a Downlink Data Notification procedure (DDN) for this suspended bearer. A DDN will be triggered for all other bearers with downlink data if they are in the IDLE state.

Customer Impact: The S-GW complies with version 10 of 3GPP 29.274. There will be no impact if the MME complies with the same version. In the case of non-compliance, the MME does not send a DBC. The bearer remains idle with the S-GW and will eventually be deleted when the next MBR is received.

S-GW Enhancements for 19.2

This section identifies all of the S-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.
This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your S-GW.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

### Command Output to Show Subscriber Throughput per TAC/RAC and APN

**CSCuv94689** - Display of PDN Connection count based on TAC/RAC/APN

**Applicable Products:** SAEGW, S-GW

#### Feature Changes

New keywords have been added to the `show sgw-service statistics all` and `show saegw-service statistics all` Command Line Interface (CLI) commands. The keywords enable operators to view S-GW and SAEGW service statistics per Tracking Area Code (TAC), per Routing Area Code (RAC), or per TAC/RAC and the associated Access Point Name (APN). Specifically, the command output provides the total number of currently active PDN connections.

**Previous Behavior:** No Command Line Interface (CLI) command was available to show S-GW/SAEGW service statistics per TAC, RAC, and APN.

**New Behavior:** A new CLI command has been introduced to show S-GW/SAEGW service statistics per TAC, RAC, and APN

#### Command Changes

`show sgw-service statistics all`

The `tac`, `rac`, and `apn` keywords have been added to the `show sgw-service statistics all` command. This allows operators to view the number of active PDN connections for a particular TAC or RAC, or a TAC/RAC and its associated APN.

`show sgw-service statistics all [ tac <integer> | rac <integer> | apn <string> ]`
Notes:

- **tac**: Specifies the specific TAC as per 3GPP standards in TS 29.274. Valid entries are from 0 to 65535.
- **rac**: Specifies the specific RAC as per 3GPP standards in TS 29.274. Valid entries are from 0 to 65535.
- **apn**: Specifies the name of a configured APN. The APN entry must be an alphanumeric string from 1 to 62 characters in length.

**show saegw-service statistics all func sgw**

The `tac`, `rac`, and `apn` keywords have been added to the `show saegw-service statistics all func sgw` command. This allows operators to view the number of active PDN connections for a particular TAC, RAC, or for a TAC/RAC and its associated APN.

**show saegw-service statistics all function sgw [ tac <integer> | rac <integer> | apn <string> ]**

Notes:

- **tac**: Specifies the specific TAC as per 3GPP standards in TS 29.274. Valid entries are from 0 to 65535.
- **rac**: Specifies the specific RAC as per 3GPP standards in TS 29.274. Valid entries are from 0 to 65535.
- **apn**: Specifies the name of a configured APN. The APN entry must be an alphanumeric string from 1 to 62 characters in length.

**Performance Indicator Changes**

**show sgw-service statistics all**

The output of this command has been enhanced to provide the number of active PDN connections for a particular TAC or RAC, or for a TAC/RAC and its associated APN.

For example:

**show sgw-service statistics all rac 1280 apn provider.com**

```
... Total Number of Pdn Connections: <Total>
```

**show saegw-service statistics all func sgw**

The output of this command has been enhanced to provide the number of active PDN connections for a particular TAC or RAC, or for a TAC/RAC and its associated APN.

For example:

**show saegw-service statistics all function sgw rac 1280 apn provider.com**

```
... Total Number of Pdn Connections: <Total>
```

**S-GW Enhancements for 19.1**

This section identifies all of the S-GW enhancements included in this release:
**Feature Changes** - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

---

**Important**

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, *some of which might* include content applicable to your S-GW.

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

---

### 128k eNodeB Support

**Related CDETS ID:** CSCut76893

#### Feature Changes

Previously, the StarOS supported up to 64k eNodeBs. However, in some densely populated regions there can be more than 64k eNodeBs. Or, there could be a large number of small Cell eNodeBs directly connecting to an S-GW over the S1-U interface. There could also be P-GW and S-GW peers in the GTPU data path. With StarOS release 19.1, up to 128k eNodebs are supported. Note that 128k is a collective limit for P-GW/S-GW peers in the GTPU data path as well as S1-U peers. This enables operators to anchor a large number of such eNodeBs or small Cell eNodeBs.

---

**Important**

128k eNodeB Support is an optional licensed feature. Contact your Cisco account or service representative for detailed information on licensing requirements.

**Previous Behavior:** Up to 64k eNodeBs were supported.

**New Behavior:** Up to 128k eNodeBs are now supported.
Customer Impact: Operators can anchor an increased number of eNodeBs or small Cell eNodeBs.

S-GW Enhancements for 19.0

This section identifies all of the S-GW enhancements included in this release:

Feature Changes - new or modified features or behavior changes. For details, refer to the S-GW Administration Guide for this release.

Command Changes - changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

This release includes enhancements that are applicable to multiple products. The following lists the various multi-product enhancements sections, some of which might include content applicable to your S-GW.

• AAA Enhancements
• CF Enhancements
• ECS Enhancements
• Firewall Enhancements
• GTPP Enhancements
• Lawful Intercept Enhancements
• MVG Enhancements
• NAT Enhancements
• SNMP MIB Enhancements
• System and Platform Enhancements

Event-Based Idle Second Micro-Checkpoint Generation for S-GW

CSCut82325 - Support event based idle sec micro-checkpoint generation for SGW

Related CDETS ID = CSCut55276

Feature Changes

To reduce the number of micro-checkpoints to peers for sessions moving from active to idle and idle to active, a new approach has been introduced using event-based micro-checkpoint generation.

This feature involves sending an idle sec micro-checkpoint from an active to standby chassis when the session state changes from active to idle or from idle to active. The micro-checkpoint carries information about the time when the session became active or idle. Upon receipt of the micro-checkpoint, the Standby chassis updates...
the active/idle time. This process enables the active and standby chassis to be synchronized with respect to when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event occurs, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not.

New configuration has been added per S-GW service to send micro-checkpoints only when UE transitions from idle to active or active to idle.

**Previous Behavior:** Micro-checkpoints were configurable only with the `timeout idle micro-checkpoint-periodicity` option in the `timeout idle` command.

**New Behavior:** The `micro-checkpoint-deemed-idle` option is added to the `timeout idle` command to configure event-based sending of micro-checkpoints.

**Customer Impact:** More efficient sending of micro-checkpoints to the standby chassis along with an increase in SRP bandwidth.

### Command Changes

**timeout idle**

The new keyword `micro-checkpoint-deemed-idle` has been added to this command to configure the time duration, in seconds, after which a session is deemed idle or active and determines whether a micro-checkpoint must be sent.

```
configure
  context context_name
    apn apn_name
      timeout idle dur_seconds [ micro-checkpoint-deemed-idle time_in_seconds ]
    end
micro-checkpoint-periodicity time_in_seconds ]
  } { default | no } timeout idle
end
```

**Notes:**

- **`micro-checkpoint-deemed-idle time_in_seconds`:** Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis.

  The `micro-checkpoint-deemed-idle` setting should be less than the `timeout idle` setting.

  `time_in_seconds` must be an integer from 10 to 1000.

  Default: 180

- **`default`:** Indicates the timeout specified is to be returned to its default behavior.

- **`no`:** Disables the timeout idle functionality.

- Either the `micro-checkpoint-deemed-idle` or `micro-checkpoint-periodicity` value can be configured for idle time duration.

- Any change from `micro-checkpoint-deemed-idle` to `micro-checkpoint-periodicity`, or vice versa, requires removing the first configuration before adding the new configuration.
Performance Indicator Changes

show configuration

The output of this command has been enhanced to show the micro-checkpoint-deemed-idle setting:

- timeout idle <duration_seconds> micro-checkpoint-deemed-idle <duration_seconds>

show sgw-service name service_name

The following new field has been added to show idle timeout configuration at the S-GW service level:

- idle seconds deemed idle checkpoint periodicity

IMSI/IMEI Available in System Event Logs of Type Error and Critical

CSCuu51587, CSCut68271 - Inclusion of IMSI/IMEI in logs

Applicable Products = GGSN, P-GW, SAEGW, S-GW

Feature Changes

Previous Behavior: The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all system event logs of type error and critical.

New Behavior: The GGSN/P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available.

Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.

Important

Table 7: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format &quot;[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d&quot;</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s&quot;</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Ran out of session handles&quot;</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format &quot;[IMSI &lt;IMSI&gt;]%s&quot;</td>
</tr>
</tbody>
</table>
### Event Log #
<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>139001</strong></td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td><strong>191006</strong></td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td><strong>10034</strong></td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td><strong>10035</strong></td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td><strong>12382</strong></td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s&quot;. For example &quot;[IMSI 11223445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td><strong>12668</strong></td>
<td>Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot;</td>
</tr>
<tr>
<td><strong>12774</strong></td>
<td>Represents pgw_purge_invalid_crr in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot;</td>
</tr>
<tr>
<td><strong>12855</strong></td>
<td>Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td><strong>12857</strong></td>
<td>Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td><strong>12858</strong></td>
<td>Represents ncqos_nrxx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td><strong>12859</strong></td>
<td>Represents ncqos_nrxx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%u&gt;:pf_id_bitmap 0x%x and tft_opcode: %d&quot;</td>
</tr>
<tr>
<td><strong>12860</strong></td>
<td>Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td><strong>12861</strong></td>
<td>Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;%s&gt;.&quot;</td>
</tr>
<tr>
<td><strong>12862</strong></td>
<td>Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state: &lt;%s&gt;, [event: &lt;%s&gt;]&quot;</td>
</tr>
<tr>
<td><strong>11830</strong></td>
<td>Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
</tbody>
</table>
**Command Changes**

**logging**

The `include-uid` keyword has been added to the `logging` command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
configure
  logging include-uid
  no logging include-uid
end
```
Performance Indicator Changes

show configuration

The output of this command has been enhanced to indicate if the logging command is enabled with the include-ueid keyword.

- logging include-ueid
- no logging include-ueid

"Newcall policy reject" Enhancement for Releasing Existing Calls

CSCuu21036 - Newcall policy reject enhancement for releasing existing calls

Applicable Products = GGSN, P-GW, SAEGW, S-GW

Feature Changes

If the newcall policy is set to reject release-existing-session and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When GGSN/P-GW/SAEGW/S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Command Changes

newcall policy

The keyword release-existing-session has been added to this command to reject and release existing IMSI/IMEI session(s) when newcall arrives.

newcall policy sgw-service { all | name service_name } reject [ release-existing-session ]
no newcall policy sgw-service { all | name service_name }

Notes:

- reject release-existing-session: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Disabled by default.

Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions.
Performance Indicator Changes

show egtpc statistics verbose

The following new field has been added to indicate such calls released:

• NewCall Reject Existing Sessions Released

S-GW Collision Handling Enhancement

CSCuu19566 - S-GW Collision Handling

Feature Changes

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The S-GW has been enhanced to process collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification (DDN) message with Create Bearer Request or Update Bearer Request.

Previous Behavior:

1. Whenever a Create Bearer Request (CBReq) and Modify Bearer Request (MBReq) [Inter MME/Inter RAT (with or without ULI change)] were detected at the S-GW ingress interface, the S-GW rejected the current CBReq and would send a failure message to the P-GW. The S-GW would then handle the incoming MBReq.
2. Whenever an Update Bearer Request (UBReq) and MBReq [Inter MME/Inter RAT (with or without ULI change)] were detected at the S-GW ingress interface, the S-GW rejected the current UBRReq and would send a failure message to the P-GW. The S-GW would then handle the incoming MBReq.
3. Whenever a Downlink Data Notification (DDN) was ongoing, the S-GW rejected the incoming Create Bearer Request (CBReq) or Update Bearer Request (UBReq) and a failure message was sent to the P-GW.

New Behavior:

1. A CBReq and MBReq [(Inter MME/Inter RAT (with or without ULI change)] collision at the S-GW ingress interface results in the messages being handled in parallel. The CBReq will wait for a Create Bearer Response (CBRsp) from the peer. Additionally, an MBReq is sent in parallel to the P-GW.
2. An UBRReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change)] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBRReq would be suspended and the MBReq would be processed. Once the MBResp is sent to the peer from the SGW ingress interface, the UBRReq procedure is resumed.
3. The Downlink Data Notification (DDN) message transaction is dis-associated from bearers. So Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

Customer Impact: No S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.
Performance Indicator Changes

show egtp statistics verbose

The output of this command has been enhanced to provide information on GTPv2 message collisions at the S-GW ingress interface, including:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type)**: The new procedure and message type.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old**: Abort the original message handling and processes the new message.
  - **Reject New**: The new message is rejected, and the original (old) message is processed.
  - **Silent Drop New**: Drop the new incoming message, and the old message is processed.
  - **Parallel Hndl**: Both the original (old) and new messages are handled in parallel.
  - **Buffer New**: The new message is buffered and processed once the original (old) message processing is done.
- **Counter**: The number of times each collision type has occurred.

---

The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

Syslogging of Reject Events

CSCuu21047 - Inclusion of IMSI in EGTPC logs for reject events

**Applicable Products** = GGSN, P-GW, SAEGW, S-GW

Feature Changes

**Previous Behavior**: The International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) were not available in the details of all eGTP-C system event logs of type error and critical.
**New Behavior: New Behavior:** The P-GW/SAEGW/S-GW can be configured to provide the IMSI/IMEI in the eGTP-C event log details for the system event logs of type error and critical, if available. If the IMSI is not available, the P-GW/SAEGW/S-GW will make the best effort to obtain the IMEI.

### Command Changes

**logging**

The `include-uid` keyword has been added to the `logging` command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

```
configure
    logging include-uid
    no logging include-uid
end
```

### Performance Indicator Changes

**show configuration**

The output of this command has been enhanced to indicate if the `logging` command is enabled with the `include-uid` keyword.

- logging include-uid
- no logging include-uid
Syslogging of Reject Events
SNMP MIB Changes in Release 19

This chapter identifies SNMP MIB objects and alarms added to, modified for, or deprecated from StarOS 19 software releases.

- SNMP MIB Object Changes for 19.5, page 455
- SNMP MIB Alarm Changes as of 19.5, page 456
- SNMP MIB Conformance Changes for 19.5, page 457
- SNMP MIB Object Changes for 19.4, page 457
- SNMP MIB Alarm Changes as of 19.4, page 459
- SNMP MIB Conformance Changes for 19.4, page 459
- SNMP MIB Object Changes for 19.2, page 460
- SNMP MIB Alarm Changes as of 19.2, page 461
- SNMP MIB Conformance Changes for 19.2, page 462
- SNMP Command Changes for 19.2, page 463
- SNMP MIB Object Changes for 19.0, page 463
- SNMP MIB Alarm Changes as of 19.0, page 464
- SNMP MIB Conformance Changes for 19.0, page 465
- SNMP Command Changes for 19.0, page 466

SNMP MIB Object Changes for 19.5

This section provides information on SNMP MIB object changes in release 19.5.

Important

For more information regarding SNMP MIB objects in this section, refer to the SNMP MIB Reference for this release.
New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 19.5.
The following objects are new in this release:
• starHdRaidMgmtCardSwitchoverCause

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 19.5.
The following objects have been modified in this release:
None in this release.

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 19.5.
The following objects have been deprecated in this release:
None in this release.

SNMP MIB Alarm Changes as of 19.5

This section provides information on SNMP MIB alarm changes in release 19.5.

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 19.5.
The following alarms are new in this release:
• starHdRaidMgmtCardSwitchover

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 19.5.
The following alarms have been modified in this release:
None in this release.
Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 19.5.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 19.5

This section provides information on SNMP MIB conformance changes in release 19.5.

<table>
<thead>
<tr>
<th>Important</th>
<th>For more information regarding SNMP MIB alarms in this section, refer to the SNMP MIB Reference for this release.</th>
</tr>
</thead>
</table>

New SNMP MIB Conformance

This section identifies new SNMP MIB units of conformance available in release 19.5.
The following units of conformance are new in this release:
None in this release.

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 19.5.
The following units of conformance have been modified in this release:
None in this release.

Deprecated SNMP MIB Conformance

This section identifies modified SNMP MIB units of conformance available in release 19.5.
The following units of conformance have been deprecated in this release:
None in this release.

SNMP MIB Object Changes for 19.4

This section provides information on SNMP MIB object changes in release 19.4.
New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 19.4.

The following objects are new in this release:

- starStatFileSizeLimit
- starStatFileSizeMeasured

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 19.4.

The following objects have been modified in this release:

- starSlotEntry
- starDeviceNum
- starSerdesNum
- starImsimgrInstId
- starLAGGroup
- starLAGMinlink
- starVRFName
- starBGPPeerIpv6Address
- starMMEEMBMSServiceVpnName
- starMMEEMBMSServiceServName
- starMMEEMBMSPeerId
- starMMEEMBMSPeerIpAddr
- starMMEEMBMSPeerPortNum

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 19.4.

The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes as of 19.4

This section provides information on SNMP MIB alarm changes in release 19.4.

**Important**

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 19.4.
The following alarms are new in this release:
None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 19.4.
The following alarms have been modified in this release:
- starSerdesLanePermDown

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 19.4.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 19.4

This section provides information on SNMP MIB conformance changes in release 19.4.

**Important**

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

New SNMP MIB Conformance

This section identifies new SNMP MIB units of conformance available in release 19.4.
The following units of conformance are new in this release:
Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 19.4.
The following alarms have been modified in this release:

- starSerdesLanePermDown

Deprecated SNMP MIB Conformance

This section identifies modified SNMP MIB units of conformance available in release 19.4.
The following units of conformance have been deprecated in this release:
None in this release.

SNMP MIB Object Changes for 19.2

This section provides information on SNMP MIB object changes in release 19.2.

Important

For more information regarding SNMP MIB objects in this section, refer to the SNMP MIB Reference for this release.

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 19.2.
The following objects are new in this release:
None in this release.

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 19.2.
The following objects have been modified in this release:
None in this release.

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 19.2.
The following objects have been deprecated in this release:
None in this release.

SNMP MIB Alarm Changes as of 19.2

This section provides information on SNMP MIB alarm changes in release 19.2.

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 19.2.
The following alarms are new in this release:

- starThreshEPDGIGEVE2SetupAttempts
- starThreshClearEPDGIGEVE2SetupAttempts
- starThreshEPDGIGEVE2AuthFailures
- starThreshClearEPDGIGEVE2AuthFailures
- starThreshEPDGIGEVE2SetupSuccess
- starThreshClearEPDGIGEVE2SetupSuccess
- starThreshEPDGIGEVE2SetupFailure
- starThreshClearEPDGIGEVE2SetupFailure
- starThreshEPDGIGEVE2SetupFailureRate
- starThreshClearEPDGIGEVE2SetupFailureRate
- starSAEGWServiceStart
- starSAEGWServiceStop
- starStatFilesizeExceeded
- starStatFilesizeClear

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 19.2.
The following alarms have been modified in this release:

- starDhcpServiceStarted
- starDhcpServiceStopped
Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 19.2.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 19.2

This section provides information on SNMP MIB conformance changes in release 19.2.

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

New SNMP MIB Conformance

This section identifies new SNMP MIB units of conformance available in release 19.2.
The following units of conformance are new in this release:

- starThreshEPDGIKEV2SetupAttempts
- starThreshClearEPDGIKEV2SetupAttempts
- starThreshEPDGIKEV2AuthFailures
- starThreshClearEPDGIKEV2AuthFailures
- starThreshEPDGIKEV2SetupSuccess
- starThreshClearEPDGIKEV2SetupSuccess
- starThreshEPDGIKEV2SetupFailure
- starThreshClearEPDGIKEV2SetupFailure
- starThreshEPDGIKEV2SetupFailureRate
- starThreshClearEPDGIKEV2SetupFailureRate

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 19.2.
The following units of conformance have been modified in this release:
None in this release.
Deprecated SNMP MIB Conformance

This section identifies modified SNMP MIB units of conformance available in release 19.2.
The following units of conformance have been deprecated in this release:
None in this release.

SNMP Command Changes for 19.2

SNMPV3 querie resulting unknows User.

CSCuq91882 - SNMPV3 querie resulting unknows User.

Feature Changes

Secure SNMPv3 Support for SNMP Trap Handling

This feature is a protocol stack activity change. This functionality is now supported in Release 19.2. The \texttt{snmp user} command supports this feature.

\textbf{Important} For more information on the \texttt{snmp user} command, see the \textit{Global Configuration Mode Commands (L-S)} in the \textit{Command Line Interface Reference}.

SNMP MIB Object Changes for 19.0

This section provides information on SNMP MIB object changes in release 19.0.

\textbf{Important} For more information regarding SNMP MIB objects in this section, refer to the \textit{SNMP MIB Reference} for this release.

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 19.0.
The following objects are new in this release:

- starDeviceNum
- starSerdesNum
Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 19.0. The following objects have been modified in this release:

None in this release.

 Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 19.0. The following objects have been deprecated in this release:

None in this release.

SNMP MIB Alarm Changes as of 19.0

This section provides information on SNMP MIB alarm changes in release 19.0.

Important

For more information regarding SNMP MIB alarms in this section, refer to the SNMP MIB Reference for this release.

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 19.0. The following alarms are new in this release:

• starSessCapReached
• starDeviceNum starSerdesLanePermDown
• starLAGGroupDownDueToMinlink
• starThreshAllFramedRoutes
• starThreshAllFramedRoutesClear
• starThreshAllTotalRoutes
• starThreshAllTotalRoutesClear
• starThreshVRFFramedRoutes
• starThreshVRFFramedRoutesClear
• starThreshVRFTotalRoutes
• starThreshVRFTotalRoutesClear

**Modified SNMP MIB Alarms**

This section identifies SNMP MIB alarms modified in release 19.0.
The following alarms have been modified in this release:
None in this release.

**Deprecated SNMP MIB Alarms**

This section identifies SNMP MIB alarms that are no longer supported in release 19.0.
The following alarms have been deprecated in this release:
None in this release.

**SNMP MIB Conformance Changes for 19.0**

This section provides information on SNMP MIB conformance changes in release 19.0.

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

**New SNMP MIB Conformance**

This section identifies new SNMP MIB units of conformance available in release 19.0.
The following units of conformance are new in this release:
None in this release.

**Modified SNMP MIB Conformance**

This section identifies modified SNMP MIB conformance available in release 19.0.
The following units of conformance have been modified in this release:
None in this release.

**Deprecated SNMP MIB Conformance**

This section identifies modified SNMP MIB units of conformance available in release 19.0.
The following units of conformance have been deprecated in this release:
None in this release.

SNMP Command Changes for 19.0

Increase Default Number of Notifications Required Before Propagation to SNMP Users

CSCuu45560 - SNMP traps not generated after unplanned card migration

Command Changes

snmp notif-threshold

This command configures the number of SNMP notifications that need to be generated for a given event before it is propagated to SNMP users. The default high value has been increased from 100 to 300.

`snmp notif-threshold count`

Notes:

• `count`

• Default: 300

• The traps creation rate will be monitored periodically (as configured by the `period` field). If the number of traps created over one period cycle exceeds the count value configured, then the trap creation will be disabled. `count` must be an integer from 1 through 10000.
System Changes in Release 19

This chapter identifies platform system-level features and functionality added to, modified for, or deprecated from StarOS 19 software releases.

- System and Platform Enhancements for Release 19.6, page 467
- System and Platform Enhancements for Release 19.3, page 469
- System and Platform Enhancements for Release 19.2, page 470
- System and Platform Enhancements for Release 19.1, page 477
- System and Platform Enhancements for Release 19.0, page 478

System and Platform Enhancements for Release 19.6

This section identifies all of the system and platform enhancements included in this release:

Feature Changes – new or modified features or behavior changes. For details, refer to the System Administration Guide for this release.

Command Changes – changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Bounced Authentication Requests Cause Call Reject with Session Disconnect Reason 'Internal Error'

CSCvb65445 - Create Session Request failing with cause Session-setup-timeout

Applicable Products: ASR 5500
Feature Changes

Previous Behavior: On Authentication Request messenger bounce, call cleanup waited until setup timer expiry to reject the call with "Disconnect Reason: Session-setup-timeout."

New Behavior: As soon as Authentication Request messenger bounce occurs, gateway will initiate call reject with GGSN/P-GW cause of "EGTP_CAUSE_NO_RESOURCES_AVAILABLE." Session Disconnect Reason will show "internal error" for call clear.

Customer Impact: Increase of "internal error" under Session Disconnect Reason might be observed.

Diagnostics Added for Nameservice Issues When Tables on CPUs Are Suspected of Containing Missing Entries

CSCvb81644 - Namespace db missing certain aaamgr instances please add diagnostics to report it

Applicable Products: All

Feature Changes

Previous Behavior: When namespace db on a card is missing corresponding aaamgr instances, even when sessmgr instances are present, the Session Manager is unable to communicate with the AAA Manager and calls are dropped. Core file analysis was required to diagnose this problem.

New Behavior: The existing Exec mode CLI command `show support details` now provides the ability to diagnose nameservice issues when tables on CPUs are missing entries. Output similar to the following is shown:

```
MSGD Stats
------------
broadcast 5051527
broadcast read err 0
broadcast domain err 0
broadcast garbled 0
nscontrol 395
nscontrol read err 0
nscontrol garbled 0
sigchld 1
remove no entry 0

Nameservice table diff: card 1 cpu 0, card 1 cpu 0
+/~ Facility Instance
-----------------------------
Tables are identical.

Nameservice table diff: card 1 cpu 0, card 2 cpu 2
+/~ Facility Instance
-----------------------------
- aaamgr 1005546
+ aaamgr 1005547
- sessmgr 1005548
+ sessmgr 1005550
+ nscontrol 100
- nscontrol 200
```
System and Platform Enhancements for Release 19.3

This section identifies all of the system and platform enhancements included in this release:

**Feature Changes** – new or modified features or behavior changes. For details, refer to the *System Administration Guide* for this release.

**Command Changes** – changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

**Improving core transfer impact during SM recovery**

CSCuv79858 - Async Core Transfer and Proclet Recovery

**Applicable Products:** ASR 5000 and ASR 5500

**Feature Changes**

This feature maintains the transfer of the core dump to the management card while asynchronously beginning proclet (task) recovery which can reduce the total outage time.

**Command Changes**

```
crash enable async-core-transfer
```

A new `async-core-transfer` keyword has been added to the Global Configuration mode `crash enable` command. When enabled this keyword gives priority to proclet restart over crash core file transfer on the active MIO. This feature is enabled by default.

```
command
    [ no ] crash enable async-core-transfer
```

**Notes:**

- When a proclet crashes, a minimum 10% of the available total memory must be free in the CPU to start a new or rename the standby proclet.

**Increase number of SSH public keys**

CSCuw27070 - Support 200 ssh public keys in authorized key config

**Applicable Products:** All
Feature Changes

Previous Behavior: The maximum number of configurable authorized SSH keys was 64.

New Behavior: The maximum number of configurable authorized SSH keys is now 200.

If you downgrade to a lower StarOS version using a saved configuration file with 200 keys, that configuration file will be loaded, but only first 64 keys will be recognized. The remaining keys will be unavailable.

Inspector is not allowed to activate crypto-group

CSCux26797 - Inspector allowed to activate a crypto-group

Products: All

Feature Changes

Previous Behavior: Inspector level users could activate a crypto group with the Exec mode crypto-group command. An authenticated, remote attacker could issue unauthorized configuration commands from the Inspector privilege level.

New Behavior: Inspector level users can no longer execute the crypto-group command.

System and Platform Enhancements for Release 19.2

This section identifies all of the system and platform enhancements included in this release:

Feature Changes – new or modified features or behavior changes. For details, refer to the System Administration Guide for this release.

Command Changes – changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Chassis Key must be entered for a Chassis ID to be created

CSCur33704 - Change chassis key configuration management

Applicable Products: ASR 5000, ASR 5500

Feature Changes

Previous Behavior: Entering a chassis key was optional; the local MAC address was used to create a default chassis ID.

New Behavior: Beginning with this release, the user must explicitly set the chassis key through the Quick Setup Wizard or the chassis key value CLI command. If it is not set, a default chassis ID using the local MAC address will not be generated. In the absence of a chassis key (and hence the chassis ID), sensitive data will
not appear in a saved configuration file. Encryption and decryption of sensitive data in configuration files will not work.

In the absence of an existing chassis ID file the **chassis keycheck** command is hidden.

### CLI Confirmation for Specific Exec Mode Configuration Commands

CSCuv20394 - Confirmation Check on Selected CLI Commands

**Applicable Products:** All

#### Feature Changes

**Previous Behavior:** You can use the **autoconfirm** command to disable confirmation prompting for configuration commands. The **autoconfirm** command is available in the Exec mode and Global Configuration mode. Enabling the autoconfirm feature automatically supplies a "Yes" response to configuration command prompts, including for critical commands such as **reload** and **shutdown**. By default autoconfirm is disabled.

The **commandguard** command requires confirmation prompting for all configuration commands. The commandguard feature overrides the autoconfirm feature (if enabled).

The function of both of these commands has not changed.

**New Behavior:** A new keyword for the **commandguard** command allows you to apply mandatory prompting for specified categories of Exec mode configuration commands, even when autoconfirm is enabled.

#### Command Changes

**commandguard exec-command**

A new **exec-command** keyword allows you to apply mandatory confirmation prompting for specified categories of Exec mode configuration commands, even when autoconfirm is enabled.

```
configure
  [no] commandguard exec-command  exec_mode_category
end
```

Notes:

- **exec-command  exec_mode_category** specifies one of the following categories of Exec mode configuration commands.
  - card
  - clear
  - copy
  - debug
  - delete
  - filesystem
  - hd
• You can enter multiple `commandguard exec-command exec_mode_category` commands.

• All Exec mode commands beginning with the specified category word will prompt for confirmation, regardless if autoconfirm is enabled.

• You can turn off confirmation prompting for a specific category using `nocommandguard exec-command exec_mode_category`.

• If autoconfirm is overridden by `commandguard exec-command` for an Exec mode command, StarOS displays an informational message indicating why autoconfirm is being overridden when you attempt to execute the command.

• Users may selectively override confirmation prompting for any Exec mode configuration command that supports the `noconfirm` keyword.

Conceal/Remove ssh server Configuration Options

CSCur33698 - ANSSI REQ E2: Allow SSH config and remove weak SSH crypto algorithms

**Applicable Products:** All

**Feature Changes**

**Previous Behavior:** The SSH v1-RSA key was supported and available to configure within the Context Configuration mode.

**New Behavior:** Version 1 of the SSH protocol is now obsolete due to security vulnerabilities. The `v1-rsa` keyword is no longer supported. Running a script or configuration that uses the SSH v1-rsa key returns an error message and generates an event log. The output of the error message is shown below:

```
Failure: SSH V1 contains multiple structural vulnerabilities and is no longer considered secure. Therefore we don't support v1-rsa SSH key any longer, please generate a new v2-rsa key to replace this old one.
```

If the system boots from a configuration that contains the v1-rsa key, you can expect a boot failure when logging in through SSH. The workaround is to log in via the Console port, re-generate a new ssh v2-rsa key, and configure server sshd. It will then be possible to log in via ssh.

The `v1-rsa` keyword has been removed from the Exec mode `show ssh key` CLI command.
Command Changes

**Important**

A keyword that was supported in a previous release may be concealed in subsequent releases. StarOS continues to parse concealed keywords in existing scripts and configuration files created in a previous release. But the concealed keyword no longer appears in the command syntax for use in new scripts or configuration files. Entering a question mark (?) will not display a concealed keyword as part of the Help text. A removed keyword will return an error message when parsed.

### ssh

Removed the `v1-rsa` keyword and concealed the `v2-dsa` keyword for the Context Configuration mode `ssh generate` CLI command.

```plaintext
configure
c   context context_name
c      ssh generate key type v2-rsa
c   end
```

The `v2-dsa` keyword is removed in the `ssh generate key type` syntax and concealed in the `ssh key name length key_length type v2-rsa` syntax.

### ssh key-size

This new Global Configuration mode CLI command configures the key size for SSH key generation for all contexts (RSA host key only).

```plaintext
configure
c   ssh key-size { 2048 | 3072 | 4096 | 5120 | 6144 | 7168 | 9216 }
c   default ssh key-size 2048
c   end
```

Notes:

- **2048**: 2048 bits (Default)
- **3072**: 3072 bits
- **4096**: 4096 bits
- **5120**: 5210 bits
- **6144**: 6144 bits
- **7168**: 7168 bits
- **9216**: 9216 bits
ciphers

This new Global Configuration mode CLI command configures the cipher priority list in sshd for SSH symmetric encryption. It changes the cipher option in the sshd_config_x file for that context.

```
cipher
  context context_name
  server sshd
  ciphers algorithm
end
```

Notes:

- **ciphers** sets the priority order of encryption algorithms used for SSH symmetric session encryption.
- **algorithm** is entered as a single string of comma-separated variables in priority order from those shown below:

  * **blowfish-cbc** – symmetric-key block cipher, Cipher Block Chaining, CBC
  * **3des-cbc** – Triple Data Encryption Standard, CBC
  * **aes128-cbc** – Advanced Encryption Standard (AES), 128-bit key size, CBC
  * **aes128-ctr** – AES 128-bit key size, Counter-mode encryption (CTR)
  * **aes192-ctr** – AES 192-bit key size, CTR
  * **aes256-ctr** – AES 256-bit key size, CTR
  * **aes128-gcm@openssh.com** – AES 128-bit key size, Galois Counter Mode [GCM], OpenSSH
  * **aes256-gcm@openssh.com** – AES 256-bit key size, GCM, OpenSSH
  * **chacha20-poly1305@openssh.com** – ChaCha20 symmetric cipher, Poly1305 cryptographic Message Authentication Code [MAC], OpenSSH

---

**Only FSC Slots with Available HD Arrays Can Be Selected**

CSCuv23480 - RAID: CLI options for FSC cards must show only drives that are present

**Applicable Products:** ASR 5500

**Feature Changes**

- **Previous Behavior:** The HD RAID Configuration mode command allowed you to select an HD array for an FSC slot where the array was not available resulting in a system crash.
- **New Behavior:** The list of `hd<slot>` disk arrays will only include FSC slots for which an array is available.
Command Changes

hd raid

For the Exec mode `hd raid` keyword commands, only those `hd<slot>` arrays having an FSC slot number with available disks can be selected.
The `select` keyword has been removed from the list of available keywords.

hd-raid select

In the HD RAID Configuration mode, only those `hd<slot>` arrays having an FSC slot number with available disks can be selected.
The `select` keyword has been removed from the list of available keywords.

configure
  hd-raid
  keyword disk
  end

Remove obsolete-encryption Keyword in show configuration and save configuration Commands

CSCur33720 - ANSSI REQ E5: MUST remove obsolete-encryption

Applicable Products: All

Feature Changes

Previous Behavior: The CLI commands `show configuration` and `save configuration` supported an `obsolete-encryption` keyword.

New Behavior: The `obsolete-encryption` keyword has been removed. However, if a user tries to execute the `show configuration` and `save configuration` commands with the `obsolete-encryption` keyword, then it will still execute the command with a warning message instead of an error message.

Remove showsecrets Keyword in show configuration and save configuration Commands

CSCur33716 - ANSSI REQ E4: MUST remove showsecrets command

Applicable Products: All

Feature Changes

Previous Behavior: The `show configuration` and `save configuration` CLI commands supported a `showsecrets` keyword.
New Behavior: The showsecrets keyword has been removed. However, if a user tries to execute the show configuration and save configuration commands with the showsecrets keyword, then it will still execute the command with a warning message instead of an error message.

Resetting tech-support Password Now Requires Entry of Old Password

CSCur33730 - ANSSI REQ E6: MUST require knowledge of testmode password to change it

Applicable Products: All

Feature Changes

Previous Behavior: The tech-support test-commands password command always set the password to the newly entered value, regardless of the whether the password had been previously set.

New Behavior: The tech-support test-commands password command only succeeds if the password is not already set. A new keyword for this command allows the administrator to replace an existing password.

Also the Setup Wizard now supports configuring the tech-support password.

Command Changes

technology test-commands password

A new optional keyword allows an administrator to replace an existing password with a single command line:

configure
technology test-commands password new_password [ old-password old_password ]
end

Notes:

• new_password is the password you wish to configure. It has either never been previously set or is different from a previously configured password. It is an alphanumeric string of 1 to 64 characters.

• If the new_password replaces an existing password, you must enter the old password for the change to be accepted.

• If the old password is not entered or does not match the existing configured value, the following error message appears: "tech-support password is already configured". A prompt then appears to accept entry of the old_password: "Enter old tech-support password:".

• Entering old-password old_password allows you to replace the existing password without being prompted to enter the old password. If you incorrectly enter the old password or do not enter the old password, an error message appears: "Failure: Must enter matching old tech-support password to replace existing password".

• If technology test-commands password new_password old-password old_password is included in a script, the password will be changed as long as old_password is valid.
Quick Setup Wizard

The Quick Setup Wizard now prompts the user to enter the tech-support password.

setup
1. Do you wish to continue with the Quick Setup Wizard [yes/no]: yes
2. Enable basic configuration [yes/no]: yes
3. Change chassis key value [yes/no]: yes
4. New chassis key value: chassis_key
5. Create new tech-support password [yes/no]: yes
6. New tech-support password: new_password
7. local context administrator username [admin]: context_admin_username
8. local context administrator password: context_admin_password
9. confirm local context administrator password: context_admin_password
10. hostname [asr5500]: hostname

System and Platform Enhancements for Release 19.1

This section identifies all of the system and platform enhancements included in this release:

Feature Changes – new or modified features or behavior changes. For details, refer to the System Administration Guide for this release.

Command Changes – changes to any of the CLI command syntax. For details, refer to the Command Line Interface Reference for this release.

Performance Indicator Changes – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the Statistics and Counters Reference for this release.

Reload DDF device upon receipt of DDF FPGA EDCRC SEU event instead of initiating an unplanned DPC card migration

CSCu75183 - Fabric support for DPC DDF reload

Applicable Products: ASR 5500, DPC

Associated CDETS ID: CSCuu26497 - DPC1 got shutdown due to DDF_CRC_ERROR

Feature Changes

Previous Behavior: A DPC would be reset causing an unplanned migration after receiving a DDF_CRC_ERROR.

New Behavior: The DPC will not be reset and switched over after receiving a single DDF_CRC_ERROR. The DDF FPGA will automatically be reprogrammed to clear the error, thereby minimizing network impact and traffic loss.

Reprogramming of DDF FPGA on DPC to Reduce Outage Time

CSCu75183 - Fabric support for DPC DDF reload
Feature Changes

The Data Firmware (DDF) FPGA provides four DMA engines for data transfer between the CPU and the NPU on an ASR 5500 DPC. The size of the FPGA makes it susceptible to CRC errors which can result in a fatal error on the DPC that initiates a card switchover for recovery.

This solution reprograms the DDF FPGA when an Error Detection Cyclic Redundancy Check (EDCRC) error is detected. Reprogramming minimizes outage time and reduces the number of lost sessions. It also eliminates the need for a DPC switchover.

To speed the recovery process, the decompressed FPGA image is now stored in memory after the initial programing. The FPGA will be reprogrammed and have data traffic flowing within four seconds after a CRC error is detected by the FPGA.

System and Platform Enhancements for Release 19.0

This section identifies all of the system and platform enhancements included in this release:

**Feature Changes** – new or modified features or behavior changes. For details, refer to the *System Administration Guide* for this release.

**Command Changes** – changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

**Performance Indicator Changes** – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

Add bucket-intervals to Output of show session disconnect-reasons

CSCut02445 - Enhancement for show session disconnect reasons output

**Applicable Products:** P-GW, S-GW, SGSN

**Associated CDETS ID:** CSCus46885 - Provide support for non-blocking message pacing

**Feature Changes**

**Previous Behavior:** By default the output of the *show session disconnect-reasons* command displays only one bucket containing a cumulative count of disconnect reasons.

**New Behavior:** The operator can configure a bucket-interval (in minutes) to display historical, cumulative counts of disconnect reasons.

This feature is configured via a CLI command which sets a time interval value that is sent to all sessmgrs. Each sessmgr fills buckets with disconnect reason counts indexed by the time interval. The time interval for filling the buckets is indexed relative to time hh:00. For example: if the time interval is 5 minutes, the bucket is filled at hh:00, hh:05, hh:10, hh:15. So if current time is 06:57, buckets with values will be 06:55:00, 06:50:00 and 06:45:00.
A circular buffer method is used to fill the buckets. There are three buckets at all sessmgrs; each bucket is filled when the interval timer expires. The bucket that is currently filled is time dependent with a calculated index:

\[
\text{index} = \frac{(\text{CURRENT\_TIME}/\text{<CONFIGURED\_TIME>})}{3}
\]

Where CONFIGURED\_TIME is set via the session disconnect-reasons bucket-interval command (1-20 minutes). For example: if CONFIGURED\_TIME is 5 minutes and the current time is 06:00:00, all sessmgrs will fill a bucket at index \(\frac{0}{5}/3 = \text{index0}\) (first bucket). Similarly, at 06:05:00 and 06:10:00 the index will be \(\frac{5}{5}/3 = \text{second}\) (index1) and third (index2) buckets respectively.

**Figure 2: Interval-Index Bucket Relationships**

Whenever a sessmgr starts or restarts, the time for which the first bucket is filled is calculated as:

\[
\text{run\_timer\_for\_seconds} = \text{CONFIGURED\_TIME} - \frac{\text{CURRENT\_TIME}}{\text{CONFIGURED\_TIME}}
\]

The subsequent buckets are filled for CONFIGURED\_TIME.

For example, if the CLI is configured at 06:03:00 and CONFIGURED\_TIME is 5 then the first bucket is filled only for 2 minutes; the next timer starts at 06:05:00.
Also if a sessmgr instance goes down at 06:06:00 and restarts at 06:07:00, StarOS will fill its first bucket for 3 minutes only; the index of the bucket will be calculated as initially described.

Figure 3: Post Start/Restart - Interval-Index Bucket Relationships

Calculation of the index and timer value based on CURRENT_TIME helps with synchronizing all sessmgs. Following a reload or sessmgr process kill, bucket values are not preserved as is the case with disconnect-reasons.

Due to asynchronous events that bring the sessmgr at different times, it is possible that the buffers overlap in time across sessmgs. This leads to a ± x-minute discrepancy across sessmgs for the same statistics.

Command Changes

`session disconnect-reasons bucket-interval`

This new Global Configuration mode command specifies the bucket-interval (CONFIGURED_TIME) for displaying historical, cumulative disconnect reasons.

```plaintext
configure
  session disconnect-reasons bucket-interval interval_minutes
no session disconnect-reasons bucket-interval interval_minutes
end
```

Notes:

- `interval_minutes` specifies a bucket-interval in minutes as an integer from 1 through 20.

Performance Indicator Changes

`show configuration`

The following new field has been added to the output of this command:
show session disconnect-reasons

A new **buckets** keyword displays disconnect reasons in bucket interval columns.

If CONNECTION_TIME is recently configured and the first timer has not expired (no buckets are filled yet), "NA" is displayed in place of timestamps for those buckets which are not filled. "NA" also appears if the buckets have been cleared with the **clear session disconnect-reasons [buckets]** command.

clear session disconnect-reasons buckets

The **buckets** keyword has been added to clear **only** the contents of the three calculated interval buckets containing disconnect-reason statistics.

**ASR 5500 Egress Traffic Prioritization**

CSCuu11520 - ASR 5500 - Traffic prioritization through NPU egress port

**Applicable Products:** ASR 5500

**Feature Changes**

The ASR5500 uses several failure detection mechanisms to provide reliability across entities within the system. One of those mechanisms is the implementation of Bidirectional Forwarding Detection (BFD) protocol per each member link in a Link Aggregation Group (LAG). BFD is used to detect link failures and notify network layer protocols in a timely manner. A false positive due to BFD protocol packet loss is unacceptable and can trigger unnecessary network re-convergence. This could happen as a result of packet loss in a congested egress port due to overloaded user data and other control flows.

This new feature separates BFD packets from other packets and provides differential treatment via priority-based delivery. The Traffic Manager component of Network Processor Unit (NPU) guarantees packet delivery according to strict priority-based scheduling.

The BFD task running on the MIO card generates BFD packets and sends them towards the egress port. Each packet is constructed with an appropriate DSCP value of 0x30 (DSCP class CS6). The NPU on the MIO receives these packets over the internal switch fabric with a Midplane Encapsulation Header (MEH).

The NPU looks up the DSCP marking table and retrieves appropriate Internal Per Hob Behavior (IPHB) values matching the DSCP value in the BFD packet. This IPHB-COS value is used to determine one of eight queues into which the packet will be enqueued.

You must define the DSCP mapping table as required. If none is defined, a table of default values will be used to determine the queue. The default table values map all the DSCP values to an IPHB value of 0 (zero). Use the Global Configuration mode **qos ip-dscp-iphb-mapping dscp** command to configure the DSCP and L2 priority mapping table. The **show qos ip-dscp-iphb-mapping** command displays the current DSCP to IPHB mapping.

In the egress direction, the NPU receives the packet from the switch fabric with an MEH header. It parses the packet and determines the egress port to which the packet will be sent. Using this physical port information, two lookups are performed to determine the base flow-id (fid). The base flow-id is used to compute the actual flow-id to make the scheduling decision by TM.
The Traffic Manager (TM) component of the NPU makes WRED (Weighted Random Early Detection) calculations based on the queue number, WRED profile and color template for the queue. The packet is then admitted to the queue subject to hierarchical scheduling functions within the TM.

TM configuration is done statistically during MIO card/NPU initialization; there are no provisions to configure any TM related parameters via the StarOS CLI. The following commands are visible to customer for monitoring purposes:

- `show npu tm statistics [reset] slot/cpu/npu`
- `show npu tm queue slot/cpu/npu [mode { both | hex | text } ]`

### Performance Indicator Changes

**show npu tm**

This new `show` command displays statistics for the ASR 5500 Traffic Manager component of an NPU.

**show npu tm queue slot/cpu/npu [mode { both | hex | text } ]**

- PORT
- Pri
- TX Frames
- WRED Frames
- RED Bytes

**show npu tm statistics slot/cpu/npu [ reset ]**

- PORT
- COS
- Current Queue Depth (256B Buffers)

### Automatic Reset of FSC Fabric

CSCuo85356 - Reset FE devices when EGQ discard thresholds exceeded

**Applicable Products:** ASR 5500 only

### Feature Changes

**Previous Behavior:** If an excessive number of discarded fabric egress packets occurred in the switch fabric, a manual reset of the Fabric Storage Card(s) is required for fabric recovery.

**New Behavior:** A new CLI command allows an operator to enable automatic resets of FSCs if an excessive number of discarded fabric egress packets is detected.
Command Changes

fabric fsc-auto-recovery

This new Global Configuration mode command enables or disables automatic FSC resets upon detection of an excessive number of discarded fabric egress packets.

configure
fabric fsc-auto-recovery { disable | enable } | max-attempts | number_attempts | unlimited | ]
end

Notes:

• max-attempts | number_attempts | unlimited | specifies how many times StarOS will attempt to reset each FSC as an integer from 1 to 99 or unlimited (will not stop until FSC is reset). Default is 1.

Important
To enable this feature, you must first configure the Fabric Egress Drop Threshold via the Global Configuration mode fabric egress drop-threshold command.

Bulkstats to Track the Number of NEMO/Framed Routes and Total Routes per VRF

CSCuu54028 - Bulkstats to Track the Number of Routes per VRF

Applicable Products: All products

Feature Changes

With this release, a new Virtual Routing and Forwarding (VRF) schema has been added to track the number of NEMO/framed routes and total routes.

Performance Indicator Changes

vrf Schema

This new bulk statistics schema tracks the number of NEMO/framed routes and total routes per VRF.

• context
• vrf
• framed-routes
• total-routes
CLI Command to Track NEMO/Framed Routes and Total Routes per VRF

CSCuu54031 - Develop two new SNMP traps for routes per VRF

Feature Changes

When `threshold route-service vrf-framed-routes` is configured and the root level version of the CLI command is issued (without context and VRF information), the framed routes threshold value is configured for every VRF in the system. When `vrf-framed-routes` is issued for a specific context and VRF name, the threshold value is configured only for that context and VRF. The threshold values are set as a percentage of the ip maximum routes for the VRF. If ip maximum routes for a VRF is not configured, then the default value is the maximum routes per context.

When `threshold route-service vrf-total-routes` is configured and the root level version of the CLI command is issued (without context and VRF information), the total routes threshold value is configured for every VRF in the system. When `vrf-total-routes` is issued for a specific context and VRF name, the threshold value is configured only for that context and VRF. The threshold values are set as the total count of the routes in the VRF which includes pool routes, interface routes, static routes, dynamic routes and framed routes.

Customer Impact: This change will improve monitoring of NEMO/framed routes and total routes.

---

Important

For descriptions of the new alarms related to this CDETS ID, see the SNMP MIB Changes Release 19 chapter in the Release Change Reference.

---

Command Changes

`threshold route-service vrf-framed-routes`

A new `threshold route-service vrf-framed-routes` command is added to display the NEMO/framed routes per VRF.

```
configure
threshold route-service
vrf-framed-routes high_thresh [ clear low_thresh ] [ context context_name vrf vrf_name ]
end
```

Notes:

`vrf-framed-routes` specifies the threshold for percentage of VRF framed routes per VRF. It is an integer from 0 through 100.

- `high_thresh` specifies the high threshold rate percentage for VRF framed routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

- `clear low_thresh` configuresthe alarm clear threshold. It is an integer from 0 through 100. The default value is 0.

- `context context_name` is the context name where the vrf-framed-routes threshold will be applied.

- `vrf vrf_name` is the VRF name where the vrf-framed-routes threshold will be applied.
For more information on the maximum route value per context, refer to Engineering Rules in the System Administration Guide.

**threshold route-service vrf-total-routes**

A new `threshold route-service vrf-framed-routes` command is added to display the NEMO/total routes per VRF.

```plaintext
configure
  threshold route-service
  vrf-total-routes high_thresh [ clear low_thresh ] [ context context_name vrf vrf_name ]
end
```

Notes:

- `vrf-total-routes` specifies the number of VRF total routes threshold value per VRF. It is an integer from 0 through 65536.
  - `high_thresh` specifies the high threshold count of total routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 65536. A value of 0 disables the threshold. The default value is 0.
  - `clear` `low_thresh` configures the alarms clear threshold. It is an integer from 0 through 65536. The default is 0.
  - `context context_name` is the context name where the vrf-total-routes threshold will be applied.
  - `vrf vrf_name` is the VRF name where the vrf-total-routes threshold will be applied.

For more information on the maximum route value per context, refer to Engineering Rules in the System Administration Guide.

---

## Configuring a VPN Context for TACACS+ Authentication

CSCur50355 - TACACS client needs to support non-local context

**Applicable Products:** All

### Feature Changes

**Previous Behavior:** TACACS+ authentication was not supported for a non-local VPN context.

**New Behavior:** TACACS+ authentication is performed on non-local VPN context logins, if TACACS+ is configured and enabled.

**Customer Impact:** Customer may elect to use TACACS+ authentication for a non-local VPN context.

---

**Important**

This behavior change does not apply to users logging in through the local VPN context.
Command Changes

on-unknown-user

If TACACS+ is enabled with the on-unknown-user stop option, the VPN context name into which the user is attempting a login must match the VPN name specified in the username string. If the context name does not match, the login fails and exits out.

Without this option the login sequence will attempt to authenticate in another context via an alternative login method. For example, without the on-unknown-user stop configuration, an admin account could log into the local context via the non-local VPN context. However, with the on-unknown-user stop configuration, the local context login would not be attempted and the admin account login authentication would fail.

configure
tacacs mode
  on-unknown-user stop
end

Notes:

• stop forces the failed TACACS+ user to exit with attempting another login method.

Critical Alarm Generated for Call Reject at the Session Manager with Full Capacity

CSCut85988 - CriticalAlarm generate for call reject at SMGR with full capacity

Applicable Products: All

Feature Changes

Previous Behavior: A minor alarm was generated when the session manager capacity was full.

New Behavior: An SNMP trap is now generated when the session manager reaches full capacity.

ICSR Bulkstats in Standby Chassis Indicate Calls Lost During Switchover

CSCut76145 - VoLTE Bulkstats during SRP Switchover

Applicable Products: All products that support ICSR.

Feature Changes

Bulkstats have been added to the Standby chassis to indicate the number of calls lost during switchover. These new bulkstats complete work initiated for CSCuq10869 - ICSR: VoLTE ICSR Bulkstats Support (Release 18.2).
Performance Indicator Changes

csr Schema

The following new statistics have been added to this schema:

• total-num-volte-cap-subs-lost-first-fc-not-sent
• total-num-subs-engaged-voice-call-lost-first-fc-not-sent
• total-num-volte-cap-subs-purged-internal-audit
• total-num-subs-engaged-voice-call-purged-internal-audit

Improved Monitoring of NEMO Prefixes and Routes

CSCuu54042 - User Level CLI to show the NEMO/framed routes and total routes per VRF

Applicable Products: All Products

Feature Changes

Previous Behavior: Previously, there was no command to show framed/NEMO/framed routes and total routes per VRF and there was no count for framed routes in show ip route.

New Behavior: A new CLI command allows an operator to show framed-prefixes and enable filtering of framed-prefixes based on sess-id and/or vrf to the display.

Performance Indicator Changes

show ip framed-prefixes

This new Exec mode command displays the framed-prefixes along with session-id, vrf-name and pool-name. The command also displays the total number of framed-prefixes matching the filtering criteria.

show ip framed-prefixes [ sess-id session_identifier | vrf vrf_identifier ]
end

Notes:

• sess-id displays framed-prefixes added by a specific session. session_identifier must be an integer from 1 to 1152.

• vrf displays VRF specific routing information. vrf_identifier must be an alphanumeric string of 1 through 63 characters.

To display the show ip framed-prefixes statistics, the following new fields are added to the output of this command:

• session-id
• Address/Mask
LAG is Usable When a Minimum Number of Links are Available

CSCuu43618 - Min Links support

**Applicable Products:** ASR 5500 - Link Aggregation

**Feature Changes**

This min-link feature specifies that a Link Aggregation Group (LAG) is up (usable) only when a minimum number of links are available for aggregation. This guarantees that a minimum amount of bandwidth is available for use.

When this feature is enabled, a LAG is not usable when the number of links in a LAG goes below the configured min-link value. Switchover to another LAG bundle (if available) automatically occurs when the number of links in the current active bundle goes below the configured min-link value.

This feature is supported only on the ASR 5500.

**Command Changes**

**link-aggregation**

A new **min-link** keyword option has been added to this Global Configuration mode command.

```
configure
  port ethernet slot/port
  link-aggregation master { global | group } number
  min-link number_links
  end
```

**Notes:**

- **number_links** specifies the minimum number of links required to avoid a LAG switchover as an integer from 1 through 255.
Performance Indicator Changes

show configuration errors
If the configured min-link value is greater than the number of links in the LAG, an error is displayed in the output of this command. This error allows the operator to take corrective action by adding extra links to the LAG or reducing the min-link value.

show configuration link-aggregation group
The following new statistic is added to the output of this command:
  - min-link number_links

show configuration port
The following new statistic is added to the output of this command when the LAG master port number is specified:
  - min-link number_links

show link-aggregation info group
The following new statistic is added to the output of this command:
  - min-link

show link-aggregation table
The following new statistic is added to the output of this command:
  - LA# (link down due to min-link failure)

show port info
The following new statistic is added to the output of this command when the LAG master port number is specified:
  - (min_link)

show port table
The following new statistic is added to the output of this command:
  - LA# (link down due to min-link failure)
New Version of FSC with Single 400GB SSD

CSCut24782 - RAID support for new FSC with single 400GB SSD

Applicable Products: ASR 5500

Feature Changes

Previous Behavior: Fabric Storage Cards (FSCs) were equipped with two 200GB solid state drives (SSDs). The two drives were in a RAID 0 configuration supported under the RAID 5 configuration across all FSCs in the ASR 5500 chassis.

New Behavior: The 200GB SSDs are no longer available. A new version of the FSC is equipped with a single 400GB SSD in a non-RAID 0 configuration. This new drive configuration required changes to the underlying Linux configuration. Those changes are supported in this release. FCS-400GB cards can be mixed with FSC-200GB cards in an ASR 5500 chassis running this StarOS release.

For the FCS-400GB only one drive option is available for all hard drive-related show and debug commands.

Performance Indicator Changes

show card table

The output of this command now displays the new FCS-400GB as "Fabric & 1x400GB Storage Card".

show hd raid verbose

The output of this command now displays only one drive as part of its FSC card details for the FCS-400GB.

Non-blocking Message Pacing on Send Requests to Session Managers

CSCus46885 - Provide support for non-blocking message pacing

Applicable Products: All products supporting ICSR

Associated CDETS ID: and CSCuv62408 - Enhancement for show session disconnect reasons [Increase range]

Feature Changes

Previous Behavior: A single message could be outstanding for a targeted facility per CPU complex.

New Behavior: In this release, there can be two outstanding messages for a targeted facility per CPU complex.

Optimize Garbage Collection for Large Memory Block Arrays

CSCuq33856 - Optimize garbage collection for mblock allocators

Applicable Products: All
Feature Changes

**Previous Behavior:** Garbage Collection (GC) ran periodically for ten different memory block allocators using inefficient techniques.

**New Behavior:** GC code no longer uses large memset arrays and an idiv for every free node, increasing the performance of each GC pass by an order of magnitude.

**ping and ping6 Send Configurable DSCP Value with ICMP Request**

CSCuu45305 - Enhancement for Quality of Service (QoS) Ping

**Applicable Products:** All

Feature Changes

**Previous Behavior:** The Exec mode ping/ping6 request is sent with a default DSCP (0).

**New Behavior:** The ping/ping6 request can be sent with a configurable DSCP value.

Command Changes

**ping/ping6**

A new keyword for the Exec mode ping and ping6 commands allows the user to set a DSCP value that will be sent with the ICMP request.

The DSCP value is mapped to an internal-class-of-service value using the existing Global Configuration mode `qos ip-dscp-iphb-mapping` command.

```
configure
  ping dscp_value
  ping6 dscp_value
end
```

Notes:

- `dscp_value` is an integer from 0 through 63.

Performance Indicator Changes

**Output of ping/ping6**

The output of the ping/ping6 ICMP request will display the DSCP value (`dscp=<value>`).

**Reduction in Sync-Up Time with Standby ICSR Chassis**

CSCu76158 - Effective Standby Sessmgr Db recovery
Applicable Products: All products that support ICSR

Feature Changes

Previous Behavior: The default method for synchronizing the SRP database requires tens of seconds of delay whenever the TCP connection between the Active and Standby session managers is established. Once the TCP connection is established, heart beat messages are exchanged between both ICSR chassis every 3 seconds. The standby chassis waits for seven heartbeat messages from the active chassis before it is ready to accept data. This causes significant delay in session manager database synchronization on the standby chassis.

New Behavior: A new aggressive method for synchronizing the session manager database reduces recovery time in the following scenarios:

- Standby Session Manager failure
- Packet processing card failure on Standby chassis
- Standby chassis reboot
- Temporary loss and recovery of SRP connection

The aggressive method reduces the number of heartbeat messages and amount of housekeeping information exchanged between ICSR chassis.

Command Changes

standby database-recovery

This new SRP Configuration mode command allows you to select normal or aggressive restoration of the SRP database.

configure
  context context_name
  service-redundancy-protocol
  standby database-recovery { aggressive | normal }
end

Notes:

- The default form of this command restores the normal mode of SRP database recovery.

SaMOG-GW Now Supports ICSR

CSCug95464 - ICSR support on SaMOG GW

Applicable Products: ICSR on SaMOG GW

Feature Changes

The SaMOG (S2a Mobility over GTP) gateway application now supports ICSR configuration on ASR 5x00 and virtualized platforms.
StarOS Authorizations for TACACS+ Users

CSCuq86655 - TACACS+ commands not being logged or some commands missing

Applicable Products: All products

Feature Changes

Previous Behavior: StarOS administrative privilege levels for individual TACACS+ privilege levels were hard-coded.

New Behavior: StarOS administration levels, as well as specific access permissions and restrictions, can be configured for TACACS+ privilege levels and individual user IDs.

Command Changes

priv-lvl

This new TACACS+ Configuration mode command configures authorized StarOS privileges for a specified TACACS+ privilege level.

configure
tacacs mode
  priv-lvl lvl_number
  authorization-level { administrator | inspector | operator | security-admin } |
  cli | ecs | ftp | li-administration | nocli | noecs | noftp | nocli-administration 
end

Notes:

• lvl_number specifies the TACACS+ priv-level as an integer from 1 through 15.

• authorization-level specifies the StarOS administrative authorization level for this privilege level.
  • administrator – Allows user to execute Administrator level configuration commands.
  • inspector – Allows user to execute Inspector commands.
  • operator – Allows user to execute Operator commands.
  • security-admin – Allows user to execute Security Administrator commands.

• Optional permission and restrictions can also be associated with this TACACS+ priv-level.
  • cli – Permits access to the StarOS command line interface.
  • ecs – Permits access to Enhanced Charging Services (ECS) commands.
  • ftp – Permits of File Transfer Protocol (FTP).
  • li-administration – Permits access to Lawful Intercept (LI) administrative commands.
  • nocli – Denies access to the StarOS CLI.
  • noecs – Denies access to ECS commands
  • noftp – Denies use of FTP.
*nocli-administration* – Denies access to StarOS Administrator and Security Administrator commands.

For detailed information about StarOS administration levels, refer to the *System Settings* chapter of the *System Administration Guide*.

**user-id**

This new TACACS+ Configuration mode command configures additional profile attributes for a specific TACACS+ user identifier.

```plaintext
configure
tacacsmode
  user-id  tacacs_userid  [li-admin | noli-admin ]
end
```

Notes:

- *tacacs_userid* identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.
- *li-admin* grants access to Lawful Intercept (LI) administrative commands.
- *noli-admin* denies access to LI administrative commands.

**Performance Indicator Changes**

**show tacacs priv-lvl**

The *show tacacs* command has been modified to include a new *priv-lvl* keyword. This keyword displays TACACS+ priv-level authorization attributes.

**Support for LZ4 Compression Algorithm**

CSCum44718 - ICSR: Compression algorithm optimization

**Applicable Products:** All products that support ICSR

**Feature Changes**

**Previous Behavior:** Only zlib compression was supported for SRP messaging payload.

**New Behavior:** Support is now available for the LZ4 compression algorithm for SRP messaging payload. The zlib algorithm remains as the default.

LZ4 is a very fast lossless compression algorithm with near-linear scalability for multi-threaded applications.
Command Changes

checkpoint session compression

A new keyword has been added to the SRP Configuration mode `checkpoint session` command. The `compression` keyword allows the user to enable the use of the LZ4 compression algorithm.

Important  The `compression` keyword will only appear if a special ICSR optimization feature license has been purchased and installed. Contact your Cisco account representative for assistance.

```
configure
context context_name
  service-redundancy-protocol
    checkpoint session compression { lz4 | zlib }
    default checkpoint session compression
    no checkpoint session
end
```

Notes:

• LZ4 compression is effective only if both chassis are configured with LZ4. If any one chassis has zlib (default) configured, the compression algorithm reverts to zlib. The algorithm is negotiated only during initial socket establishment. Once agreed no more negotiation takes place until the TCP socket connection is reset.

• `default` reverts SRP to using the zlib compression algorithm.

Important  A change in the configured compression algorithm resets the TCP Link.

Performance Indicator Changes

show session subsystem facility sessmgr

This `show` command now provides information and statistics for the SRP compression algorithm used for geographic redundancy (ICSR).

• Geog Redundancy Compression Info
• Chkpoint Compression Supported: <lz4 or zlib>
• Chkpoint Compress Agreed: <lz4 or zlib>
• <lz4 or zlib> Compression Statistics:
  • CompSuccess
  • DeCompSuccess
  • CompFailure
Support for LZ4 Compression Algorithm

- DeCompFailure
- init
- deinit
- CompInbytes
- CompOutbytes
- DeCompInbytes
- DeCompOutbytes
- Compr ratio
VPC-DI Changes in Release 19

This chapter identifies features and functionality added to, modified for, or deprecated from VPC-DI in StarOS 19 software releases.

- VPC-DI Feature Changes for 19.1, page 497

VPC-DI Feature Changes for 19.1

This section identifies all of the VPC-DI enhancements included in this release:

- **Feature Changes** – new or modified features or behavior changes. For details, refer to the *VPC-DI System Administration Guide* for this release.

- **Command Changes** – changes to any of the CLI command syntax. For details, refer to the *Command Line Interface Reference* for this release.

- **Performance Indicator Changes** – new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the *Statistics and Counters Reference* for this release.

---

**Important**

For more information regarding features in this section, refer to the *VPC-DI System Administration Guide* for this release.

---

Scale up distribution of BFD sessions

CSCux05660 - Eliminate kernel source based routing

**Applicable Products:** VPC-DI

**Feature Changes**

VPC-DI now implements an npushm table containing multihost nexthops that vnpu/knpusim/npusim processes can access when a BFD packet requiring source-based routing is handled. BFDLC-generated control and echo
packets with multihost nexthops are then sent directly to the SF egress service port and not to the IP address pool driver on the SF demux card.

With this new functionality the number of layer 3 interfaces has been scaled up dramatically. Link level failures will be detected more quickly resulting in the prompt elimination of failing ports/cards from the data path.