# CONTENTS

## About this Guide

- Conventions Used ........................................... xxxiv
- Supported Documents and Resources ......................... xxxv
- Related Common Documentation .............................. xxxv
- Related Product Documentation ............................. xxxv
- Obtaining Documentation .................................. xxxvi
- Contacting Customer Support ................................. xxxvii

### AAA Changes in Release 17

AAA Enhancements for 17.5 ........................................ 39
- CSCuv64729 - Configurable CC values .......................... 40
  - Feature Changes ........................................... 40
- CSCuv94938 - SGSN-address and SGSN_Change event trigger for pgw/ggsn ... 41
  - Feature Changes ........................................... 41

AAA Enhancements for 17.3 ........................................ 42
- CSCus66465 - show diameter route status command causes high CPU utilization alarms ... 42
  - Feature Changes ........................................... 42
- CSCut26323 - Round-robin algorithm support for RADIUS mediation-device for hex IMSI ... 42
  - Feature Changes ........................................... 42
- CSCut26850 - Enhance multiple diameter peers to use same Host-name .......................... 43
  - Feature Changes ........................................... 43
  - Command Changes .......................................... 43

AAA Enhancements for 17.2 ........................................ 45
- CSCum90063 - Counters and Bulkstats for total-usage-report in PCC schema ................. 45
  - Performance Indicator Changes .............................. 45
- CSCur89572, CSCus36547, CSCur13994 - Diameter support for ................................. 45
  - Feature Changes ........................................... 45
- CSCus30296, CSCus30276 - [ePDG] Diameter changes for tunnel endpt ip support in SWm interface ... 45
  - Feature Changes ........................................... 46

AAA Enhancements for 17.1 ........................................ 47
- CSCtz79646, CSCuh67284 - PCSCF discovery - v4/v6 addresses not sent always for v4/v6 pdn req ... 47
  - Feature Changes ........................................... 47
- CSCud26703 - Enable / disable multiple back to back CCR-U from PGW/GGSN .......... 47
  - Feature Changes ........................................... 47
  - Command Changes .......................................... 47
  - Performance Indicator Changes .............................. 48
- CSCud65027 - EPC - CCR-U not sent after RAR received ............................................. 49
  - Feature Changes ........................................... 49
  - Feature Changes ........................................... 49
  - Command Changes .......................................... 50
- CSCuo72213 - RLF Feature qualification on S6b ..................................................... 50
  - Feature Changes ........................................... 50
- CSCup05517 - Gy Validity Timer to start on receipt of CCA in all cases ....................... 50
  - Feature Changes ........................................... 51
  - Command Changes .......................................... 51
- CSCup52642 - Restoration priority indicator avp is not ignored in 16.0 builds ............... 51
Feature Changes ................................................................. 51
CSCup75566 - MFL 2772- Add CC-Group AVP in Gx Dictionary .............................................. 51
Feature Changes ................................................................. 52
CSCug63995 - USAGE_REPORT compatibility handling with PCRF ........................................ 52
Feature Changes ................................................................. 52
Command Changes ................................................................. 52
CSCur26626 - [ePDG] Non UICC device support EAP-TLS/EAP-TTLS support Diameter changes 53
Feature Changes ................................................................. 53
CSCur27981 - T-bit not working for RF retried msg ................................................................. 53
Feature Changes ................................................................. 53
CSCur37593 - [ePDG] Missing AVPs in SWm standard dictionary .............................................. 53
Feature Changes ................................................................. 53
CSCur43509 - PCEF is not triggering 29 as APN-AMBR mod failure in CCR ................................ 54
Feature Changes ................................................................. 54
CSCur77837 - VoWiFi feature Selective Use of BEARER-USAGE for VoWiFi and VoLTE ............................................. 54
Feature Changes ................................................................. 54
AAA Enhancements for 17.0 ........................................................................................................ 55
CSCts30745 - [PDSN-VR0Gx] CCR-U sent twice when Gx asks for usage report for a mon key .... 55
Feature Changes ................................................................. 55
CSCtz97964 - PCSCF discovery - v4/v6 addresses not sent always for v4/v6 pdn req .......... 55
Feature Changes ................................................................. 55
CSCua99869, CSCue68175 - Radius policy (Firewall Policy) support in Gx ................................ 56
Feature Changes ................................................................. 56
CSCuf73716 - PI: The CLI ........................................................................................................ 56
Feature Changes ................................................................. 56
Command Changes ................................................................. 56
CSCuf82575 - [ePDG] Auth-Failure counter for epdg-service stats is not incrementing .... 57
Feature Changes ................................................................. 57
CSCug33751 - Host statistics not supported in DCCA ............................................................. 57
Feature Changes ................................................................. 57
Command Changes ................................................................. 57
CSCug58210 - RAT-TYPE should be 2003 for eHRPD in Gxa message ................................ 58
Feature Changes ................................................................. 58
CSCuh99978 - Implement COA rate limiting .............................................................................. 59
Feature Changes ................................................................. 59
CSCui12490 - Enhancement in RF Stats .................................................................................... 59
Feature Changes ................................................................. 59
Performance Indicator Changes ................................................................................................. 59
CSCui59026 - Enhancements in ASR5x00 Timer Implementation - Gy Changes ................... 61
Feature Changes ................................................................. 61
Command Changes ................................................................. 61
CSCui53808 - With OCS unreachable CCR-U includes unexpected AVP OTHER_QUOTA_TYPE 62
Feature Changes ................................................................. 62
CSCui34791 - full checkpoint to micro checkpoint conversion ................................................ 62
Feature Changes ................................................................. 62
CSCui56688, CSCum66195 - Need to support NAS-Port-Id in Access-Request ..................... 63
Feature Changes ................................................................. 63
Command Changes ................................................................. 63
CSCui26482 - Remaining-Service-Unit AVP not sent -FUI-Redirect and Granted units zero .... 64
Feature Changes ................................................................. 64
CSCui77461 - aaaproxy in warn state during customer call model run .................................... 64
Feature Changes ................................................................. 64
Command Changes ................................................................. 65
CSCum87917, CSCum70480, CSCum36649, CSCum36659, CSCum69764 - Support for Gx Sync after Session or Message Loss .................................................. 65
  Feature Changes .......................................................... 65
  Command Changes .......................................................... 66
  Performance Indicator Changes ......................................... 66
CSCum14422 - S6b: Support for 2014 4G S6b Spec .......................... 68
  Feature Changes .......................................................... 68
CSCum17342 - Support is not required for following AVP's in WLAN Rf message .......... 69
  Feature Changes .......................................................... 69
CSCum17434, CSCum14422,CSCum24018 - AAA provide Restoration Priority Indicator to PGW ... 69
  Feature Changes .......................................................... 69
CSCum36863 - Support webauth changes in Samog Radius dictionary .................. 69
  Feature Changes .......................................................... 69
  Command Changes .......................................................... 70
CSCum37008 - Radius based GTPv2 access support .......................... 70
  Feature Changes .......................................................... 70
CSCum41224 - Diameter Support for MME Node Restoration .................. 70
  Feature Changes .......................................................... 70
CSCum52650 - IMSA Support for Over ride Control feature .................. 71
  Feature Changes .......................................................... 71
CSCum54804 - STa support for webauth users ................................ 71
  Feature Changes .......................................................... 71
CSCum57172 - Radius messages should carry Framed-IPv6-Prefix in auth/acct requests ... 72
  Feature Changes .......................................................... 72
CSCum59592 - SLg Interface - Include MSISDN AVP in procedures ............... 72
  Feature Changes .......................................................... 72
CSCum65582 - Customer CDMA migration - PDSN Gy dictionary ................ 72
  Feature Changes .......................................................... 72
CSCum65600 - Diameter CCR-U reporting: tigger events based counters ......... 72
  Feature Changes .......................................................... 72
CSCum65709, CSCum67960 - Gy support for Accelerated ECS - Phase2 ............ 73
  Feature Changes .......................................................... 73
  Performance Indicator Changes ......................................... 73
CSCum67205 - [S6a/S6d] AVP support for MTC feature ........................ 73
  Feature Changes .......................................................... 73
CSCum67557 - PGW selection of Gx interface based on APN ........................ 73
  Feature Changes .......................................................... 74
CSCum67660 - Configurable dictionaries on Diameter interfaces ................. 74
  Feature Changes .......................................................... 74
CSCum69764 - CCR-u & CCR-f routing enhancement for Customer RDR ............. 74
  Feature Changes .......................................................... 74
CSCum75446, CSCum20550, CSCum36649, CSCum36659 - Support for FUA in Local Policy 75
  Feature Changes .......................................................... 75
  Command Changes .......................................................... 75
  Performance Indicator Changes ......................................... 76
CSCum76157, CSCum98934, CSCum36329, CSCum17342 - 2014 Customer Network Upgrade ... 76
  Feature Changes .......................................................... 76
  Performance Indicator Changes ......................................... 76
CSCum76162, CSCum65446, CSCum87983 - Rf and Gy checkpoint synchronization .......... 77
  Feature Changes .......................................................... 77
CSCum76201, CSCum65453 - Configurable Rf Containers triggered off of Gy events 78
  Feature Changes .......................................................... 78
  Command Changes .......................................................... 78
CSCum87203 - Customer CDMA - Gx dictionary on PDSN .......................... 79
### ADC Changes in Release 17

ADC Enhancements for 17.5

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>80</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>80</td>
</tr>
</tbody>
</table>

ADC Enhancements for 17.0

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>80</td>
</tr>
</tbody>
</table>

Support for Volume Reporting in Local Policy

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>81</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>81</td>
</tr>
</tbody>
</table>

Sending Rule report during reconnect to pcrf.

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>82</th>
</tr>
</thead>
</table>

Unreported usage should not be reported back to acs.

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>82</th>
</tr>
</thead>
</table>

Support for Session Rel Cause in all dictionaries.

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>82</th>
</tr>
</thead>
</table>

Bulkstats counter not present for CCR-Event Retry

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>83</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Indicator Changes</td>
<td>83</td>
</tr>
</tbody>
</table>

[g-n-gp] : 'user-equipement-info' AVP should be present in SIS RF records

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>83</th>
</tr>
</thead>
</table>

show ims-authorization policy-control statistics... show ip as 0.0.0.0

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>84</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>84</td>
</tr>
</tbody>
</table>

GY : Triggers not sent in CCR-U message

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>84</th>
</tr>
</thead>
</table>

Display support for some of dcca stat values

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>84</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Indicator Changes</td>
<td>84</td>
</tr>
</tbody>
</table>

RAA/ASA not received when OCS sends RAR/ASR for a Offline Session

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>85</th>
</tr>
</thead>
</table>

Support for sending Event Timestamp in CCR Initial

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>86</th>
</tr>
</thead>
</table>

Support for Volume Reporting in Local Policy

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>87</th>
</tr>
</thead>
</table>

### Release Change Reference, StarOS Release 17
ECS Changes in Release 17 ................................................................. 121

ECS Enhancements for 17.4 ................................................................. 122
CSCu82709 - Multiple failures after VPC-SI upgrade build 56341 -> build 57028 ................................................................. 122
Feature Changes ........................................................................... 122
CSCu43602 - Malformed Packet is passed from Gi to S5 without applying Quota of Gy ................................................................. 122
Feature Changes ........................................................................... 122
Performance Indicator Changes ....................................................... 123

ECS Enhancements for 17.3 ................................................................. 124
CSCue60917 - EDRs to include Rating Group and Service ID fields ................................................................. 124
Feature Changes ........................................................................... 124
Command Changes ........................................................................ 124
Performance Indicator Changes ....................................................... 125
CSCu91211 - Quota not requested in CCR-I when preemptively in CA set (dynamic-only) ................................................................. 125
Feature Changes ........................................................................... 125
CSCu80666 - Dis-engage TRM when a flow moves from one bearer to another ................................................................. 125
Feature Changes ........................................................................... 125
CSCu96377 - Reset Flow-Bearer mapping is missed in certain scenarios ................................................................. 126
Feature Changes ........................................................................... 126
ECS Enhancements for 17.2 ................................................................. 127
CSCus12168 - [ECSv2]: Pop-Up Notification use case .................................................................127
Feature Changes .......................................................................................................................127
Command Changes ....................................................................................................................127
Performance Indicator Changes ...............................................................................................127

CSCur65449 - Rule Inheritance: Show CLI should use subscriber level flag ................................128
Feature Changes .......................................................................................................................128

ECS Enhancements for 17.1 ........................................................................................................129

CSCui22770 - SFR - PSP algorithm modification ......................................................................129
Feature Changes .......................................................................................................................129
Command Changes ....................................................................................................................129
Performance Indicator Changes ...............................................................................................131

CSCuo23705 - per-rulebase bulkstats to show number of subscribers using that rulebase ..........131
Feature Changes .......................................................................................................................131
Performance Indicator Changes ...............................................................................................131

CSCuo68909 - TCP flows modification (RFC 1122, Section 4.2.2.13) .......................................132
Feature Changes .......................................................................................................................132
Command Changes ....................................................................................................................132
Performance Indicator Changes ...............................................................................................132

CSCup08420, CSCup49998, CSCur67850 - PGW (Gp) rejecting dynamic rule with Unknown Bearer ID cause .........................................................................................................................133
Feature Changes .......................................................................................................................133

CSCup30908 - Incl X-header for IPv4 Unique Identity with ..........................................................133
Feature Changes .......................................................................................................................133
Command Changes ....................................................................................................................133

CSCup31650 - Req29 - PCEF supervision-maintenance KPIs (phase 2) .......................................134
Feature Changes .......................................................................................................................134
Performance Indicator Changes ...............................................................................................134

CSCup48750 - [ECS] UDR enhancement to support NEMO MR Hosts ............................................134
Feature Changes .......................................................................................................................134
Command Changes ....................................................................................................................134
Performance Indicator Changes ...............................................................................................134

CSCuq30619 - active-charging cli need to be removed from ecs mode .......................................137
Feature Changes .......................................................................................................................137

CSCuq45238 - Different disconnect reason is required for PCRF unreachable case ....................137
Feature Changes .......................................................................................................................137

CSCur31337 - vrf-name attribute in EDR and UDR ...................................................................138
Feature Changes .......................................................................................................................138
Command Changes ....................................................................................................................138

CSCur47328 - PGW-CDR issues for WiFi calls & in LTE-WiFi & WiFi-LTE Handoffs ................139
Feature Changes .......................................................................................................................139

CSCur56899 - ECS rule matching wrong for app ......................................................................139
Feature Changes .......................................................................................................................139

ECS Enhancements for 17.0 .......................................................................................................140

CSCub32971 - GGSN/PGW support Customer's customized processing on Gy interface ............140
Feature Changes .......................................................................................................................140

CSCuf55484 - Support of ULI as X-header field in HE feature ..................................................140
Feature Changes .......................................................................................................................140

CSCuh60799 - Remove memory fair usage feature ....................................................................141
Feature Changes .......................................................................................................................141
Command Changes ....................................................................................................................141

CSCui88377 - Removal of Rule-deactivation-time not working .................................................142
Feature Changes .......................................................................................................................142

CSCuj14841, CSCum33077 - Flow Aware Packet Acceleration (FAPA) ....................................142
Feature Changes .......................................................................................................................142
Command Changes

Performance Indicator Changes

CSCum33088 - Simplification of retransmitted pkt charging Phase 2

Feature Changes

Command Changes

CSCum52646, CSCum52657, CSCum52650 - ECS Support for Override Control

Feature Changes

Command Changes

Performance Indicator Changes

CSCum52736 - Dual Factor Authentication – Radius Based (MPN)

Feature Changes

Command Changes

Performance Indicator Changes

CSCum59452, CSCum88067 - Enhanced DNS for IPv6 (MPN)

Feature Changes

CSCum62403 - Support of Simultaneous Create Bearer Request and Update Bearer Request

Feature Changes

CSCum67974 - Enhance CLI to display summary of active sessions per rulebase

Feature Changes

Performance Indicator Changes

CSCum79237, CSCum79229, CSCum85815 - ECS support for Configurable Micro Checkpoint Syncup Timer

Feature Changes

Command Changes

CSCum88267 - MVG: URL Based Readdressing

Feature Changes

Command Changes

Performance Indicator Changes

CSCum88678 - RF charging should be supported for flows accelerated by

Feature Changes

CSCum88705 - FDR/EDR should be supported in A-ECS

Feature Changes

CSCun17417 - Discontinue support for charge-volume variants except ip, constant

Feature Changes

Command Changes

CSCun81110 - Expand HTTP URL field in EDR from 256 to 2000+ characters

Feature Changes

Command Changes

Performance Indicator Changes

CSCun83874 - [A-ECS] Support post-processing rules in Accelerated Path

Feature Changes

CSCup28989 - PGW session mgr memory usage increased in 17.0

Feature Changes

CSCup48914 - wsp user-agent ends-with is not getting optimized

Feature Changes

CSCup73278 - Incorrect ruledef match for frag traffic with reassembly timeout

Feature Changes

CSCup86339 - Assert sessmgr_ipv4.c:10235 : sessmgr_ipv4_process_user_pkt_part2()

Feature Changes

CSCuq20248 - Fail planned switchover when OC batch processing is in progress

Feature Changes

CSCuq30728 - PGW:Assertion failure at process_bearer_binding_rsp

Feature Changes

CSCui50221 - P4: show active-charging service all prints ICMP w/out v4/v6 details

Release Change Reference, StarOS Release 17
ePDG Changes in Release 17 ................................................................. 159
  ePDG Enhancements for 17.2............................................................ 160
    CSCus30276, CSCus30296 - Support for tunnel endpt ip in SWm interface 160
    Feature Changes ........................................................................ 160
  ePDG Enhancements for 17.1............................................................ 161
    CSCur47221 - PGW reselection attempts to be made configurable .... 161
    Feature Changes ........................................................................ 161
    CSCub02436 - EMERGENCY PDN- ePDG ........................................ 162
    Feature Changes ........................................................................ 162
    CSCup8875 - [ePDG] Non UICC device support EAP-MSCHAPV2/EAP-TLS/EAP-TTLS support 162
    Feature Changes ........................................................................ 162
    CSCur03639 - [ePDG] P-CSCF IPv4 address support in ePDG .......... 162
    Feature Changes ........................................................................ 162
    CSCur47280 - ePDG need to set HO flag set when v4 IP addr is zero from UE 162
    Feature Changes ........................................................................ 162
  ePDG Enhancements for 17.0............................................................ 163
    CSCtz75077 - ASR5500 Support for ePDG ........................................ 163
    Feature Changes ........................................................................ 163
    CSCum39855 - [ePDG] - Support local configuration as preferred PGW selection mechanism 164
    Feature Changes ........................................................................ 164
    CSCum45189 - [ePDG] Crypto performance - Scale improvement on ASR5500 164
    Feature Changes ........................................................................ 164
    Command Changes ...................................................................... 164
    CSCum67523 - Initiate Session Checkpoint upon Session Creation. 164
    Feature Changes ........................................................................ 164
    CSCum84927 - [ePDG] - No need to retransmit the CSR if the prev resp parsing failed 165
    Feature Changes ........................................................................ 165
    CSCum87789 - Trap for failed Diameter or Radius peer success after XGW/PGW/HA/ePDG failover 165
    Feature Changes ........................................................................ 165
    CSCuo23369 - [ePDG]:Intelligent graceful PDN disconnection during maintenance-mode 165
    Feature Changes ........................................................................ 165
GGSN Changes in Release 17 ................................................................ 167
  GGSN Enhancements for 17.5 ............................................................ 168
    CSCzn47162 - Routing Behind the Mobile Station on an APN .......... 168
    Feature Changes ........................................................................ 168
    Command Changes ...................................................................... 169
    Performance Indicator Changes .................................................... 169
  GGSN Enhancements for 17.3 ............................................................ 170
    CSCus80195 - T3/N3 timer with 100 ms granularity ...................... 170
    Feature Changes ........................................................................ 170
    Command Changes ...................................................................... 171
    CSCus80582 - 3G call - All packets are dropped due to APN AMBR limiting 172
    Feature Changes ........................................................................ 172
    Command Changes ...................................................................... 172
  GGSN Enhancements for 17.1 ............................................................ 174
    CSCuh06473, CSCuq23971 - Cause IE enhancement for Delete Bearer Request 174
    Feature Changes ........................................................................ 174
    Command Changes ...................................................................... 175
    CSCuo89377 - Different Credit-Control Treatment at Gy for Out-roamers 178
    Feature Changes ........................................................................ 178
    Command Changes ...................................................................... 178
CSCup14481 - P-CSCF discovery mode on ggsn output can be made more transparent ........................................... 179
Feature Changes ........................................................................................................................................ 179
Performance Indicator Changes .............................................................................................................. 179
CSUp59406 - sesstrc task in over state during longevity/aggravator run ...................................................... 180
Feature Changes ........................................................................................................................................ 180
Command Changes .................................................................................................................................... 180
CSCuq35259 - [17.0 FCS]ARP value not in synch with ACS n SESSMGR for secondary bearer ............. 181
Feature Changes ........................................................................................................................................ 181
CSCR19546 - AccTermCause User_Request if session disconnect Invalid-source-IP-address .......... 181
Feature Changes ........................................................................................................................................ 181
GGSN Changes in Release 17.0 ................................................................................................................. 182
CSTr45924 - root privileges for ftp-user, no restriction to specific ftp-directory .................................. 182
Feature Changes ........................................................................................................................................ 182
CSCui40177 - GGSN to send micro chkpt for ue initiated and network initiated update ....................... 183
Feature Changes ........................................................................................................................................ 183
CSCui17195 - GTP echo and GTP message retry shall be configured separately ................................ 183
Feature Changes ........................................................................................................................................ 183
CSCum17169 - Per APN, and QCI, GTP-C v2 responses ........................................................................... 183
Feature Changes ........................................................................................................................................ 183
CSCum17370 - PDN session handling for Invalid IMEI & IMSI-less devices ............................................. 187
Feature Changes ........................................................................................................................................ 187
CSCum17389 - Dependency to support Per APN, and QCI, GTP-C v2 responses .................................. 187
Feature Changes ........................................................................................................................................ 187
CSCum17434 - AAA provide Restoration Priority Indicator to PGW ......................................................... 188
Feature Changes ........................................................................................................................................ 188
CSCum42664 - Bit Rate mapping across Gx and GTP based interfaces ...................................................... 189
Feature Changes ........................................................................................................................................ 189
CSCum51838 - GGSN Support for PCSCF Discovery ................................................................................. 190
Feature Changes ........................................................................................................................................ 190
CSCum56817 - Use of well-known APN for Customer-specific 4G subs .................................................... 190
Feature Changes ........................................................................................................................................ 190
CSCum66168 - DHCPv6: IPv6 default prefix AAA and Delegated Prefix Corelation .................................. 190
Feature Changes ........................................................................................................................................ 190
CSCum88464 - Intelligent graceful PDN disconnection during maintenance-mode .............................. 192
Feature Changes ........................................................................................................................................ 192
CSCum98092 - MS-to-MS traffic for Ipsec ............................................................................................... 193
Feature Changes ........................................................................................................................................ 193
CSCUm51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change .......... 194
Feature Changes ........................................................................................................................................ 194
CSCUm91294 - Inactivity timeout to be displayed under Session Release Reasons ........................... 194
Feature Changes ........................................................................................................................................ 194
CSCu77196 - NAS-Port-Id support on GGSN .......................................................................................... 194
Feature Changes ........................................................................................................................................ 194
CSCu95634 - P-CSCF Info (PCO IE) for Secondary Context/ Update PDP Rsp .......................................... 195
Feature Changes ........................................................................................................................................ 195
CSCu96798 - Counter type is not correct for all the variables of gtpc schema ........................................ 196
Feature Changes ........................................................................................................................................ 196
## GTPP Changes in Release 17

### GTPP Enhancements for 17.3

- CSCts50004, CSCum62796 - IPSG: EGCDR is not working with subscriber profile
- Command Changes

### GTPP Enhancements for 17.0

- CSCub32971 - GGSN/PGW support customer’s customized processing on Gy interface
- Feature Changes

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>Command Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCu73716 - PI: The CLI</td>
<td></td>
</tr>
<tr>
<td>CSCu25644 - Incorrect pdpType for a ipv4v6 call in GCDR</td>
<td></td>
</tr>
<tr>
<td>CStm25831 - PI: Accounting mode GTPP and gtppp group config should be shown in apn</td>
<td></td>
</tr>
<tr>
<td>CStm9328 - GTTP requests should be sent to any available CGF server in a group</td>
<td></td>
</tr>
<tr>
<td>CStm75381, CStm46390, CStm46415, CStm46585, CStm46276, CStm46607, CStm46305, CStm46287, CStm99212, CStm15607, CStm15880, CStm16109, CStm75689, CStm75713 - CDR module restructuring: Phase-II</td>
<td></td>
</tr>
<tr>
<td>CStm79565, CStm47539, CStm47494 - CDR support for including LAPI (signaling priority)</td>
<td></td>
</tr>
<tr>
<td>CStm85305 - sponsor ID should be populated in the PGW-CDR</td>
<td></td>
</tr>
<tr>
<td>CStm85499 - Support for LAPI bit in SCDR</td>
<td></td>
</tr>
<tr>
<td>CStm85810 - Support for LAPI bit in SGWCDR</td>
<td></td>
</tr>
<tr>
<td>CStm71456, CStm82539 - Diff order of support zone config causes stranded CDR stuck</td>
<td></td>
</tr>
<tr>
<td>CStm75702 - CDR module restructuring: Integration changes</td>
<td></td>
</tr>
<tr>
<td>CStm04619 - PGW-Gz CDR HDD: CGF parse shows few AVPs incorrect</td>
<td></td>
</tr>
<tr>
<td>CStm08800 - gtppp egcdr new-path cli</td>
<td></td>
</tr>
<tr>
<td>CStm52199 - cust21: incorrect encoding, tag 28 used for FCI and rATType</td>
<td></td>
</tr>
<tr>
<td>CStm21862 - Changing the default monpro to new routines from 17.0 onwards</td>
<td></td>
</tr>
</tbody>
</table>
L-ESS Enhancements for 17.0 ................................................................. 236
  CSCum67352 - L-ESS should support pushing and pulling of files from servers over IPV6 ..... 236
Feature Changes ............................................................................... 236
IPv6 support in L-ESS ......................................................................... 236

MME Changes in Release 17 ................................................................ 237
MME Enhancements for 17.7 ................................................................. 238
  CSCuv27053 - Purge-request towards only one HSS after sessmgr crash .................. 238
  Feature Changes ............................................................................ 238
  CSCux33388, CSCur41900 - CLI Control for Target Access Restriction ................. 239
  Feature Changes ............................................................................ 239
  Command Changes for the MME .................................................... 240
  Performance Indicator Changes .................................................... 241
MME Enhancements for 17.5 ................................................................. 243
  CSCui60043 - Changing MME dictionary for LUR - feature list ......................... 243
  Feature Changes ............................................................................ 243
  CSCuv45609 - MME Misbehaves while S1-HO-SGW-RELoc fails due to no response for MBreq. 244
  Feature Changes ............................................................................ 244
  CSCuv16974 - Cell Traffic Trace files to include eNodeBId eNodeBUeS1ApId ........... 244
  Feature Changes ............................................................................ 244
  Command Changes ........................................................................ 244
  Performance Indicator Changes .................................................... 245
  CSCuv68974 - EMM CC under CCP for SGS is incorrectly displaying as msi-unknown-in-hlr 245
  Feature Changes ............................................................................ 245
  Command Changes ........................................................................ 245
  Performance Indicator Changes .................................................... 246
  CSCuv73207 - MME not compliance with 3GPP 24.301 CR 2098 ......................... 246
  Feature Changes ............................................................................ 246
  Performance Indicator Changes .................................................... 246
  CSCuv87445 - During IRAT 3G to 4G iphone doesnt include APN, MME not req. apn from HS 247
  Feature Changes ............................................................................ 247
  CSCuv88869 - MME to drop repeated IDR from HSS ...................................... 247
  Feature Changes ............................................................................ 247
  CSCuv83605 - CSCuv96073 - Increase the hss-peer-service limit in MME to 64 .... 247
  Feature Changes ............................................................................ 247
  CSCuv21831 - MME Co location with SGSN in Pool Not Achieved .................... 248
  Feature Changes ............................................................................ 248
  Command Changes ........................................................................ 248
  CSCuv38345 - Deletion of Notify Messages in PGW-initiated Bearer Deactivation .... 249
  Feature Changes ............................................................................ 249
MME Enhancements for 17.4 ................................................................. 250
  CSCur41900 - TAU Reject with EMS Cause #15 mapping instead of #19 ................ 250
  Feature Changes ............................................................................ 250
  Performance Indicator Changes .................................................... 251
  CSCus24510 - MME support for EMERGENCY_CALL_RELEASE event in lcs service 251
  Feature Changes ............................................................................ 251
  CSCus32369, CSCuv68398 - wrong type of list TAI list IE sent in ATTACH/TAU Accept 252
  Feature Changes ............................................................................ 252
  Command Changes ........................................................................ 252
  CSCus57109 - MME Not Incrementing any Paging Stats for DDN Without EBI ...... 253
  Feature Changes ............................................................................ 253
  CSCus68029 - Configurable wait time value for ISDA reqd for state/location retrieval 253
  Feature Changes ............................................................................ 253
  Command Changes ........................................................................ 254
Performance Indicator Changes ............................................................... 254
CSCu29470 - Counter esm-msgtx-pdcon-rej not equal to the sum of all esm-ms 255
Performance Indicator Changes ............................................................... 255
CSCu48619 - MME Rejects UBR During a Handover Collision between S10-HO and X2-HO 256
Feature Changes .................................................................................. 256
CSCu51391 - Scaling support for Cell Tracing ......................................... 256
Feature Changes .................................................................................. 256
Command Changes ............................................................................... 257
template-session-trace ........................................................................ 258
Performance Indicator Changes ............................................................... 259
CSCu65408 - MME Write-Replace-Warning Request encoded incorrectly .... 259
Feature Changes .................................................................................. 259
CSCu67762 - Enforce license for MTC functionality ............................... 260
Feature Changes .................................................................................. 260
CSCu82559 - MME doesn't send Charging Characteristics in EGTP_CREATE_SESSION_REQUEST 260
Feature Changes .................................................................................. 260
CSCu85658 - Support serving node and handover event for emergency call in LCS 261
Feature Changes .................................................................................. 261
Command Changes ............................................................................... 261
CSCu85922 - Problem with DNS query for APN with 'gprs' anywhere in APN Name 262
Feature Changes .................................................................................. 262
CSCu88343 - Emergency PDN Connectivity Request Rejected by MME ...... 263
Feature Changes .................................................................................. 263
CSCu02890 - Enforce license for MTC functionality ................................ 263
Feature Changes .................................................................................. 263
CSCu1929 - Incorrect Feature-List Bit Set for S6a - ODB-all-OG .............. 263
Feature Changes .................................................................................. 263
CSCu41626 - Issues observed while compressing archived Cell Traffic trace files 264
Feature Changes .................................................................................. 264
MME Enhancements for 17.3 .................................................................. 265
CSCu24510 - MME support for EMERGENCY_CALL_RELEASE event in lcs service 265
Feature Changes .................................................................................. 265
CSCu34861 - MME is not using NAPTR with least preference first for MSC selection 266
Feature Changes .................................................................................. 266
Command Changes ............................................................................... 266
Performance Indicator Changes ............................................................... 266
CSCu18023 - MME standards violation - IDA without Supported-Features AVP 267
Feature Changes .................................................................................. 267
MME Enhancements for 17.2 .................................................................. 268
CSCt45571, CSCu25145, CSCu70096 - MME: eMBMS Support ............... 268
Feature Changes .................................................................................. 268
Performance Indicator Changes ............................................................... 269
CSCu56502 - SRVCC: Partial HO- providing voice services when SGSN is not responsive 269
Feature Changes .................................................................................. 269
Performance Indicator Changes ............................................................... 270
CSCu86490 - Include IMEI and IMSI in traceRecording element in Cell Traffic trace 270
Feature Changes .................................................................................. 270
CSCu88194 - New Reject cause needs to be added under Bearer Alloc Reject ESM message 270
Feature Changes .................................................................................. 270
Performance Indicator Changes ............................................................... 271
CSCu98725 - MME sessmgr task goes to over state when cell trace traffic is ON 271
Feature Changes .................................................................................. 271
CSCur19886 - Sessmgr crash sess/mme/mme-app/app/mme_egtp_fw.c:1014 271

Release Change Reference, StarOS Release 17
Feature Changes ................................................................. 271
CSCur50736 - PDN Connectivity Reject: Incorrect ESM cause#27 .................................................. 272
Feature Changes ................................................................. 272
Command Changes ............................................................... 272
Performance Indicator Changes ............................................ 273
CSCur97956, CSCum97512 - paging event causing failures (PSC3 only, DPC is not) ......................... 274
Feature Changes ................................................................. 274
Command Changes ............................................................... 274
CSCus00927 - S1 and SGs associations not equally distributed across mmemgr tasks ................. 275
Feature Changes ................................................................. 275
Command Changes ............................................................... 275
Performance Indicator Changes ............................................ 276
CSCus14148 - Dynamic Paging cache size allocation through CLI .............................................. 276
Feature Changes ................................................................. 276
Command Changes ............................................................... 277
CSCus16004 - MME rounds down max bitrate in VoLTE leading to packet loss ......................... 278
Feature Changes ................................................................. 278
CSCus36547, CSCur9572 - 'State/Location Information Retrieval' flag support in Feature-list AVP278 278
Feature Changes ................................................................. 278
Command Changes ............................................................... 279
Performance Indicator Changes ............................................ 280
CSCus36908 - MME recovered stats should be displayed with cumulative count ......................... 281
Feature Changes ................................................................. 281
CSCus50162 - QOS: Incorrect Reliability Class Mapping from QCI=5 ....................................... 282
Feature Changes ................................................................. 282
MME Enhancements for 17.1 ................................................................ 283
CSCup41525, CSCur94789, CSCur89174 - MME to support back up of counters and to be recovered after smgr rcvry ................................................................. 283
Feature Changes ................................................................. 283
Command Changes ............................................................... 284
Performance Indicator Changes ............................................ 285
CSCup59406 - sesstrc task in over state during longevity/aggravator run .................................. 288
Feature Changes ................................................................. 288
Command Changes ............................................................... 288
CSCup63874 - Increase the number of APN in remapping table ................................................. 289
Feature Changes ................................................................. 289
CSCup95642 - [QvPC-DI] unable to start GTPUMgr, insufficient unserved memory .................. 289
Feature Changes ................................................................. 289
CSCur38243 - MME discards EGTP_CREATE INDIRECT_DATA_FORWARDING_TUNNEL_RSP ............... 289
Feature Changes ................................................................. 289
MME Enhancements for 17.0 ................................................................ 291
CSCua06554 - MME sends update bearer response reject when collision with TAU ................. 291
Feature Changes ................................................................. 291
CSCub06751 - NASTAR Cell tracing .................................................................................. 292
Feature Changes ................................................................. 292
Command Changes ............................................................... 292
Performance Indicator Changes ............................................ 292
CSCuf59965, CSCum41122, CSCum55668 - Customized Inter-MME/SGW S1-Handover & TAU Procedure for PS-LTE Support ................................................................. 293
Feature Changes ................................................................. 293
Command Changes ............................................................... 293
Performance Indicator Changes ............................................ 295
CSCuh04641 - Timers for congestion conditions .................................................................. 295
Feature Changes ................................................................. 295
Command Changes

Performance Indicator Changes

CSCu07972 - Stats: Counting of failures where no REJECT or ACCEPT is send

Feature Changes

Performance Indicator Changes

CSCu17198 - [SGW] GTP echo and GTP message retry shall be configured separately

Feature Changes

Command Changes

Performance Indicator Changes

CSCu35622 - Ability to define same TAI in multiple TAI Lists

Feature Changes

Command Changes

Performance Indicator Changes

CSCu35642 - Improve ENB support from 32K to 64K

Feature Changes

CSCu35668 - Node Restoration: MME handling of PGW restart

Feature Changes

Command Changes

Performance Indicator Changes

CSCu37090, CSCuo78943, CSCuo78935, CSCuq60916 - MME needs to support MME Restoration Lite

Feature Changes

Command Changes

Performance Indicator Changes

CSCu37443, CSCum67205 - MTC Support : Subscribed periodic TAU times

Feature Changes

Command Changes

Performance Indicator Changes

CSCu37475 - MTC Support : Reject causes with MM & SM back-off time

Feature Changes

Command Changes

Performance Indicator Changes

CSCu68847, CSCum82648 - MME to support Network Provided Location Info (NPLI) for IMS

Feature Changes

CSCu88872 - TAU procedure counters incremented in wrong bucket

Feature Changes

CSCup02441 - IM exit procedure's failure counter not getting populated for scctp down

Feature Changes

CSCup49398 - IM_Exi1_Failure counter not pegged properly

Feature Changes

CSCup54025 - S1 and SGs associations not equally distributed across mmemgr tasks

Feature Changes

CSCup82616 - Handling display of Cell Trace logs and the Cell Trace config

Performance Indicator Changes

CSCup98586

Performance Indicator Changes

MVG Changes in Release 17

MVG Enhancements for 17.0

CSCtr17295 - [MVG-0500] - Policy-Link monitoring congestion trigger

Feature Changes

Command Changes

Performance Indicator Changes

CSCua96416 - Video : URL stripping

Feature Changes

Release Change Reference, StarOS Release 17
Command Changes ........................................................................................................... 332
Performance Indicator Changes ....................................................................................... 333
CSCum68267 - MVG: URL Based Readdressing ............................................................... 333
Feature Changes .............................................................................................................. 333
Command Changes ........................................................................................................ 333
Performance Indicator Changes ....................................................................................... 334

NAT Changes in Release 17 ............................................................................................ 337
NAT Enhancements for 17.0 ............................................................................................ 338
CSCuf30336 - fw-and-nat policy ID checkpointing to peer chassis ................................. 338
Feature Changes .............................................................................................................. 338
CSCuh60799 - Remove memory fair usage feature ......................................................... 338
Feature Changes .............................................................................................................. 338
CSCum39918 - KPI for NAT Port Chunk Blocking per Sub ........................................... 338
Feature Changes .............................................................................................................. 338
Command Changes ........................................................................................................ 339
Performance Indicator Changes ....................................................................................... 340
CSCum39930 - Pilot Packet to Multiple Destinations ...................................................... 341
Feature Changes .............................................................................................................. 341
CSCum39932 - Pilot Packet Statistics Enhancement ....................................................... 342
Feature Changes .............................................................................................................. 342
CSCum67985 - L3/L4 NAT to interwork with Accelerated ECS ...................................... 343
Feature Changes .............................................................................................................. 343

PDSN Changes in Release 17 ......................................................................................... 345
PDSN Enhancements for 17.1 .......................................................................................... 346
CSCup93612 - PDSN support for enhanced PPP Redirection .......................................... 346
Feature Changes .............................................................................................................. 346
Command Changes ........................................................................................................ 347
Performance Indicator Changes ....................................................................................... 347

P-GW Changes in Release 17 ......................................................................................... 349
P-GW Enhancements for 17.5 .......................................................................................... 350
CSCuv73563 - Support for SN1-QOS-Traffic-Policy AVP received from Radius server on PGW 350
Feature Changes .............................................................................................................. 350
Command Changes ........................................................................................................ 352
CSCzn47162 - Routing Behind the Mobile Station on an APN ....................................... 353
Feature Changes .............................................................................................................. 353
Command Changes ........................................................................................................ 353
Performance Indicator Changes ....................................................................................... 354
P-GW Enhancements for 17.4 .......................................................................................... 355
CSCus82761 - Charging Id in GTPv2 S2b/S2a ................................................................. 355
Feature Changes .............................................................................................................. 355
CSCut53373, CSCuu63751, CSCuu64308 - PGW initiates UBR while no QoS change ....... 356
Feature Changes .............................................................................................................. 356
Command Changes ........................................................................................................ 356
Performance Indicator Changes ....................................................................................... 357
CSCus03709 - Command <b>clear sub</b> with grep does not prompt for confirm .......... 357
Feature Changes .............................................................................................................. 357
Command Changes ........................................................................................................ 357
P-GW Enhancements for 17.3 .......................................................................................... 358
CSCus12585 - Bulkstat counter sessstat-bearrel-ded often zero when rel-dedbear is not ... 358
Feature Changes .............................................................................................................. 358
CSCus80195 - T3/N3 timer with 100 ms granularity ......................................................... 359
Feature Changes .............................................................................................................. 359
Command Changes ........................................................................................................... 359
CSCus82761 - Charging Id in GTPv2 S2b/S2a .................................................................. 361
Feature Changes .............................................................................................................. 361
CSCut22844 - SegFault: libc.so.6/__strlen_sse2_bsf() ................................................. 361
Feature Changes .............................................................................................................. 361
Command Changes ........................................................................................................ 361
CSCut38800 - PGW sends CCR-U with RESOURCES_LIMITATION for VoLTE calls in 17.1 build.362
Feature Changes .............................................................................................................. 362
CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure .............................................................................................................. 362
Feature Changes .............................................................................................................. 362
Command Changes ........................................................................................................ 362
P-GW Enhancements for 17.2 ......................................................................................... 364
CSCur22641 - QoS enforcement issue using GxR10 during IRAT on R15.0 PGW .......... 364
Feature Changes .............................................................................................................. 364
P-GW Enhancements for 17.1 ......................................................................................... 366
CSCug80236 - Cause code mapping difference in LTE/UMTS authorization-reject 5003 .. 366
Feature Changes .............................................................................................................. 366
CSCug96117 - Alternate Care-of Address Mobility Option support on PGW/LMA ......... 367
Feature Changes .............................................................................................................. 367
Command Changes ........................................................................................................ 367
Performance Indicator Changes ...................................................................................... 368
CSCuh06473, CSCuq23971 - Cause IE enhancement for Delete Bearer Request .......... 368
Feature Changes .............................................................................................................. 368
Command Changes ........................................................................................................ 369
CSCul30091 - PGW fails to resolve P-CSCF address ....................................................... 371
Feature Changes .............................................................................................................. 371
CSCum51840 - eHRPD support: PGW fails to resolve P-CSCF address ....................... 372
Feature Changes .............................................................................................................. 372
CSCum51844 - eHRPD Additional support for PCSCF Discovery ................................. 372
Feature Changes .............................................................................................................. 372
CSCuo51256 - Filter-ID Invalid name should not overwrite default ACL configuration .. 373
Feature Changes .............................................................................................................. 373
Command Changes ........................................................................................................ 373
Performance Indicator Changes ...................................................................................... 374
CSCuo92945 - 110 cause when temp fail not configured is treating as success ............ 374
Feature Changes .............................................................................................................. 374
CSCup44058 - Acct msg shows both v4 and v6 addr even if v4 is denied for static alloc . 375
Feature Changes .............................................................................................................. 375
CSCup44635 - SM support for CSCul22770, SFR - PSP algorithm modification ......... 375
Feature Changes .............................................................................................................. 375
CSCup59406 - sessstrc task in over state during longevity/aggravator run ................... 375
Feature Changes .............................................................................................................. 375
Command Changes ........................................................................................................ 376
CSCuq19244 - PGW doesn't initiate dns query to resolve p-cscf addr after ehrpd-epdg ho . 376
Feature Changes .............................................................................................................. 376
CSCuq63677 - Assertion failure at Function: sessmgr_sessstrcAllocate_clp_data() ....... 377
Feature Changes .............................................................................................................. 377
CSCuq98887 - pgw sends ICMP MTU too big when user pkt size is greater than 1500 .. 377
Feature Changes .............................................................................................................. 377
CSCur08331 - [17.1] P-CSCF discovery over GTP S2a via the APCO parameter in the CSR ......................................................................................................................... 377
Feature Changes .............................................................................................................. 377
CSCur15224 - [ePDG] PGW Support for IPv4 and IPv6 P-CSCF address in private extn IE ......................................................................................................................... 378
Feature Changes .............................................................................................................. 378
CSCur33479 - DCCA-GTP cause code APN access denied not working for PGW and GGSN .... 378

Release Change Reference, StarOS Release 17
Feature Changes ........................................................................................................ 378
CSCur1701 - Disconnect Reason Not Updated correctly For Saegw-collapsed call .......... 380
Feature Changes ........................................................................................................ 380
CSCur52706 - PGW/GGSN: Disc-reason Bulkstats verification reqd for CSCur33479 ... 380
Performance Indicator Changes .................................................................................. 380
CSCur47338 - [SysTest] audit-gtpmgr-failure CRR recovery failures observed .......... 380
Feature Changes ........................................................................................................ 380
CSCur74924 - DCCA-GTP cause code mapping not working for system-failure ...... 381
Performance Indicator Changes .................................................................................. 381
CSCur84831 - P-CSCF Discovery TO-BE Initiated S4-SGSN to LTE (and vice versa) Handoff ... 381
Feature Changes ........................................................................................................ 381
P-GW Enhancements for 17.0 ..................................................................................... 382
CSCug47563 - ASR5K LMA fails to assign client IP address using external DHCP Server 382
Feature Changes ........................................................................................................ 382
Command Changes ..................................................................................................... 383
CSCuh35078 - PGW responds to Create Session Request with Mandatory IE incorrect .. 383
Feature Changes ........................................................................................................ 383
CSCuh48881 - TCP support for DNS upon P-CSCF discovery .................................. 384
Feature Changes ........................................................................................................ 384
CSCui72349, CSCug75135 - PGW LORC mechanism for subscriber billing ................. 384
Feature Changes ........................................................................................................ 384
CSCum17169 - Per APN, and QCI, GTP-C v2 responses ........................................... 384
Feature Changes ........................................................................................................ 384
Command Changes ..................................................................................................... 385
Per APN, and QCI, GTP-C v2 responses ..................................................................... 385
Performance Indicator Changes .................................................................................. 385
CSCum17282 - VoLTE Retainability KPI ................................................................... 388
Feature Changes ........................................................................................................ 388
Performance Indicator Changes .................................................................................. 388
CSCum17389 - [17.0] EGTPC Dependency to support Per APN, and QCI, GTP-C v2 responses 389
Feature Changes ........................................................................................................ 389
CSCum17434 - [17.0] AAA provide Restoration Priority Indicator to PGW ................. 390
Feature Changes ........................................................................................................ 390
Command Changes ..................................................................................................... 390
Performance Indicator Changes .................................................................................. 390
CSCum17462 - PGW Support for PCSCF Recovery .................................................... 391
Feature Changes ........................................................................................................ 391
Performance Indicator Changes .................................................................................. 392
CSCum17490 - EGTPC Support - PGW Support for PCSCF Recovery ....................... 392
Feature Changes ........................................................................................................ 392
CSCum17693 - Rejecting non-emergency 9th network initiated DRB per UE ............. 392
Feature Changes ........................................................................................................ 392
CSCum41945, CSCum17370 - EGTPC - PDN session handling for Invalid IMEI & IMSI-less devices393
Feature Changes ........................................................................................................ 393
Performance Indicator Changes .................................................................................. 393
CSCum42664, CSCum41968, CSCum76157 - Bit Rate mapping across Gx and GTP based interfaces 393
Feature Changes ........................................................................................................ 393
Command Changes ..................................................................................................... 394
Performance Indicator Changes .................................................................................. 394
CSCum56817 - Use of well-known APN for customer-specific 4G subs ..................... 395
Feature Changes ........................................................................................................ 395
CSCum66168 - DHCPv6: IPv6 default prefix AAA and Delegated Prefix Corelation ... 395
Feature Changes ........................................................................................................ 395
PSF Enhancements for 17.0

CSCum88464, CSCup56698 - Intelligent graceful PDN disconnection during maintenance-mode 397
Feature Changes 397
Command Changes 397
Performance Indicator Changes 398
show session disconnect-reasons verbose 398

CSCun46475 - PGW is sending wrong S6b STR Termination Cause 398
Feature Changes 398
CSCun85038 - PGW/SAEGW - Network Provided Location Info (NPLI) for IMS [SM Support] 399
Feature Changes 399
CSCuo06912 - PGW call fails if Framed-Pool enforced from radius 399
Feature Changes 399
CSCuo11336 - Update bearer Request not triggered on FUA action from Gy 400
Feature Changes 400
CSCuo38762 - congestion-control threshold related CLI not visible in show config 400
Feature Changes 400
CSCuo90006 - Formulation of P-CSCF Address Output as part of show sub full all 400
Feature Changes 400
CSCup27196 - License for 17.0 401
Feature Changes 401
CSCup54622 - CLI equivalent for these bulkstats variables of egtpc schema 401
Feature Changes 401
Performance Indicator Changes 401
CSCup60931 - [17.0] PGW should not send UBR after PCSCF recovery MBR on emergency APN 402
Feature Changes 402
CSCup89213 - Incorrect cause-code in DB Req for PCRF initiated session termination 403
Feature Changes 403
CSCuq19244 - PGW doesnt initiate dns query to resolve p-cscf addr after ehrpd-epdg ho 403
Feature Changes 403
CSCuq50437 - absolute timer truncated on MSB causing premature disconnects 404
Feature Changes 404

PSF Changes in Release 17

PSF Enhancements for 17.1

CSCup77724 - Pkts not reaching isp when junk policy configured for uplink protection 406
Feature Changes 406

PSF Enhancements for 17.0

CSCuc83562 - [SFW] Need a way to make PPTP work without PPTP Analyser 407
Feature Changes 407
CSCue68175, CSCua99869 - Firewall changes for Radius policy support in Gx 407
Feature Changes 407
CSCuf30336 - fw-and-nat policy ID checkpointing to peer chassis 408
Feature Changes 408
CSCug91538, CSCug91568 - Move sfw/nat info to 'show active-charging subscribers ...' 408
Feature Changes 408
Performance Indicator Changes 408
CSCuh60799 - Remove memory fair usage feature 409
Feature Changes 409
CSCul71133 - Merge all the uplink firewall feature enabling to single CLI 409
Feature Changes 409
CSCum02425 - Total DOS Attacks counter not to be updated for NAT only enabled 410
Contents

SAEGW Changes in Release 17 ........................................... 411
SAEGW Enhancements for 17.5 ........................................... 412
SAEGW Enhancements for 17.4 ........................................... 413
CSCuu31324 - Idle subscribers not being cleared from SPGW ........................................... 413
  Idle Subscribers Cleared Properly ........................................... 413
SAEGW Enhancements for 17.3 ........................................... 414
CSCuu31324 - Idle subscribers not being cleared from SPGW ........................................... 414
  Feature Changes ........................................... 414
SAEGW Enhancements for 17.3 ........................................... 415
CSCuu31324 - Idle subscribers not being cleared from SPGW ........................................... 415
  Feature Changes ........................................... 415
CSCuu37427 - Assertion failure egtpc_handle_create_sess_req_msg_at_sgw_ingress ........................................... 416
  Feature Changes ........................................... 416
SAEGW Enhancements for 17.2 ........................................... 417
CSCur22641 - QoS Enforcement Issue using GxR10 During IRAT ........................................... 417
  Feature Changes ........................................... 417
CSCur61470 - S2B Support on SAE-GW ........................................... 418
  Feature Changes ........................................... 418
  Performance Indicator Changes ........................................... 419
SAEGW Enhancements for 17.1 ........................................... 421
CSCuh06473, CSCui42763, CSCuq23971 - Cause IE enhancement for Delete Bearer Request ........................................... 421
  Feature Changes ........................................... 421
  Command Changes ........................................... 422
CSCup59406 - sesstrc task in over state during longevity/aggravator run ........................................... 424
  Feature Changes ........................................... 424
  Command Changes ........................................... 425
CSCur43509 - 17.1: MLF-3298: PCEF is not triggering 29 as APN-AMBR mod failure in CCR ........................................... 425
  Feature Changes ........................................... 425
SAEGW Enhancements for 17.0 ........................................... 426
CSCuh24813 - InTracer Support: Auto and more simultaneous traces - SAEGW ........................................... 426
  Feature Changes ........................................... 426
CSCum17434 - AAA provide Restoration Priority Indicator to PGW ........................................... 427
  Feature Changes ........................................... 427
  Performance Indicator Changes ........................................... 427
CSCum93697 - Per QCI data stats for collocated S&P calls ........................................... 428
  Feature Changes ........................................... 428
  Performance Indicator Changes ........................................... 428
CSCun86828 - CBR - MBR collision causing MME to delete dedicated bearer ........................................... 435
  Feature Changes ........................................... 435
CSCuo90006 - Formulation of P-CSCF Address Output as part of show sub full all ........................................... 435
  Feature Changes ........................................... 435
CSCup89193 - SGW Access peer profile should be reflected in show output ........................................... 436
  Feature Changes ........................................... 436
CSCup97222 - Wrong Termination-Cause sent in CCR over Gx for ims default bearer ........................................... 436
  Feature Changes ........................................... 436
  Performance Indicator Changes ........................................... 436
CSCuq46858 - NPLI: UBReq not triggered by PGW, when PCRF requests for ULI in RAR ........................................... 436
  Feature Changes ........................................... 436

SaMOG Changes in Release 17 ........................................... 439
SaMOG Enhancements for 17.0 ........................................... 440
### SecGW Changes in Release 17

**SecGW Changes in Release 17**

Feature Changes
Command Changes
Performance Indicator Changes

#### CSCu60305, CSCup63789 - Pseudonym/Fast reauth NAI support on SaMOG

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>440</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>440</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>441</td>
</tr>
</tbody>
</table>

#### CSCum95466, CSCum36863, CSCum36878, CSCum42124, CSCup84932 - Support Webauth on SaMOG GW

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>442</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>442</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>445</td>
</tr>
</tbody>
</table>

#### CSCum35258 - AAA protocol agnostic GTP version support

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>447</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>447</td>
</tr>
</tbody>
</table>

#### CSCum35265 - Prepaid subscriber and Voucher support for LBO

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>448</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>448</td>
</tr>
</tbody>
</table>

#### CSCum36839 - APN Local breakout support under SaMOG-3G license

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>448</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>449</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>449</td>
</tr>
</tbody>
</table>

#### CSCum42089 - Support for PGW fallback

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>449</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>450</td>
</tr>
</tbody>
</table>

#### CSCum79992 - Session disconnect reason needs to be changed for SSID change

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>450</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>450</td>
</tr>
</tbody>
</table>

#### CSCum58418 - [SAMOG] Flexibility to config to egress-egtp from diff context under CGW

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>450</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>450</td>
</tr>
</tbody>
</table>

#### CSCup81813 - [SAMOG] ‘Unsupported NAI’ in EAP pkt should be changed to ‘Unknown NAI’

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>451</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>451</td>
</tr>
</tbody>
</table>

### SecGW Changes for 17.1

**SecGW Enhancements for 17.1**

Feature Changes

#### CSCui46785 - Need to target 40Gbps throughput performance for WSG on VSM SSI

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>454</th>
</tr>
</thead>
</table>

### SecGW Changes for 17.0

**SecGW Enhancements for 17.0**

Feature Changes

#### CSCtt22271 - RFC 4303 ESN

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>456</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>456</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>457</td>
</tr>
</tbody>
</table>

#### CSUh37234 - Layer 3 based High Availability

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>458</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>458</td>
</tr>
<tr>
<td>Command Changes - Reverse Route Injection</td>
<td>458</td>
</tr>
<tr>
<td>Command Changes - Anchor Route Configuration</td>
<td>460</td>
</tr>
<tr>
<td>Command Changes - HSRP</td>
<td>460</td>
</tr>
</tbody>
</table>

#### CSCum19793 - WSG as IKEv2 Initiator

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>460</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>461</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>462</td>
</tr>
</tbody>
</table>

#### CSCum81454 - CLI to support Allow one tunnel per remote IKE_ID feature

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>463</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>463</td>
</tr>
</tbody>
</table>

#### CScu07192 - SecGW - Supporting TLS for Connectedapp

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>464</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Changes</td>
<td>463</td>
</tr>
</tbody>
</table>

#### CSCup53154 - Upgrade oneP package to rel7 / dev7 which supports CSS

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>464</th>
</tr>
</thead>
</table>

#### CSCup72627 - snmp mib CLI enabling/disabling snmp tunnel stats retrieving

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>464</th>
</tr>
</thead>
</table>
SGSN Changes in Release 17

SGSN Enhancements for 17.7
- CSCuq63874
  - Feature Changes
- CSCuq37542
  - Feature Changes
- CSCty74246
  - Feature Changes
- CSCus06673
  - Feature Changes
- CSCuu74352
  - Feature Changes
- CSCuu59020
  - Feature Changes
- CSCus64306
  - Feature Changes
- CSCuv92478
  - Feature Changes
- CSCux33388, CSCur41900
  - CLI Control for Target Access Restriction
  - Feature Changes
- CSCus74248
  - Feature Changes
- CSCup81922
  - Feature Changes

SGSN Enhancements for 17.4
- CSCur1900 - TAU Reject with EMS Cause #15 mapping instead of #19
  - Feature Changes
- CSCus64306 - SGSN cannot reject RAU with MNC/MCC that arrive in HEX
  - Feature Changes
- CSCus91182 - UPCQ Need Not be Sent With DT in Certain Scenarios to Modify MS INIT
  - Feature Changes
- CSCus59020 - RAB Assignment Request sent with Alternate RAB param without RAB param
  - Feature Changes
- CSCuu74352 - No rab release during upc/dpc collision
  - Feature Changes
- CSCup02890 - Enforce license for MTC functionality
  - Feature Changes

SGSN Enhancements for 17.2
- CSCus06673 - RAB Setup Fails with cause invalid-rab-parameters-combination
  - Feature Changes
- CSCus50162 - QOS : Incorrect Reliability Class Mapping from QCI=5
  - Feature Changes

SGSN Enhancements for 17.1
- CSCup92045 - Need Linkmgr CPU added to bulkstats for SGSN cpty monitoring
  - Feature Changes
- CSCty74246 - SNMP trap when generated does not include the Restart count
  - Feature Changes
- CSCup97718 - SGSN should modify MR timer value based on backoff timer value.
  - Feature Changes
- CSCup37542 - Assertion failure at sess/sgsn/sgsn-app/pmm_pmm_fsm.c:6829
  - Feature Changes
- CSCup63874 - Increase the number of APN in remapping table
  - Feature Changes
SGSN Enhancements for 17.0

CSCue95642 - [QvPC-DI] unable to start GTPUMgr, insufficient unserved memory
Feature Changes

CSCur94789 - CLI 'statistics-backup sgsn mme backup-int 1' not applied
Command Changes

CSCts49833, CSCua43669, CSCuj06794 - Location reporting in Connected mode for S4 SGSN
Feature Changes

CSCus82739 - LORC feature shall be supported over S4 interface
Command Changes

CSCty44479 - APN Restriction on S4-SGSN
Feature Changes
Command Changes

CSCty82285 - Increasing Lawful interception capacity on SGSN
Feature Changes

CSCut09826 - Need a cli to control ‘Release Access Bearers Request’
Feature Changes

CSCud63677, CSCui21269, CSCuh77293 - SM application changes for PGW restart notification
Feature Changes

CSCuh75222 - SGSN to display number of HSPA subscribers
Feature Changes

CSCuh89000 - S6d/Gr interface selection based on UE capability
Feature Changes

CSCu88489 - Enhancement for SGSN behavior with RAU response
Feature Changes

CSCu17198, CSCui17195 - GTP echo and GTP message retry number shall be configured separately
Feature Changes

CSCui29734 - Support of pooled and non-pooled RNCs/BSCs
Feature Changes

CSCui86798 - SGSN per RA level stats
Feature Changes

CSCum14414 - Inconsistency seen when Deactivate sent with and without tear down
Feature Changes

CSCum47774, CSCum50056 - M2M Features to be supported by SGSN
Feature Changes

Contents
Performance Indicator Changes ................................................................. 518
CSCum62444 - SGSN to backup counters and recover them after session manager crash ... 518
Feature Changes ................................................................................... 518
Command Changes ................................................................................ 519
Performance Indicator Changes ................................................................. 521
CSCum67205, CSCup61646 - S6d AVP support for MTC feature ......................... 551
Feature Changes ................................................................................... 551
Command Changes ................................................................................ 551
CSCuo54664 - Port 21/1 reported errors, LMI down ........................................ 553
Feature Changes ................................................................................... 553
Command Changes ................................................................................ 554
CSCuo88086 - Update Location Answer with 36 EPS and 36 GPRS subscription fails ... 554
Feature Changes ................................................................................... 554
CSCuo92276 - Support for "Subscribed Periodic TAU/RAU Timer withdrawn" in MAP DSD ... 554
Feature Changes ................................................................................... 554
CSCup06636 - UE cap in ctxt rsp,gtp ident rsp to be used for interface selection .......... 555
Feature Changes ................................................................................... 555
CSCup11529 - Statistics and bulkstats support for MTC .................................... 555
Feature Changes ................................................................................... 555
Performance Indicator Changes ................................................................. 555
CSCup39995 - Reduce the number of SF failures to trigger CARD reboot .............. 561
Feature Changes ................................................................................... 561
CSCup46980 - SGSN not sending the Equipment status in show subscriber output ....... 561
Feature Changes ................................................................................... 561
Performance Indicator Changes ................................................................. 561
CSCup71741 - Congestion-Control: SM stats implementation required with LAPI .... 562
Performance Indicator Changes ................................................................. 562
CSCup79825 - Unexpected Data Value stats not pegged when check_imei_resp as UDV ... 562
Feature Changes ................................................................................... 562
Performance Indicator Changes ................................................................. 563
CSCup82824 - New disconnect reason for MM APN based congestion control .......... 563
Feature Changes ................................................................................... 563
CSCup99278 - Support for supported features negotiation with HSS is required ....... 563
Feature Changes ................................................................................... 563
CSCzn37980 - S4 SGSN functionality to be implemented .................................... 564
Feature Change .................................................................................... 564
Command Changes ................................................................................ 564

S-GW Changes in Release 17 .......................................................................... 565
S-GW Enhancements for 17.5 ...................................................................... 566
S-GW Enhancements for 17.4 ...................................................................... 567
CSCut14324 - SGW sending PDP Reject with No resources on 3G Attach dual Bearer ... 567
Feature Changes ................................................................................... 567
CSCuu37427, CSCut14324 - Assertion failure egtpc_handle_create_sess_req_msg_at_sgw_ingress ... 568
Feature Changes ................................................................................... 568
S-GW Enhancements for 17.3 ...................................................................... 569
CSCut14324 - SGW sending PDP Reject with No resources on 3G Attach dual Bearer ... 569
Feature Changes ................................................................................... 569
S-GW Enhancements for 17.2 ...................................................................... 570
S-GW Enhancements for 17.1 ...................................................................... 571
CSCum88408, CSCum93286 - Separate Paging for IMS Service Inspection ............ 571
Feature Changes ................................................................................... 571
Command Changes ................................................................................ 572
associate sgw-paging-profile three-tuple ................................................... 573
CSCup59406 - sesstrc task in over state during longevity/aggravator run ............... 573
Feature Changes .......................................................... 573
Command Changes ........................................................ 573
CSCu53899 - Instance 5 should be sent in UL IDFT rsp from s.sgw to s.mme ................. 574
Feature Changes ........................................................ 574
S-GW Enhancements for 17.0 ............................................... 575
CSCue35977 - EGTPC MME restoration support at SGW ........................................... 575
Feature Changes ........................................................ 575
Command Changes ........................................................ 575
CSCuh34589 - MME restoration support at S-GW .................................................... 576
Feature Changes ........................................................ 576
Command Changes ........................................................ 577
Performance Indicator Changes ........................................... 579
CSCul04397 - Network Provided Location Info (NPLI) for IMS .................................. 582
Feature Changes ........................................................ 582
CSCul17198 - [SGW] GTP echo and GTP message retry shall be configured separately .... 583
Feature Changes ........................................................ 583
Command Changes ........................................................ 583
Performance Indicator Changes ........................................... 584
CSCum61765 - [17.0] SGW support for PCSCF Discovery ............................................. 584
Feature Changes ........................................................ 584
CSCum65507, CSCum88401 - Support DDN Profile at SGW ....................................... 585
Feature Changes ........................................................ 585
CSCum79565 - MTC-Feature: CDR support for including LAP1 (signaling priority) ........ 589
Feature Changes ........................................................ 589
CSCum88387 - Graceful PDN Shutdown ............................................................... 589
Feature Changes ........................................................ 589
CSCum88401, CSCum65507 - Packet drop timer for Volte bearer .................................. 589
Feature Changes ........................................................ 589
CSCup42450 - SGW TRAFPOL:counters for default bearer aren't getting updt ............... 590
Feature Changes ........................................................ 590
CSCuq55963 - SGW ISR paging is not initiated for bearer activation for ISR sesion ........... 590
Feature Changes ........................................................ 590

SNMP MIB Changes in Release 17 ........................................................................ 591
SNMP MIB Object Changes for 17.5 ......................................................... 592
New SNMP MIB Objects .............................................................................. 592
Modified SNMP MIB Objects ................................................................. 592
Deprecated SNMP MIB Objects .............................................................. 592
SNMP MIB Alarm Changes for 17.5 ......................................................... 593
New SNMP MIB Alarms .............................................................................. 593
Modified SNMP MIB Alarms ................................................................. 593
Deprecated SNMP MIB Alarms .............................................................. 593
SNMP MIB Conformance Changes for 17.5 ............................................... 594
New SNMP MIB Conformance ............................................................... 594
Modified SNMP MIB Conformance .......................................................... 594
Deprecated SNMP MIB Conformance ........................................................ 594
SNMP MIB Object Changes for 17.4 ......................................................... 595
New SNMP MIB Objects .............................................................................. 595
Modified SNMP MIB Objects ................................................................. 595
Deprecated SNMP MIB Objects .............................................................. 595
SNMP MIB Alarm Changes for 17.4 ......................................................... 596
New SNMP MIB Alarms .............................................................................. 596
Modified SNMP MIB Alarms ................................................................. 596
Deprecated SNMP MIB Alarms .............................................................. 596
SNMP MIB Conformance Changes for 17.4 ............................................... 597
New SNMP MIB Conformance

597

Modified SNMP MIB Conformance...........................................597

Deprecated SNMP MIB Conformance..........................................597

SNMP MIB Object Changes for 17.3.......................................598

New SNMP MIB Objects................................................................598

Modified SNMP MIB Objects.....................................................598

Deprecated SNMP MIB Objects................................................598

SNMP MIB Alarm Changes for 17.3...........................................599

New SNMP MIB Alarms............................................................599

Modified SNMP MIB Alarms.....................................................599

Deprecated SNMP MIB Alarms................................................599

SNMP MIB Conformance Changes for 17.3.................................600

New SNMP MIB Conformance....................................................600

Modified SNMP MIB Conformance...........................................600

Deprecated SNMP MIB Conformance........................................600

SNMP Command Changes for 17.3...........................................601

CSCur13393 - Cisco ASR5000 SAE-GW High CPU Utilisation Vulnerability...........................................................................601

Command Changes.................................................................601

snmp runtime-debug..................................................................601

SNMP MIB Object Changes for 17.2...........................................603

New SNMP MIB Objects............................................................603

Modified SNMP MIB Objects.....................................................603

Deprecated SNMP MIB Objects................................................603

SNMP MIB Alarm Changes for 17.2...........................................604

New SNMP MIB Alarms............................................................604

Modified SNMP MIB Alarms.....................................................604

Deprecated SNMP MIB Alarms................................................604

SNMP MIB Conformance Changes for 17.2.................................605

New SNMP MIB Conformance....................................................605

Modified SNMP MIB Conformance...........................................605

Deprecated SNMP MIB Conformance........................................605

SNMP MIB Object Changes for 17.1...........................................606

New SNMP MIB Objects............................................................606

Modified SNMP MIB Objects.....................................................606

Deprecated SNMP MIB Objects................................................606

SNMP MIB Alarm Changes for 17.1...........................................607

New SNMP MIB Alarms............................................................607

Modified SNMP MIB Alarms.....................................................607

Deprecated SNMP MIB Alarms................................................607

SNMP MIB Conformance Changes for 17.1.................................609

New SNMP MIB Conformance....................................................609

Modified SNMP MIB Conformance...........................................609

Deprecated SNMP MIB Conformance........................................609

SNMP MIB Object Changes for 17.0...........................................610

New SNMP MIB Objects............................................................610

Modified SNMP MIB Objects.....................................................610

Deprecated SNMP MIB Objects................................................610

SNMP MIB Alarm Changes for 17.0...........................................611

New SNMP MIB Alarms............................................................611

Modified SNMP MIB Alarms.....................................................611

Deprecated SNMP MIB Alarms................................................611

SNMP MIB Conformance Changes for 17.0.................................612

New SNMP MIB Conformance....................................................612

Modified SNMP MIB Conformance...........................................612
Deprecated SNMP MIB Conformance .......................................................... 612

**System Changes in Release 17 ................................................................. 613**

System and Platform Enhancements for Release 17.3 ........................................ 614
- CSCuq86655 - TACACS Privilege Level needs to support Security Admin .......... 614
  Feature Changes ....................................................................................... 614
  Command Changes ................................................................................... 614
  Performance Indicator Changes ................................................................. 615
System and Platform Enhancements for Release 17.2 ........................................ 616
- CSCuq62755 - Force an SRP switchover when a configured EGP Discard Threshold occurs ................................................................................. 617
  Feature Changes ....................................................................................... 617
System and Platform Enhancements for Release 17.1 ........................................ 617
- CSCuq90891 - Russia timezone update ...................................................... 618
  Feature Changes ....................................................................................... 618
- CSCuq39932 - Update support for Russian Timezones .................................... 618
  Feature Changes ....................................................................................... 618
- CSCuo50026 - Feature Changes ................................................................. 619
System and Platform Enhancements for Release 17.0 ........................................ 623
- CSCtr45924 - root privileges for ftp-user, no restriction to specific ftp-directory ..................................................................... 623
  Feature Changes ....................................................................................... 623
  Command Changes ................................................................................... 623
- CSCtr55441 - VoLTE related ICSR optimization .............................................. 624
  Feature Changes ....................................................................................... 625
- CSCum39930 - Pilot Packet to Multiple Destinations ........................................ 626
  Feature Changes ....................................................................................... 626
  Command Changes ................................................................................... 626
- CSCum39932 - Pilot Packet Statistics Enhancement ......................................... 626
  Feature Changes ....................................................................................... 627
  Performance Indicator Changes ................................................................. 627
- CSCum50058 - ICSR Stats Reporting through BulkStats .................................. 628
  Feature Changes ....................................................................................... 628
  Performance Indicator Changes ................................................................. 628
- CSCum50087 - Configurable Subscriber State Management Audit Process-Phase2 .............................................................................. 629
  Feature Changes ....................................................................................... 630
  Command Changes ................................................................................... 630
- CSCum87749 - Configurable SRP Redundancy/AAA/Diameter Guard Time(r) ................................................................. 630
  Feature Changes ....................................................................................... 630
  Command Changes ................................................................................... 631
- CSCum87759 - Configurable MinRtAdvInterval .............................................. 631
  Feature Changes ....................................................................................... 632
  Command Changes ................................................................................... 632
- CSCum87764 - Announcing Routes from Standby Chassis ................................ 632
  Feature Changes ....................................................................................... 632
  Command Changes ................................................................................... 633
- CSCum87769 - Chassis to Chassis BFD Monitoring ......................................... 633
  Feature Changes ....................................................................................... 633
  Command Changes ................................................................................... 633
- CSCum87774 - MFL 1858: KPI to Increase the 32K BGP routes per context to 64K (MPN) ................................................................. 635
  Feature Changes ....................................................................................... 635
  Command Changes ................................................................................... 635
- CSCum87782 - Increase the number of configurable SSH hosts and keys in ctx ................................................................. 636
  Feature Changes ....................................................................................... 636
VPC-DI Changes in Release 17

VPC-DI Feature Changes for 17.1
CSCum87789 - Trap for failed Diameter or Radius peer success
Feature Changes
CSCum98092 - MS-to-MS traffic for Ipsec
Feature Changes
CSCun88666 - [ePDG] require ipsec-large support
Feature Changes
Command Changes
Performance Indicator Changes
CSCuo55792 - new switchover reason as dual active + dual standby and bulkstat support
Feature Changes
Performance Indicator Changes
CSCuo84001 - [ares] Need User configurable command to monitor FAP Egress drops
Feature Changes
Command Changes
CSCuo84086 - IPv6 support for NTP
Feature Changes
CSCuo84096 - IPv6 support for SNMP
Feature Changes
CSCuo90200 - Show configuration do not display Checkpoint Session duration
Feature Changes
Command Changes
CSCup90954 - BGP: VRF CLI 'ip maximum-routes' threshold of 32K should be 64K (NEMO)
Feature Changes
Command Changes
CSCup91637 - FTP server with ipv6 is not working
Feature Changes
CSCuq49149 - NTP service does not work without ipv4 address for SPI0 int
Feature Changes
CSCzn41068 - ICSR support for L2TP on GGSN/PGW
Feature Changes

VPC-DI Feature Changes for 17.0
CSCui20002 - SSI knpusim
Feature Changes ................................................................. 650
CSCui20092 - SSI support for virtio/vmxnet3 vNIC types ................................. 650
  Feature Changes ............................................................ 650
CSCup57481 - CFE support for passthrough NIC types ..................................... 651
  Feature Changes ............................................................ 651
CSCuq13550 - 'show hardware' should show NIC multi-q support, hugepage, etc... .... 651
  Feature Changes ............................................................ 651
  Performance Indicator Changes ................................................ 651
CSCuq13580 - SI/DI installer should have option to leave VMs running .................. 651
  Feature Changes ............................................................ 651
CSCuq13684 - SI/DI install script should have option to package disk images ............ 652
  Feature Changes ............................................................ 652
VPC-SI Changes in Release 17 .................................................. 653
  VPC-SI Feature Changes for 17.0 ............................................ 654
  CSCui20002 - SSI knpusim ................................................... 654
    Feature Changes .......................................................... 654
  CSCui20092 - SSI support for virtio/vmxnet3 vNIC types .................................. 654
    Feature Changes .......................................................... 654
  CSCuq13550 - 'show hardware' should show NIC multi-q support, hugepage, etc... .... 654
    Feature Changes .......................................................... 654
  CSCuq13580 - SI/DI installer should have option to leave VMs running .................. 655
    Feature Changes .......................................................... 655
  Performance Indicator Changes ................................................ 655
  CSCuq13580 - SI/DI installer should have option to leave VMs running .................. 655
    Feature Changes .......................................................... 655
  CSCuq13684 - SI/DI install script should have option to package disk images ............ 655
    Feature Changes .......................................................... 655
About this Guide

This preface describes the Release Change Reference, how it is organized and its document conventions.

This book includes new feature descriptions and configuration, performance, and security changes for StarOS Release 17. The Release Change Reference is separated into individual chapters per product and also includes chapters for system level, SNMP MIB, and accounting management changes. Each chapter is also separated into sections that indicate the changes to the product documentation sorted by the date that this change was included in the product documentation.

For new feature descriptions and configuration, performance, and security changes that occurred in earlier releases, see the Release Change References for those releases.
## Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</td>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td>![!]</td>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td>![⚠️]</td>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

### Typeface Conventions

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as screen display</td>
<td></td>
</tr>
<tr>
<td>This typeface represents displays that appear on your terminal screen, for example:</td>
<td></td>
</tr>
<tr>
<td>Login:</td>
<td></td>
</tr>
<tr>
<td>Text represented as <strong>commands</strong></td>
<td></td>
</tr>
<tr>
<td>This typeface represents commands that you enter, for example:</td>
<td></td>
</tr>
<tr>
<td>show ip access-list</td>
<td></td>
</tr>
<tr>
<td>This document always gives the full form of a command in lowercase letters.</td>
<td></td>
</tr>
<tr>
<td>Commands are not case sensitive.</td>
<td></td>
</tr>
<tr>
<td>Text represented as <strong>command variable</strong></td>
<td></td>
</tr>
<tr>
<td>This typeface represents a variable that is part of a command, for example:</td>
<td></td>
</tr>
<tr>
<td>show card slot_number</td>
<td></td>
</tr>
<tr>
<td>slot_number is a variable representing the desired chassis slot number.</td>
<td></td>
</tr>
<tr>
<td>Text represented as menu or sub-menu names</td>
<td></td>
</tr>
<tr>
<td>This typeface represents menus and sub-menus that you access within a software application, for example:</td>
<td></td>
</tr>
<tr>
<td>Click the <strong>File</strong> menu, then click <strong>New</strong></td>
<td></td>
</tr>
</tbody>
</table>
Supported Documents and Resources

Related Common Documentation

The following common documents are available:

- *AAA Interface Administration Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration Reference*
- *Installation Guide* (platform dependant)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependant)
- *Thresholding Configuration Guide*

Related Product Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following product documents are also available and work in conjunction with the *Release Change Reference*:

- *ADC Administration Guide*
- *CF Administration Guide*
- *ECS Administration Guide*
- *ePDG Administration Guide*
- *eWAG Administration Guide*
- *GGSN Administration Guide*
- *HA Administration Guide*
- *HeNB-GW Administration Guide*
- *HNB-GW Administration Guide*
- *HSGW Administration Guide*
- *InTracer Installation and Administration Guide*
- *IPSec Reference*
- *IPSG Administration Guide*
- *MME Administration Guide*
- MURAL Installation Guide
- MURAL User Guide
- MVG Administration Guide
- NAT Administration Guide
- PDSN Administration Guide
- PSF Administration Guide
- P-GW Administration Guide
- SAEGW Administration Guide
- SaMOG Administration Guide
- SecGW Administration Guide
- SGSN Administration Guide
- S-GW Administration Guide

Obtaining Documentation

The most current Cisco documentation is available on the following website:
http://www.cisco.com/cisco/web/psa/default.html

Use the following path selections to access the Release Change Reference documentation:
Products > Wireless > Mobile Internet> Platforms > Cisco ASR 5000 Series > Cisco ASR 5000
Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
AAA Changes in Release 17

This chapter identifies accounting management features and functionality added to, modified for, or deprecated from AAA in StarOS 17 software releases.
AAA Enhancements for 17.5

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

**Feature Changes** - new or modified feature 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.

**CSCuv64729 - Configurable CC values**

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

### Feature Changes

**Selective Disabling of Credit-Control based on Charging Characteristics Profile**

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. In this release, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The `cc profile cc-profile-index prepaid prohibited` CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored. If no CC group is defined, the default CC group is applied.

**Limitations:**

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session setup. Once the credit-control-group is selected after session setup, this feature is not applicable.

### Command Changes

**cc-profile**

This new CLI command has been added under APN configuration to configure Charging Characteristic values as postpaid/prepaid to enable/disable Gy session towards the OCS.
AAA Changes in Release 17

AAA Enhancements for 17.5

configure

context context_name

apn apn_name

cc-profile { cc_profile_index | any } { prepaid-prohibited | credit-control-group cc_group_name }

no cc-profile cc_profile_index

des

Notes:
- cc_profile_index: Specifies the CC profile index. cc_profile_index must be an integer from 0 through 15.
- any: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring “any” CLI command will not override other specific configurations under APN.
- prepaid-prohibited: Disables prepaid Gy session for the configured profile index.
- cc_group_name: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

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

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Support for SGSN-Address AVP and SGSN_CHANGE Event Trigger

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 17.3

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

**Feature Changes** - new or modified feature 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.

**CSCus66465** - show diameter route status command causes high CPU utilization alarms

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

**Feature Changes**

**Changes to “show diameter route” Command**

*Previous Behavior:* The keyword option “*status*” in the CLI command “*show diameter route status*” was earlier visible to customers.

*New Behavior:* Now, the “*status*” keyword is made hidden as this is intended for internal debugging purpose.

**CSCut26323** - Round-robin algorithm support for RADIUS mediation-device for hex IMSI

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

**Feature Changes**

**Change in Radius Server Selection Method for Hex based IMSI addresses**

The current implementation maps a given IMSI to the same RADIUS server. The round-robin algorithm across IMSI takes into account only the decimal values. Now it includes the hexadecimal values as well for PMIPv6.

*Previous Behavior:* For subscribers with IMSI containing hexadecimal characters the round robin algorithm fails causing the messages to be forwarded to a single RADIUS server all the time. This algorithm works only for decimal based IMSI addresses.

*New Behavior:* In this release, support is extended to hexadecimal based IMSI addresses. That is, IMSI based round robin would be done for subscribers with hexadecimal based IMSI addresses.
CSCut26850 - Enhance multiple diameter peers to use same Host-name

Applicable Products: ePDG, GGSN, HA, HeNBGW, HNBGW, HSGW, IPSG, MME, PDSN, P-GW, SGSN, SAEGW, SaMOG, S-GW

Feature Changes

Provision for Multiple SCTP Associations towards Same Diameter Peer

The current endpoint configuration allows each SCTP association to be uniquely identified by a Diameter peer name. But there was a requirement where two SCTP associations are identified with the same peer name. This kind of reused peer-name was used by HSS peers which act as Active and Standby HSS nodes. The SCTP associations in HSS behave in a manner such that one association is always SCTP active (for the active HSS) while the other SCTP association with the standby HSS would be closed and would keep flapping. In order to allow configuring multiple SCTP associations with same peer-name, a new optional keyword "destination-host-name" has been introduced in the peer CLI command that is available as part of the Endpoint configuration.

Important: This enhancement is applicable to 17.2.2 and later releases.

This additional configuration option will allow multiple unique peers (Diameter HSS servers) to be configured with the same host name. With this enhancement, MME will be capable of provisioning multiple Diameter SCTP associations to reach the same HSS peer name. This configuration will also ensure that all the Diameter messages are exchanged properly with the configured destination host.

Internally the peers are identified with unique peer-name. But the Origin-host AVP provided by the server (in CER/CEA/Appmsgs) is validated against both peer-name and destination-host-name provided in the CLI. Even if multiple peers are responding with same Origin-Host, this can be validated and accepted based on the CLI configuration.

Previous Behavior: Current Diameter endpoint implementation does not provide the flexibility to configure two Diameter peers (servers) with the same host name.

New Behavior: The existing endpoint peer CLI command has been enhanced to include optional Destination Host Name information to address the customer’s requirement.

If a peer is selected by Diameter base protocol to forward an application request, then the host name specified through the "destination-host-name" option will be used to encode the Destination-Host AVP.

This keyword "destination-host-name" is made optional for backward compatibility. That means, if the destination-host-name is not specified in the CLI, the peer name itself is copied to the destination-host-name for backward compatibility.

Command Changes

peer

A new optional keyword "destination-host-name" has been added as part of the peer CLI command in Diameter endpoint configuration to allow configuring multiple unique peers with the same host name.

configure

    context context_name
`diameter endpoint endpoint_name`

`peer [*] peer_name [*] [ realm realm_name ] [ destination-host-name host_name ] { address ipv4/ipv6_address [ [ port port_number ] [ connect-on-application-access ] [ send-dpr-before-disconnect disconnect-cause disconnect_cause ] [ sctp ] ] + | fqdn fqdn [ [ port port_number ] [ send-dpr-before-disconnect disconnect-cause disconnect_cause ] [ rlf-template rlf_template_name ] ] ] }

`no peer peer_name [ realm realm_name ]`

`end`

Notes:

- `destination-host-name host_name`: Specifies the destination host name as an alphanumeric string of 1 through 63 characters.
AAA Enhancements for 17.2

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

**Feature Changes** - new or modified feature 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.

**CSCum90063 - Counters and Bulkstats for total-usage-report in PCC schema**

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

**Performance Indicator Changes**

**IMSA Schema**

The following bulkstat variable is newly added to this schema to track the total volume usage report processed by IMSA.

- dpca-imsa-usage-report

This variable is required to get the VoGx reporting rate and is very critical for the capacity and performance tool.

**CSCur89572, CSCus36547, CSCur13994 - Diameter support for “EPS-Location-Information” AVP**

Applicable Products: MME

**Feature Changes**

**AVP Support for Spec Compliancy Requirements**

This feature enables MME to send UE current location information or last known location information through “EPS-Location-Information” AVP in the Insert-Subscriber-Data-Answer (IDA) message. This AVP is signaled from MME to HSS through the S6a interface in order to comply with 3GPP TS 29.272 v11.9.0 specification.

**CSCus30296, CSCus30276 - [ePDG] Diameter changes for tunnel endpt ip support in SWm interface**

Applicable Products: ePDG
Feature Changes

AVP Support in SWm Standard Dictionary

**Previous Behavior:** UE-Local-IP-Address AVP was never included in DER message sent to AAA server during initial authentication.

**New Behavior:** This feature enables ePDG to include the UE-Local-IP-Address AVP in the standard SWm dictionary. This AVP will carry the IKEv2 tunnel endpoint IP address in DER messages.
AAA Enhancements for 17.1

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

**Feature Changes** - new or modified feature 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.

**CSCtz79646, CSCuh67284 - PCSCF discovery - v4/v6 addresses not sent always for v4/v6 pdn req**

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

**Feature Changes**

**Send P-CSCF Address Based on PCO Request**

**Previous Behavior:** IMSA will select the servers if requested server address type and selected row server-address type are the same. Otherwise, it will return NULL.

**New Behavior:** P-CSCF server selection algorithm is modified such that the P-CSCF server selection now happens based on UE-requested server-type.

**CSCud26703 - Enable / disable multiple back to back CCR-UUs from PGW/GGSN**

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

**Feature Changes**

**Multiple CCR-UUs Support Over Gx Interface**

**Previous Behavior:** ASR5K node earlier supported only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update was dropped (like RAT change/ULI change).

**New Behavior:** ASR5K supports a configurable CLI command “max-outstanding-ccr-u” under IMS Authorization Service configuration mode to allow multiple CCR-UUs towards PCRF. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.
Though the `max-outstanding-ccr-u` CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

These are the access side updates for which CCR-U might be triggered:

- Bearer Resource Command
- Modify Bearer Request (S-GW change, RAT change, ULI change)
- Modify Bearer Command

These are the following internal updates for which CCR-U is triggered:

- S-GW restoration
- Bearer going down (GGSN, BCM UE_Only)
- ULI/Timezone notification
- Default EPS bearer QoS failure
- APN AMBR failure
- Charging-Rule-Report
- Out of credit / reallocation of credit
- Usage reporting
- Tethering flow detection
- Access network charging identifier

**Customer Impact:** Based on the CLI configuration signaling might increase.

### Command Changes

**max-outstanding-ccr-u**

This command enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        [ default ] max-outstanding-ccr-u value
  end
```

**Notes:**

- `value` must be an integer value from 1 through 12. The default value is 1.

### Performance Indicator Changes

**show ims-authorization policy-control statistics**
The following fields are newly added to the output of this show command to support multiple outstanding CCR-U per session.

- Responses in Queue
  - Current Responses in Queue
  - Purged Responses
  - Total Response in Queue
- Requests in Queue for LP
  - Current Requests in Queue
  - Purged Requests
  - Total Requests Fwd to LP

**CSCud65027 - EPC - CCR-U not sent after RAR received**

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

**Feature Changes**

**Handling Users Session During CCR-RAR Collision**

*Previous Behavior:* In case of CCR-RAR collision for user’s session supporting multiple services, ASR5K did not initiate a new Credit-Control-Request message to perform re-authorization for the remaining services/rating-groups (RGs).

*New Behavior:* Generic support is provided to re-authorize the remaining services/rating-groups, post CCR-RAR collision, for user’s session supporting multiple services to complete the credit re-authorization process.

That is, in this scenario, ASR5K will send RAA with Result-Code 2002 and will wait for pending response from the server. Once a response is received for the pending request, ASR5K will initiate another CCR-U containing all the active RGs with Forced-Reauth as the reporting-reason to complete the re-authorization.

**CSCum75837, CSCuq98021 - Support of gtp-cause-code "APN access denied-no subscription"**

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

**Feature Changes**

**Support for New GTP Cause Code**

A new gtp-cause-code “apn-access-denied-no-subscription” is introduced to send the GTP cause code as “GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION” in GTP response. The GTP cause code is set based on the Diameter result codes “auth-rejected(5003)”, “credit-limit-reached(4012)”, “user-unknown(5030)” and “end-user-service-denied(4010)".
Command Changes

diameter result-code

A new keyword “apn-access-denied-no-subscription” is added to this command for mapping the Diameter result-codes with this GTP cause code.

configure

  require active-charging

  active-charging service service_name

    credit-control service_name

    diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code apn-access-denied-no-subscription

    default diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code

end

Notes:

- If this CLI command is configured and if the CCR-U is received with auth-rejected(5003) or credit-limit-reached(4012) or user-unknown(5030) or end-user-service-denied(4010), then the gtp result-code is sent as “apn-access-denied-no-subscription”.
- Earlier, GTP_NO_RESOURCES_AVAILABLE was sent as a default GTP result code. Now with this CLI configured and the corresponding Diameter result codes received, GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION is sent on GTPC.
- This CLI command is applicable only for CCR-I messages.

CSCuo72213 - RLF Feature qualification on S6b

Applicable Products: GGSN, MME, P-GW

Feature Changes

RLF Feature Support on S6b

It has been verified that the Rate Limiting Function (RLF) is supported on S6b Diameter interface. That is, the RLF framework is used by S6b for rate-limiting/throttling Diameter messages on S6b interface.

CSCup05517 - Gy Validity Timer to start on receipt of CCA in all cases

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

Configuration Support for Starting Validity Timer for FUI-Redirect

A new CLI configuration option is available to control the starting of validity timer for the FUI-redirect scenario. Based on the configuration value, DCCA decides when to start the redirect-validity-timer. By default, it is started on receiving the first matching packet.

Command Changes

diameter redirect-validity-timer

A new CLI command is added to control the starting of validity timer on receipt of CCA in all cases.

configure

require active-charging

active-charging service service_name

credit-control service_name

diameter redirect-validity-timer { immediate | traffic-start }

default diameter redirect-validity-timer

diameter redirect validity timer

Notes:

- **immediate**: This keyword will make the redirect-validity-timer to get started immediately.
- **traffic-start**: This keyword will make the redirect-validity-timer to get started only on receiving matching traffic. This is the default configuration.

CSCup52642 - Restoration priority indicator avp is not ignored in 16.0 builds

Applicable Products: GGSN, P-GW

Feature Changes

Flag Setting for Restoration-Priority AVP

**Previous Behavior:** M flag was enabled for Restoration-Priority AVP in customer-specific S6b dictionary. Due to this, the subscriber call got rejected when this AVP was sent.

**New Behavior:** The M flag for this AVP is now removed in the customer-specific S6b dictionary.

CSCup75566 - MFL 2772- Add CC-Group AVP in Gx Dictionary

Applicable Products: GGSN, P-GW
Feature Changes

Parsing of QoS-Information AVP in dpca-custom19 Dictionary

**Previous Behavior:** QoS-Information AVP will always be sent in CCR message for custom Gx dictionary “dpca-custom19”.

**New Behavior:** QoS-Information AVP will not be sent always. This behavioral change is made to avoid the risk at the customer’s PCRF with more signaling than it can handle.

**CSCuq63995 - USAGE_REPORT compatibility handling with PCRF**

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

Feature Changes

**USAGE_REPORT Compatibility Handling with PCRF**

The Event-Trigger AVP’s USAGE_REPORT value has been changed by 3GPP in subsequent releases. To be able to gracefully handle the change when moving between 3GPP releases supporting the different values for the Usage Report, the existing CLI command `diameter map usage-report` is modified to support configuration of multiple values of usage report mapping.

While migrating from older versions to current version, all of the sessions created before the migration will continue to use 26 as usage report event trigger value. The new session will use usage-report value based on PCRF value or default value.

**Previous Behavior:** Current implementation of “`diameter map usage-report`” CLI command supports only one value of configuration out of 26, 29 and 30 in usage report map.

**New Behavior:** This CLI is extended to support configuration of multiple values of usage report mapping.

Command Changes

`diameter map usage-report`

This CLI command is modified to support configuration of multiple values of usage report mapping.

```
configure
  context context_name
    ims-auth-service service_name
    policy-control
      diameter map usage-report { 29 | [ 26 | 33 ] [ 26 | 33 ] }
      default diameter map usage-report
    end
```
CSCur26626 - [ePDG] Non UICC device support EAP-TLS/EAP-TTLS support Diameter changes

Applicable Products: ePDG

Feature Changes

New AVP in DER Message for SWm Dictionary

Previous Behavior: Diameter AVP “Framed-MTU” was neither supported nor sent in the DER message over SWm interface.

New Behavior: Framed-MTU AVP is now sent in the DER message if it is configured under ePDG Service configuration mode. This AVP is included in the standard SWm dictionary for non-UICC devices certificate based device authentication.

Customer Impact: Framed-MTU should be supported by AAA server.

CSCur27981 - T-bit not working for RF retried msg

Applicable Products: P-GW

Feature Changes

T Flag on Retried Rf Messages

Previous Behavior: T bit was not set when the Rf message is retried to the same server in the case of customer-specific SWm dictionary. That is, the T bit was not set for the Rf message that was retried due to backpressure scenario.

New Behavior: For customer-specific SWm dictionary, the T bit is set when the message is retried to the same Rf primary/secondary server.

P-GW is configured using the `app-level-retransmission set-retransmission-bit` command to set the T flag on retransmission so that the Rf peer is aware of the message being a retransmission and hence can respond back as desired.

CSCur37593 - [ePDG]Missing AVPs in SWm standard dictionary

Applicable Products: ePDG

Feature Changes

New AVPs in SWm Standard Dictionary

These Diameter AVPs are included in the standard SWm dictionary for ePDG.

- Subscription-ID — This AVP is being recognized and parsed in DEA message.
- User-Name — This AVP is being recognized and parsed in AAA message.
• Auth-Session-State — This AVP is being recognized and parsed in ASR message.

**CSCur43509 - PCEF is not triggering 29 as APN-AMBR mod failure in CCR**

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

**Feature Changes**

**Parsing of Event Trigger for USAGE_REPORT**

**Previous Behavior:** When diameter map usage-report is mapped to 26, then APN AMBR modification failure event trigger is not supported.

**New Behavior:** APN AMBR modification failure event trigger is now supported for all usage report trigger values (26, 33, 29).

**CSCur77837 - VoWiFi feature Selective Use of BEARER-USAGE for VoWiFi and VoLTE**

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

**Feature Changes**

**Selective Use of Bearer-Usage for VoWiFi and VoLTE**

**Previous Behavior:** Bearer-Usage AVP was always sent in the CCR-I message for WLAN access type. Hence, PCRF used to reject the subscriber call.

**New Behavior:** Bearer-Usage AVP is sent only when the value of IP-CAN-Type AVP is GPRS/EPS.

In this release, the Bearer-Usage AVP will not be sent for WLAN for gx-standard dictionary.
AAA Enhancements for 17.0

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

**Feature Changes** - new or modified feature 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.

CSCts30745 - [PDSN-VRoGx]CCR-U sent twice when Gx asks for usage report for a mon key

**Applicable Products:** PDSN

**Feature Changes**

**Signaling on Gx Interface**

**Previous Behavior:** Extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

**New Behavior:** Extra CCR-U is not generated now for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

Also, extra CCR-U is not generated now when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

CSCtz79646 - PCSCF discovery - v4/v6 addresses not sent always for v4/v6 pdn req

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

**Feature Changes**

**Send P-CSCF Address Based on PCO Request**
Prev **Previous Behavior**: IMSA will select the servers if requested server address type and selected row server-address type are the same. Otherwise, it will return NULL.

**New Behavior**: P-CSCF server selection algorithm is modified such that the P-CSCF server selection now happens based on UE-requested server-type.

**CSCua99869, CSCue68175 - Radius policy (Firewall Policy) support in Gx**

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

**Feature Changes**

**Support for Firewall Policy on Gx**

The Diameter AVP “SN-Firewall-Policy” has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface.

This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

**CSCuf73716 - PI: The CLI "accounting-mode radius-diameter" is not for diameter**

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

**Feature Changes**

**Configuration Changes to Accounting Mode**

The existing CLI command “accounting-mode” in APN configuration mode is used only for RADIUS/GTPP accounting and not for Diameter accounting. Hence, the `diameter` keyword has been removed from this command. That is, the CLI command “accounting-mode radius-diameter” has been modified to “accounting-mode radius”.

**Important**: The existing command “accounting-mode radius-diameter” will still be supported under concealed mode. So, the existing configuration can be reloaded, but the new configuration will show “accounting-mode radius”.

**Command Changes**

**accounting-mode radius-diameter**

The existing CLI command “accounting-mode radius-diameter” in APN configuration mode has been modified to “accounting-mode radius.”
configure

context context_name

apn apn_name

  accounting-mode radius [ no-interims | no-early-pdus ]

  default accounting-mode

end

Notes:
- In the accounting-mode command, the keyword “diameter” has been removed.

CSCuf82575 - [ePDG] Auth-Failure counter for epdg-service stats is not incrementing

Applicable Products: ePDG

Feature Changes

Changes to Session Disconnect Reason

Previous Behavior: ePDG used to indicate session disconnect reason as “invalid-aaa-attribute” when AAA server rejects the DEA.

Also, it used to send the STR for error result-codes received in the second DEA for SWm dictionaries.

New Behavior: Now, the disconnect reason “auth-failed” is set when the session is rejected by AAA server due to authentication failure and if AVP failure is encountered then “invalid-aaa-attribute” will be set.

When, in second DEA, the 4001 result code is sent by AAA server ePDG does not send the STR but clears the Diameter session with “auth_failed” as disconnect reason.

Customer Impact: The session disconnect reason is now corrected.

CSCug33751 - Host statistics not supported in DCCA

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

Feature Changes

Host Statistics Support in Gy

Previous Behavior: Currently, DCCA/Gy statistics were incremented only in those cases when the messages were sent and received from directly connected Diameter peers. If the origin-host is different than the provisioned peers in the answer message, the statistics were not incremented. Similarly, if the Diameter messages are sent to Diameter host (which are reachable through directly connected peers), the statistics were not counted.
New Behavior: These are corrected now with this release and DCCA statistics reporting is enhanced to cover counter increments in the above situations.

The “show active-charging credit control statistics server” CLI command will support a new keyword “all” to enable administrator see all server (including Diameter peers and hosts) statistics. Host statistics will be displayed under Uncategorized statistics.

These additional bulkstat counters help operators to measure the performance of the Gy peers.

Command Changes

clear active-charging credit-control statistics server

`all` is a new keyword in this command to clear the statistics for all the Diameter peers and hosts.

```plaintext
clear active-charging credit-control statistics server { all | ip-address ip_address [ port port_num ] | name server_name } [ | { grep grep_options | more } ]
```

Notes:
- `all`—Displays all available statistics including host statistics. The host statistics will be displayed under Uncategorized statistics.

show active-charging credit-control statistics server

`all` is a new keyword in this command to enable administrator see all server statistics including host statistics.

```plaintext
show active-charging credit-control statistics server { all | ip-address ip_address [ port port_num ] | name server_name } [ | { grep grep_options | more } ]
```

Notes:
- `all`—Displays the statistics for all the peers and hosts. The host statistics will be displayed under Uncategorized statistics.

CSCug58210 - RAT-TYPE should be 2003 for eHRPD in Gxa message

Applicable Products: HSGW

Feature Changes

Value Change for RAT-Type Attribute

Previous Behavior: The value of RAT-Type attribute for HRPD implementation is 2003 in 3GPP release 8, and 2001 for eHRPD in 3GPP releases 9 and 10. These values are valid as per the older version of 3GPP TS 29.212.

New Behavior: HSGW now supports RAT-Type value as 2001 for HRPD in Gxa message, and 2003 for eHRPD as per the latest version (v9.6.0) of 3GPP TS 29.212.
CSCuh99978 - Implement COA rate limiting

Applicable Products: ePDG, GGSN, P-GW

Feature Changes

Support for CoA Rate Limiting

It has been verified that the rate of CoA/DM message handling requested by customer is already supported without causing any degradation in system behavior (memory, CPU, crashes, etc).

CSCui12490 - Enhancement in Rf Stats

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

Feature Changes

Enhanced KPIs for Rf Interface

For a better troubleshooting and analyzing issues related to Rf (billing), additional Diameter accounting and authentication statistics and bulkstatistics are supported:

- to identify the number of times CCF responds back with some key response codes.
- to indicate breakdown of interim records cut due to various Change Conditions.
- to distinguish request/response timeout i.e. Application timeout (vs) no response received from the CCF/peer.
- to find the current number of Rf (offline) sessions.

Performance Indicator Changes

Diameter Accounting Schema

The following bulkstat variables are new in this release:

- acri-vol-limit
- acri-time-limit
- acri-rat-change
- acri-tz-change
- acri-plmn-change
- acri-max-charg-cond
- acri-sdf-vol-limit
- acri-sdf-time-limit
- acri-aii-timer
- diameter-acct-msg-success
- diameter-acct-msg-err-protocol
- diameter-acct-msg-err-transient
- diameter-acct-msg-err-permanent
- diameter-acct-msg-err-other
- diameter-acct-res-timeout

**System Schema**

The following bulkstat variables are new in this release:

- diamacct-msg-acastartreqtmo
- diamacct-msg-acastartrestmo
- diamacct-msg-acainterimreqtmo
- diamacct-msg-acainterimrestmo
- diamacct-msg-acastopreqtmo
- diamacct-msg-acastoprestmo

The following bulkstat variables are removed from the system schema:

- diamacct-msg-acastarttmo
- diamacct-msg-acainterimtmo
- diamacct-msg-acainterimtmo
- diamacct-msg-acastoptmo

**show diameter aaa-statistics**

The following fields are new in this release:

- Session Stats – Under Authentication Servers Summary
  - Active Auth Sessions
  - Active Acct Sessions
- Message Stats – Under Accounting Servers Summary
  - ACA-Start Req-Timeouts
  - ACA-Start Res-Timeouts
  - ACA-Interim Req-Timeouts
  - ACA-Stop Req-Timeouts
  - ACA-Stop Res-Timeouts
- AC Message Error Stats – Under Accounting Servers Summary
  - Response Timeouts
- ACR Message Interim Event Stats – Under Accounting Servers Summary
  - Volume-limit
  - Time-Limit
• RAT-Change
• TimeZone-Change
• PLMN-Change
• Max-Charging-Condition
• Service-Data-Time-Limit
• Service-Data-Vol-Limit
• AII-Timer

• Result Code Stats – Under Accounting Servers Summary
  • Result Code 2xxx
  • Result Code 3xxx
  • Result Code 4xxx
  • Result Code 5xxx
  • Other Result Code

The following fields under “Message Stats” in “Accounting Servers Summary” are removed from the CLI output:

• ACA-Start Timeouts
• ACA-Interim Timeouts
• ACA-Stop Timeouts

CSCui59026 - Enhancements in ASR5x00 Timer Implementation - Gy Changes

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

Feature Changes

Configuration Changes to Gy Timers

Previous Behavior: Current timers on the Gy interface were configured in seconds. Additionally, the Gy timers were common for all message types e.g. CCR-I, CCR-T, CCR-U, CCR-E.

New Behavior: This feature implementation involves modifying the existing CLI command “diameter pending-timeout” under Credit Control Configuration mode to accept the timeout value in deciseconds instead of seconds and allow configuring independent timers for all message types like CCR-I, CCR-U, CCR-T and CCR-E.

Customer Impact: This feature enhancement provides additional flexibility for operator to configure independent timers with reduced granularity.

Command Changes

diameter pending-timeout
The existing CLI command “diameter pending-timeout” under Credit Control Configuration mode has been modified such that the time can be specified in deciseconds along with different message types. The default time will be 100 deciseconds (10 seconds).

```
configure
    require active-charging
    active-charging service service_name
    credit-control group group_name
        diameter pending-timeout timer_value deciseconds msg-type { any | ccr-event | ccr-initial | ccr-terminate | ccr-update }  
    default diameter pending-timeout variable
    end
```

Notes:
- The feature implementation ensures that the modified timer configuration is backward compatible. If the CLI command is configured without “deciseconds” and “msg-type”, the configured time will be taken as seconds and while displaying the CLI it will be converted to deciseconds and msg-type will be “any”.

**CSCui53808 - With OCS unreachable CCR-U includes unexpected AVP**

**OTHER_QUOTA_TYPE**

Applicable Products: GGSN, P-GW

**Feature Changes**

**Granted Quota for Usage Reporting**

**Previous Behavior:** CCR-U triggered on server retries does not take server granted quota into account for reporting USU.

**New Behavior:** CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created mscc, interim quota configuration is taken as reference for reporting USU.

**CSCuj34791 - full checkpoint to micro checkpoint conversion**

Applicable Products: GGSN, P-GW

**Feature Changes**

**Full and Micro Checkpoint Optimizations**
Whenever there is any major event happened then instead of sending micro checkpoint, full checkpoint is sent to keep the call data on active and standby chassis synchronized. But this introduces lot of performance overhead and thereby causing performance impact on both the active and standby chassis.

In order to reduce the performance impact, the control events having smaller updates resulting in full checkpoints are targeted for micro checkpoint conversion. That is, the full checkpoints in case of internal and external triggers are converted to micro checkpoints.

**CSCuj56588, CSCum66195 - Need to support NAS-Port-Id in Access-Request**

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

**Feature Changes**

**Support for NAS-Port-ID Attribute**

**Previous Behavior:** NAS-Port-Id attribute was never sent as part of any RADIUS messages because it was not supported.

**New Behavior:** NAS-Port-Id attribute is now included in the Access-Request and Accounting-Start messages in P-GW calls. This attribute is added to the RADIUS dictionary “starent”, and is disabled by default. If the attribute needs to be enabled, the same can be done by using the CLI command “radius attribute accounting nas-port-id” or “radius attribute authentication nas-port-id” in AAA Server Group Configuration mode.

**Customer Impact:** If the customer does not have P-GW session licence, there will not be any impact, as the CLI will not be visible and this attribute will not be sent in the RADIUS messages.

Existing customers with P-GW session license who use starent dictionary or a custom dictionary which encompasses starent dictionary will not have any impact. The `radius attribute` CLI command should be configured to enable the NAS-Port-Id attribute to be sent in RADIUS messages.

**Command Changes**

`radius attribute accounting

`nas-port-id` is a new keyword in this command to enable the NAS-Port-Id accounting attribute to be sent in RADIUS Access-Request and Accounting-Start messages.

`configure
c

context context_name

aaa group group_name

[ no ] radius attribute accounting nas-port-id

default radius attribute accounting
end

Notes:
• **nas-port-id** – Enables NAS-Port-Id accounting attribute, if it is supported in the configured RADIUS dictionary.

**radius attribute authentication**

**nas-port-id** is a new keyword in this command to enable the NAS-Port-Id authentication attribute to be sent in RADIUS authentication messages.

```bash
configure
    context context_name
    aaa group group_name
        [ no ] radius attribute authentication nas-port-id
    default radius attribute authentication
end
```

Notes:

• **nas-port-id** – Enables NAS-Port-Id authentication attribute, if it is supported in the configured RADIUS dictionary.

### CSCul26482 - Remaining-Service-Unit AVP not sent -FUI-Redirect and Granted units zero

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

**Feature Changes**

#### Encoding of SN-Remaining-Service-Unit AVP for Final Reporting

The Starent-specific AVP “SN-Remaining-Service-Unit” behavior is inherited from “Used-Service-Unit” AVP. This Final-Reporting is missing for the Remaining-Service-Unit AVP, which is now incorporated.

**Previous Behavior:** The AVP “SN-Remaining-Service-Unit” was not sent in the CCR-T and CCR-U messages with reporting Reason FINAL when the FUI action was received as Redirect and the granted units was zero in CCA.

**New Behavior:** For the Final-Reporting, the AVP “SN-Remaining-Service-Unit” will be encoded.

### CSCul77461 - aaaproxy in warn state during customer call model run

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

**Feature Changes**

#### Limited GTPP Group Configuration
The AAA proxy allocates a lot of memory on a per GTPP group basis statically regardless of the usage. So if the number of GTPP groups is reduced to around 6 then the issue with the AAA proxy going to warn memory state will not be observed.

**Previous Behavior:** Up to a maximum of 32 GTPP groups were allowed to be configured.

**New Behavior:** Now there is a limit of configuring only up to six GTPP groups. In case customers are using more than six GTPP groups, the AAAProxy will use more memory than is supported and will be in “warn” state of memory.

**Customer Impact:** On an analysis, it is determined that customers have not yet exceeded a maximum of six GTPP groups in the configuration. With the reduction in the number of GTPP groups configured, there will no CDR loss as CDRs are archived in AAA manager when AAA proxy goes to warn state.

**Command Changes**

gtp group

This CLI command allows the user to configure only up to six GTPP groups.

```
configure
  context context_name
    apn apn_name
      gtpp group group_name [ accounting-context ac_context_name ]
    default gtpp group
    no gtpp group group_name
  end
```

**CSCul98917, CSCum70480, CSCum36649, CSCum36659, CSCuo59964 - Support for Gx Sync after Session or Message Loss**

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

**Feature Changes**

**Support for Session Recovery and Session Sync**

Currently PCRF and ASR5K gateway node are in sync during normal scenarios and when Gx assume positive is not applied. However, there are potential scenarios where the PCRF might have been locally deleted or lost the Gx session information and it is also possible that due to the loss of message, gateway node and PCRF can be out of sync on the session state.

While these are rare conditions in the network, the desired behavior is to have PCRF recover the Gx session when it is lost and also to have PCRF and gateway sync the rule and session information. This feature provides functionality to ensure PCRF and gateway can sync on session information and recover any lost Gx sessions. Configuration support has been provided to enable session recovery and session sync features. Dynamic dictionaries also support the Gx session sync feature.
**Previous Behavior:**

- If the PCRF deletes or loses session information during a Gx session update (CCR-U) initiated by the gateway, PCRF will respond back with DIAMETER_UNKNOWN_SESSION_ID resulting in session termination even in the case of CCR-U.
- If the PCRF deletes or loses session information and an Rx message is received, PCRF will not be able to implement corresponding rules and will result in failure of subscriber voice or video calls.
- For subscriber’s existing Rx sessions and active voice/video calls, PCRF will not be able to initiate cleanup of the sessions towards the gateway and can result in wastage of the resources in the network (dedicated bearers not removed) or can result in subscriber not able to place calls on hold or conference or remove calls from hold.
- For out of sync scenarios, PCRF and gateway could be implementing different policies and can result in wastage of resources or in poor subscriber experience. Existing behavior does not provide for a way to sync the entire session information.

**New Behavior:** The gateway node and PCRF now supports the ability to exchange session information and GW provides the complete subscriber session information to enable PCRF to build the session state. This will prevent the occurrence of the above mentioned scenarios and ensure that GW and PCRF are always in sync. In order to support Gx sync, two new keywords are added to the `diameter encode-supported-features` command.

**Command Changes**

```
diameter encode-supported-features
```

Two new keywords are added in this command to enable the Session Recovery and Session Sync feature. When this feature is enabled, gateway node and PCRF will exchange session information and the gateway provides the complete subscriber session information to enable PCRF to build the session state.

```
configure

context context_name

  ims-auth-service service_name

  policy control

    diameter encode-supported-features { session-recovery | session-sync }

    { default | no } diameter encode-supported-features

end
```

**Performance Indicator Changes**

**Diameter Schema**

The following bulkstatistic variables are new in this schema to support Session Recovery and Session Sync feature.

- `read-sdr`
- `read-sdr-err`
- `write-sda`
• write-sda-err
• sess-not-found

**DPCA Schema**

The following bulkstatistic variables are new in this schema to support Session Recovery and Session Sync feature.

• sync-req-cca-rcvd
• sync-req-rar-rcvd
• sync-req-ccr-sent
• rcvry-req-cca-rcvd
• rcvry-req-ccr-sent

**IMSA Schema**

The following bulkstatistic variables are new in this schema to support Session Recovery and Session Sync feature.

• dpca-imsa-session-recovery
• dpca-imsa-session-sync
• dpca-imsa-sync-req-ccarcvd
• dpca-imsa-sync-req-rar-rcvd
• dpca-expres-sess-rcvry-req

**show diameter statistics proxy**

The output of this CLI command “`show diameter statistics proxy`” is enhanced to display the number of SDR read success, number of SDR read failures, number of SDR write success, number of SDR write errors and number of requests received to recover the session but the session is not found.

The following fields are new in this release:

- Session Discovery Request and Answer Statistics
  - Read SDRs
  - Read SDR Errors
  - Write SDAs
  - Write SDA Errors
  - Session Not Found

**show ims-authorization service name**

The output of this CLI command “`show ims-authorization service name`” is enhanced to display the new features “Session Recovery” and “Session Sync”.

**show ims-authorization service statistics**

The output of this CLI command “`show ims-authorization service statistics`” is enhanced to display the number of CCR-Us sent for Session Recovery and Session Sync.
The following fields are newly added under “Re-Authorization Triggers”:

- Session Recovery
- Session Sync

**show ims-authorization policy-control statistics**

The output of this CLI command “show ims-authorization policy-control statistics” is enhanced to display the number of times session recovery request experimental result code is received from PCRF and the number of RARs/CCAs in which the session sync request is received.

The following field is newly added under “DPCA Experimental Result Code Stats”:

- Session Recovery Req

The following fields are new in this release:

- Session Sync Request Stats
  - RAR
  - CCA

**show ims-authorization policy-control statistics service service_name**

The output of this CLI command “show ims-authorization policy-control statistics service <service_name>” is enhanced to display the number of session recovery requests received in CCA and subsequent CCR updates sent, number of session sync requests received in RAR/CCA and subsequent CCR updates sent.

The following fields are new in this release:

- Session Recovery Request
  - CCA rcvd
  - CCR sent
- Session Sync Request
  - RAR rcvd
  - CCA rcvd
  - CCR sent

**CSCum14422 - S6b: Support for 2014 4G S6b Spec**

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

**Feature Changes**

**Support for 2014 4G S6b Spec**

**Previous Behavior:** Starent-Subscriber-Permission AVP is seen in AAA message with the value configured.

**New Behavior:** As per the 2014 4G S6b specification, the AVP “Starent-Subscriber-Permission” can only take value 0x20 (Network Mobility). If this AVP is set to any value other than 0x20, the gateway node rejects this message and terminates the session.
Also, a new AVP “Restoration-Priority” is included in AAA message and sent over S6b interface.

**CSCum17342 - Support is not required for following AVP's in WLAN Rf message**

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

**Feature Changes**

**AVP Support for WLAN Rf Calls**

- **Previous Behavior:** In the case of aaa-custom4 dictionary, the 3GPP-MS-TimeZone, 3GPP-User-Location-Info, and 3GPP2-BSID AVPs were sent for WLAN call.
- **New Behavior:** As per the latest customer-specific Rf specification, these AVPs are not being expected in Rf messages; hence these AVPs will not be sent for WLAN call for aaa-custom4 dictionary.

**CSCum17434, CSCum14422,CSCum24018 - AAA provide Restoration Priority Indicator to PGW**

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

**Feature Changes**

**Support for Restoration Priority Indicator**

To distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections, the gateway will now support receiving a new AVP “Restoration-Priority-Indicator” from AAA server over the S6b interface. The gateway will be able to provide KPIs based on the AVP value.

**Important:** Restoration-Priority-Indicator is applicable only for IMS PDN and will be used only to determine the relative restoration priority among PDN connections to the IMS APN.

**Customer Impact:** The customer will now be able differentiate the VoLTE subscriber from non-VoLTE subscriber based on the value of “Restoration Priority Indicator” AVP.

**CSCum36863 - Support webauth changes in Samog Radius dictionary**

**Applicable Products:** SaMOG

**Feature Changes**

**New RADIUS Dictionary for Supporting Web Authorization Feature**
A new RADIUS dictionary “custom71” is created to support the attribute “CS-AVPair” required as part of Web Authorization feature for SaMOG. In addition to custom71, custom72 to custom75 are also defined and reserved for future use.

**Command Changes**

```plaintext
radius dictionary

Keywords “custom71” to “custom75” are added to this command to define new RADIUS dictionaries for future use.

configure

  context context_name

    aaa group group_name

    radius dictionary { custom71 | custom72 | custom73 | custom74 | custom75 }

    default radius dictionary

end
```

Notes:
- custom71 is defined for Web Authorization feature for SaMOG. The other new custom dictionaries are reserved for future use.

**CSCum37008 - Radius based GTPv2 access support**

**Applicable Products:** SaMOG

**Feature Changes**

**New RADIUS Dictionary for Supporting CS-AVPair Attribute in RADIUS Access-Accept**

A new RADIUS dictionary “custom71” has been defined similar to custom70 and configured with an additional RADIUS attribute “CS-AVPair”. This attribute will be sent in the RADIUS Access-Accept message from SaMOG to WLC.

This attribute will be used to send MIP6-Feature-Vector, MIP-Home-Agent-Host, DEA-Flags, APN-OI-Replacement.

**CSCum41224 - Diameter Support for MME Node Restoration**

**Applicable Products:** MME

**Feature Changes**

**AVP Support for MME Node Restoration**
In support of MME Node Restoration feature, a new AVP “Restoration-Priority” is now encoded and sent over S6a interface as per the 3GPP spec 29.272, Release 11.

**CSCum52650 - IMSA Support for Over ride Control feature**

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

**Feature Changes**

**Custom AVPs for Override Control Feature**

As per the standards PCRF cannot modify policy/charging parameters of predefined/static policies. It can enable/disable the rules dynamically from PCRF. In order to modify the Charging/Policy parameters from PCRF, a new custom AVP “Override-Control” is defined on the Gx interface. This AVP is used to enable the PCRF to override charging and policy parameters for a specified set of rules or charging actions. Override Control is a set of AVPs received from PCRF.

**Important:** Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

As part of the Override Control feature, the override may be applied at a rule level, at a charging action level, and/or at wild card level. This AVP may be present more than once if override at rule level and charging action level are to be sent in the same message.

**CSCum54804 - STa support for webauth users**

**Applicable Products:** SaMOG

**Feature Changes**

**Extended AVP Support for STa Interface for Web Authorization**

The Diameter STa dictionary for SaMOG now includes the following AVPs in AAA message:

- Filter-Id – String type AVP that contains the name of ACL rule that is to be applied by SaMOG
- SN1-Rulebase – String type AVP that contains the name of ECS rule that is to be applied by SaMOG
- Framed-Pool – String type AVP that contains the name of IP pool to be used to be SaMOG for allocating UE IP
- SN1-VPN-Name – String type, which contains the name of the context in SaMOG where IP pool is defined.
- SN1-Primary-DNS-Server – IP address of DNS server to be conveyed to UE
- SN1-Secondary-DNS-Server – IP address of DNS server to be conveyed to UE

The STa dictionary for SaMOG has further been enhanced to include 3GPP-IMSI AVP in ASR message.
CSCum57172 - Radius messages should carry Framed-IPv6-Prefix in auth/acct requests

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

Feature Changes

Support for Framed-IPv6-Prefix in RADIUS Messages

It is confirmed that the Framed-IPv6-Prefix is supported in RADIUS authentication and accounting request messages for custom9 RADIUS dictionary.

CSCum59592 - SLg Interface - Include MSISDN AVP in procedures

Applicable Products: MME

Feature Changes

Support for MSISDV AVP on SLg Interface

This feature is required for SLg interface to implement MSISDN and IMEI based mapping along with existing IMSI based mapping in diamproxy.

If only MSISDN AVP is received from server with PLR in SLg interface, then lookup is performed and the message is forwarded to correct session manager based on MSISDN.

CSCum65582 - Customer CDMA migration - PDSN Gy dictionary

Applicable Products: HA, PDSN

Feature Changes

Support for Standard Gy Dictionary on PDSN

A 3GPP release 8 compliant standard Gy dictionary is defined for PDSN. This dictionary is required as part of CDMA migration to Cisco.

CSCum65600 - Diameter CCR-U reporting: tigger events based counters

Applicable Products: GGSN, P-GW

Feature Changes

Statistics Support for CC Update Reporting Reasons
It has been verified that CCR Update Reporting Reason statistics are available as part of “show active-charging credit-control statistics” command. These statistics indicate which event triggers are responsible for Interim Diameter update messages (CCR-update).

The corresponding bulkstatistics support is also available in the DCCA Group schema.

**CSCum65709, CSCum67960 - Gy support for Accelerated ECS - Phase2**

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

**Feature Changes**

**Gy Support for Flow Aware Packet Acceleration Feature**

The “show active-charging sessions full” command will be updated to display if the MCC supports acceleration. The Accelerated status of MCC will only be visible if the chassis has license for the Flow Aware Packet Acceleration (FAPA) feature.

**Performance Indicator Changes**

**show active-charging sessions full**

The following field is newly added to the output of this show command to indicate whether or not the MCC supports acceleration.

- Accelerated

**CSCum67205 - [S6a/S6d] AVP support for MTC feature**

**Applicable Products:** MME, SGSN

**Feature Changes**

**Support for AVPs for MTC Feature**

MME and SGSN will now use the following AVPs to support MTC feature.

- Subscribed-Periodic-RAU-TAU-Timer –This AVP contains the subscribed periodic TAU/RAU timer value in seconds, that will be used as an indication to decide for allocating a locally configured periodic RAU/TAU timer value to the UE.

- Subscribed-Periodic-RAU-TAU-Timer-Withdrawal flag in DSR Flags AVP – This bit, when set, indicates that the subscribed periodic RAU TAU Timer value will be deleted from the subscriber data.

**CSCum67557 - PGW selection of Gx interface based on APN**

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

Selection of Gx Interface based on APN

It is confirmed that P-GW allows selection of different Gx Primary/Secondary connections for different APNs.

CSCum67660 - Configurable dictionaries on Diameter interfaces

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

Feature Changes

Dynamically Configurable Dictionaries on Diameter Interfaces

Diameter dictionaries need frequent customization primarily due to the difference in the interpretation of the standards and any new customized features as required. As the Diameter dictionaries are statically defined for each interface and for each operator separately, the turn around time to customize these dictionaries is high. Hence, a new Dynamic Dictionary framework has been introduced. This will facilitate creation of a new Diameter dictionary in ABNF encoding format which is a readable text file and loading it to the chassis using a new CLI. Then, apply this dictionary to any application which talks to external Diameter servers such as PCRF, OCS and AAA servers. Dynamic dictionary support also exists for all Diameter - AAA interfaces. MME/SGSN - HSS Diameter interfaces like S6a and S6d are not supported in this release.

**Important:** It is highly necessary that you must not create dynamic dictionary for your customization needs. Contact your Cisco account representative for any new dynamic dictionary creation request.

It has been confirmed that the Diameter dictionaries can be dynamically configured on various Diameter interfaces like Gx, Gy, etc.

CSCum69764 - CCR-u & CCR-f routing enhancement for Customer RDR

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

Feature Changes

CCR Routing Enhancement

In a scenario where a PCEF is connected to OCS via multiple Diameter proxies, PCEF chooses the same Diameter proxy for the subsequent messages as long as it is available.

Any subsequent messages (CCR-U/CCR-T) to the same host are sent via the same peer. Once the next-hop is chosen via round-robin method, the subsequent message for the session is sent to the same next-hop (peer).
CSCum75446, CSCum20550, CSCum36649, CSCum36659 - Support for FUA in Local Policy

Applicable Products: P-GW, SAEGW

Feature Changes

Support for FUA in Local Policy

Local Policy is used as an option to fallback when there is a failure with PCRF. Local Policy supports Out-Of-Credit/Reallocation-of-Credit and can install different policies for these event-triggers. In this release, Local Policy Engine is enhanced to include Final-Unit-Action (FUA) and Filter ID as two parameters based on which different policies can be pushed.

**Important:** This feature will be active only when Gx Assume Positive is active.

On reconnect to server event, P-GW will send the status of current active rules to PCRF. Operator could enable more use cases with Local Policy even if PCRF connection is lost.

Command Changes

```
class condition

final-unit-action is a new keyword in this command to allow configuring different filter IDs and different FUA actions for the events like out-of-credit, etc.

configure

local-policy-service service_name

ruledef ruledef_name

condition priority priority final-unit-action [ eq | ge | gt | le | lt | match | ne | nomatch ] [ terminate | redirect | restrict-access ]+ [ filter-id ] [ eq | ge | gt | le | lt | match | ne | nomatch ] filter-id

no condition priority priority

don
```

Notes:

- When the Final-Unit-Action (FUA) received from the session manager during out-of-credit scenario matches with the configured FUA, then one of the following actions will be taken. If the filter-id is configured, then at least one filter-id should be matched.
  - **redirect:** Redirects the service
  - **restrict-access:** Restricts the service
  - **terminate:** Terminates the service
• *filter-id:* This variable denotes the name of the filter list for the user. *filter-id* is a string of 1 through 128 characters. Note that `match`, `nomatch`, `ne`, and `eq` are more appropriate operators though other values can also be used. Wild card values can be specified for string match.

**Performance Indicator Changes**

**show local-policy statistics all**

The following new field has been introduced as part of this feature enhancement to support FUA in local policy.

- Final Unit Action

**CSCum76157, CSCul98934, CSCum36329, CSCum17342 - 2014 Customer Network Upgrade**

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

**Feature Changes**

**4G Network Upgrade 3GPP Standard Baseline Release Compliance**

As part of the 2014 4G network upgrade, the following requirements are supported:

- Session Release Cause in CCA-U messages
- 3GPP Standard based Pending Transaction Support

**Session Release Cause in CCA-U messages**

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages.

In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

**Support for Pending Transaction per 3GPP Standards**

The following changes are implemented:

- Support for Negotiation of PT in initial session establishment.
- Support for receiving/sending 4144 with 3GPP Vendor ID in CCA/RAA.
- Retry of CCR-U when 4144 is received from PCRF.
- No Support for 4198 with Proprietary Vendor ID.
- Recovery of negotiated Supported features.

**Performance Indicator Changes**

**IMSA Schema**

The following bulkstat variables are modified in this release:
• dpca-insuffcnt-srvr-resrce — changed as dpca-rar-insuffcnt-srvr-resrce
• dpca-ue-subscription-chngd — changed as dpca-rar-ue-subscription-chngd
• dpca-unknown-reason — changed as dpca-rar-unknown-reason

The following bulkstat variables are new in this release:
• dpca-cca-insuffcnt-srvr-resrce
• dpca-cca-ue-subscription-chngd
• dpca-cca-unknown-reason

**show ims-authorization policy-control statistics**

The following fields are grouped under RAR message:
• RAR
  • Unspecified Reason
  • UE Subscription Changed
  • Insuffcnt Srvr Resource

The following fields are newly added under CCA message:
• CCA
  • Unspecified Reason
  • UE Subscription Changed
  • Insuffcnt Srvr Resource

**CSCum76162, CSCum65446, CSCum87983 - Rf and Gy checkpoint synchronization**

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

**Feature Changes**

**Support for Rf and Gy Checkpoint Synchronization**

Rf and Gy check-pointing are handled by different internal processes. The Rf billing is handled by the AAAMgr, while the Gy billing is handled through the ACSMgr which is part of the SessMgr. Both these processes are separate and are check-pointed by the system at different instances with no correlation done to ensure they are reporting the same values.

This feature implements a common timer based approach for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing.

Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.
CSCum76201, CSCum65453 - Configurable Rf Containers triggered off of Gy events

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

Feature Changes

Configurable Rf Containers for Gy Events

This feature allows an Rf trigger to be generated for each of the Gy reporting reasons/events:

- FINAL
- QUOTA_EXHAUSTED
- VALIDITY_TIME
- OTHER_QUOTA_TYPE
- RATING_CONDITION_CHANGE
- FORCED_REAUTHORISATION
- QUOTA_HOLD_TIME
- THRESHOLD

New change-conditions are added at Rf to support the events. Also, new event triggers are added at Rf to support the events.

Previous Behavior: Gy used to trigger ACR-I immediately or containers were cached based on Policy Accounting Configuration, after triggering CCR-U and was not waiting for CCA-U.

New Behavior: In this release, containers will be closed only after CCA-U was received successfully. The new behavior is to cache the containers and not to generate interims immediately for all the new Gy event triggers configured. This is achieved through the use of a new CLI command “`gy-rf-trigger-type`” in Credit Control Group Configuration mode.

Also, the current behavior of cutting and sending an ACR is changed to caching a container and not sending the ACR until the configured threshold is passed.

This behavior of waiting for response before closing the containers is limited only to CCR-U and ACR-Is and ACR-Stop will be triggered immediately after CCR-T is sent.

Customer Impact: Customers should not use the existing CLI command “`trigger-type`” under Accounting Policy accounting configuration along with the newly added CLI command “`gy-rf-trigger-type`” in Credit Control Configuration mode.

Command Changes

`gy-rf-trigger-type`

This is a new command to enable Gy event triggers for generation of matching Rf ACR containers.

`configure`

`require active-charging`
active-charging service service_name

credit control

gy-rf-trigger-type { final | forced-reauthorization | holding-time | quota-exhausted | rating-condition-change | threshold | validity-time }

{ default | no } gy-rf-trigger-type

diagnostic

Notes:
- The CLI command “gy-rf-trigger-type” is applicable only for CCR-U and not CCR-T.

CSCum87203 - Customer CDMA - Gx dictionary on PDSN

Applicable Products: HA, PDSN

Feature Changes

Support for Standard Gx Dictionary on PDSN

A standard Gx dictionary “r8-standard-gx” is defined for PDSN. This dictionary is required as part of CDMA migration to Cisco.

CSCun65005, CSCun65020, CSCup75403 - PGW/SAEGW: Network Provided Location Info (NPLI) for IMS.

Applicable Products: GGSN, MME, P-GW, SAEGW, S-GW

Feature Changes

Reporting of NPLI over Gx

A new feature “netloc” (feature bit 10) has been added as part of the Supported-Features AVP to implement the Network Provided Location Information (NPLI) feature for IMS. NPLI is used to support variety of applications like emergency call, Lawful intercept, charging, etc.

Important: NPLI is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

The NetLoc feature indicates the support for reporting of the Access Network Information. The netloc feature bit will be sent to PCRF on demand via CCR-I message. A new event trigger “ACCESS_NETWORK_INFO_REPORT (45)” and a new Diameter AVP “Required-Access-Info” have been added to support the NPLI enhancement.
Previous Behavior: The gateway node used to convey access network information (e.g. user location and/or user time zone information) to PCRF through ECS-IMSA only during session establishment or whenever any of these information are modified/updated.

New Behavior: As part of this feature, Application Function (AF) can request the PCRF to report the access network information, and if requested the gateway node has to provide this access network information to PCRF even though it has not changed.

The gateway node provides the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP. The gateway also provides the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

PCRF will use event trigger “ACCESS_NETWORK_INFO_REPORT(45)” to request this information from the gateway along with “Required-Access-Info” AVP.

Command Changes

diameter encode-supported-features

netloc is a new keyword in this command to enable the NetLoc feature. When this feature is enabled, the gateway node sends the netloc feature bit to PCRF on demand via CCR-I message.

configure

context context_name

ims-auth-service service_name

policy control

diameter encode-supported-features netloc

{ default | no } diameter encode-supported-features

end

Notes:
• netloc keyword is visible only when the corresponding feature license is installed.

Performance Indicator Changes

IMSA Schema

The following bulkstat variable is newly added in this schema.

• dpca-imsa-access-nw-info-report

show ims-authorization service name

As part of the NPLI feature enhancement, the following are the changes to the fields in the output of this show command.

• net-loc – Displayed as part of the “Supported Features” field if configured
• Access-Network-Info-Report – Displayed for “Reauth Trigger” field if the corresponding trigger is configured
show ims-authorization sessions full all

As part of the NPLI feature enhancement, the following change is observed for the field “Event Triggers” in the output of this show command.

- Access-Network-Info-Report – Displayed for “Event Triggers” field if the corresponding trigger is configured

show ims-authorization service statistics all

As part of the NPLI feature enhancement, the following field is newly added under “Re-Authorization Triggers” in this show command output.

- Access Network Info Report

**CSCun75893, CSCui96079 - Support for Volume Reporting in Local Policy**

*Applicable Products: P-GW, SAEGW*

**Feature Changes**

**Support for Volume Reporting in Local Policy**

This feature provides support for time based reconnect to PCRF instead of the event based for CCR-U failure scenarios.

**Previous Behavior:** The following behaviors were observed with respect to the Volume Reporting for Local Policy:

- In the event of CCR-U failure, CCR-U was triggered to PCRF only on receiving subscriber event.
- When a CCR-U failure happened and a call continued without Gx, unreported volume is lost as the threshold is set to infinity. In next CCR-U triggered to PCRF, the cumulative volume was sent to PCRF.
- RAR was rejected with result-code diameter_unable_to_comply (3002) when the validity timer is running.

**New Behavior:** With the timer-based implementation, this feature introduces the following changes to the existing behavior:

- When send-usage-report is configured, the CCR-U with usage report will be sent immediately after the local-policy timer-expiry.
- The unreported usage will not be returned to ECS. Thus, usage since last tried CCR-U will be sent to PCRF.
- RAR will be accepted and the rules received on RAR will be installed even when the timer is running.

**Customer Impact:** Session can be connected to PCRF immediately instead of waiting for subscriber event, and the updated usage report can be sent.

**Command Changes**

**action priority**

`send-usage-report` is a new keyword in this command to send CCR-U along with volume report immediately.

**configure**

```
local-policy-service service_name
```
**Action Definition**

```plaintext
actiondef actiondef_name

  action priority priority { reconnect-to-server [ send-usage-report ] }

  no action priority priority

end
```

**Notes:**

- `send-usage-report`: Triggers CCR-U with volume report immediately. The default behavior is that the CCR-U will not be triggered immediately.

---

**CSCuo31658 - Sending Rule report during reconnect to pcrf**

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

**Feature Changes**

**Updated Rule Report During PCRF Reconnect**

**Previous Behavior:** Rule report was not sent in the CCR messages when PCRF is retried after the expiry of validity timer.

**New Behavior:** Rule report will be sent to the PCRF during reconnect when the CLI command `diameter encode-event-avps local-fallback` is configured under Policy Control Configuration mode.

**Customer Impact:** Customers can now see the updated rule report.

---

**CSCup01650 - Unreported usage should not be reported back to acs.**

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

**Feature Changes**

**Customized Processing of Unreported Volume**

**Previous Behavior:** Unreported usage was reported back to ACS manager when the CCR message failed and the failure handling was set to continue action.

**New Behavior:** Unreported volume will not be sent to ACS manager for dpca-custom15 dictionary alone as the customer needs only the difference of the volume and not the cumulative volume.

---

**CSCup08773 - Support for Session Rel Cause in all dictionaries.**

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

Support for Session Release Cause in Gx Dictionaries

**Previous Behavior:** Session-Release-Cause AVP was earlier supported in CCA-U message only for standard Gx dictionaries and a few customer specific Gx dictionaries.

**New Behavior:** Now, the support for Session-Release-Cause AVP is extended to all the Gx dictionaries.

**Customer Impact:** If PCRF supports sending Session-Release-Cause AVP in CCA-U, P-GW will terminate the subscriber call.

CSCup09827 - Bulkstats counter not present for CCR-Event Retry

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

Performance Indicator Changes

DCCA Schema

To provide bulkstats support for the CCR-Event Retry, the following new bulk statistic variable has been added to DCCA schema.

- ccr-event-retry

DCCA Group Schema

To provide bulkstats support for the CCR-Event Retry, the following new bulk statistic variable has been added to DCCA group schema.

- cc-ccr-event-retry

CSCup31005 - [gn-gp] : 'user-equipement-info' AVP should be present in SIS RF records

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

Feature Changes

Parsing of User-Equipment-Info AVP in all Rf Records

**Previous Behavior:** User-Equipment-Info AVP was sent only in START records for all Rf dictionaries except one customer-specific Rf dictionary.

**New Behavior:** For all Rf dictionaries, the “User-Equipement-Info” AVP is now sent in all the Rf records i.e. START, INTERIM and STOP records as per the latest RF EPS 5.0 specification.
CSCup34373 - show ims-authorization policy-control statistics... show ip as 0.0.0.0

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

Feature Changes

IPV6 Address Support for Gx Server

The command “show ims-authorization policy-control statistics service <service name> server ip-address <ipv4 or ipv6 address>” now allows to display IMS authorization server information in IPv6 address notation.

Command Changes

show ims-authorization policy-control statistics service

In addition to IPV4 address, this command now accepts IPV6 address also as part of the server information.

show ims-authorization policy-control statistics service <service name> server ip-address <ipv4 or ipv6 address>

CSCup39309 - GY : Triggers not sent in CCR-U message

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

Feature Changes

RAT-Type AVP Value for EVDO and EVDO_REVA

Previous Behavior: RAT-Type AVP used to encode 0x3b for both EVDO and EVDO_REVA.

New Behavior: The EVDO_REVA calls will be having RAT-Type value 0x40 in Gy interface. The EVDO calls will continue to the same 0x3b value for RAT-Type AVP.

Customer Impact: For EVDO_REVA calls, the customer will find the RAT-Type AVP value as 0x40.

CSCup81987 - Display support for some of dcca stat values

Applicable Products: GGSN, HA, ISPG, P-GW

Performance Indicator Changes

DCCA Group Schema

The following bulkstat variable is deprecated from this release:
show active-charging credit-control statistics debug-info

The following fields are new in this release:

- ccrt_backpressure_err
- mscc_qht
- mscc_ttc
- auth_life_time
- ocs_unreachable_time
- start_envelope_tick
- stop_envelope_tick
- start_qht_timer
- stop_qht_timer
- start_ttc_timer
- stop_ttc_timer
- start_auth_life_timer
- stop_auth_life_timer
- start_ocs_unreachable_timer
- stop_ocs_unreachable_timer
- cat_nocharge
- cca_err_unanswered

The following field has been removed from active charging DCCA stats:

- rep_reason_titsu_time

CSCuq37530 - RAA/ASA not received when OCS sends RAR/ASR for an Offline Session

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

Feature Changes

Parsing of RAA and ASA for Offline Charging Session

Previous Behavior: When a DCCA session goes offline, and OCS sends the RAR/ASR, those messages are ignored.

New Behavior: RAA/ASA will be sent along with 5002 unknown session id result code for an offline charging session on receiving RAR/ASR from server.
CSCuq53616 - Support for sending Event Timestamp in CCR Initial

Applicable Products: GGSN, P-GW

Feature Changes

Event-Timestamp AVP in CCR-I

Event-Timestamp AVP will be sent in the CCR-I message for dpca-custom8 dictionary. This AVP indicates the call arrival time i.e. the time stamp of session creation on Gx Interface.

Customer Impact: Customer will know the time at which call landed on the gateway node.
Chapter 2
ADC Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from ADC in StarOS 17 software releases.
ADC Enhancements for 17.5

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.

---

**CSCuu71291 - Develop rule matching capability for ssl sni feature**

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

**Related IDs:** CSCuu67445, CSCuu71216, CSCuu71264, CSCuu71316, CSCuv37026, CSCuv64469, CSCuv65109, CSCuv76197, CSCuv88857

---

**Feature Changes**

**SNI Detection Support**

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.

---

**Important:** The SNI Detection feature requires a valid Application Detection and Control license. Contact your Cisco Account representative for more information.

**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.
ADC Enhancements for 17.0

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.

**CSCue79102 - Skypeout detection required**

**Feature Changes**

**Support for Voipout Sub-classification**

A new sub-classification “voipout” for applications/protocols is supported in this plugin release in addition to other supported sub-classifications — Audio, File Transfer, IM, Video and Unclassified.

**Important:** The Voipout sub classification is available only when the plugin is installed in 16.2 and later releases.

**Previous Behavior:** Skypeout traffic was classified as Skype-audio for releases prior to 16.2.

**New Behavior:** Skypeout traffic will be detected as “voipout” sub-classification of Skype application.

**Command Changes**

```
 edr p2p
```

In this release, “voipout-end” is a new event added for `p2p_event_list` to support detection of the Skypeout calls of Skype application.

```
configure

 rulebase rulebase_name

      edr p2p p2p_event_list [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] +

      { default | no } edr p2p p2p_event_list

 end
```

Notes:
- The ADC Plugin supports the “voipout-end” event in addition to “audio-end” and “video-end” events.

**p2p traffic-type**

In this release, voipout is a new keyword in this command to support detection of the Skypeout calls of Skype application.

```plaintext
configure

ruledef ruledef_name

[ no ] p2p traffic-type operator voipout

end
```

Notes:
- `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

**show active-charging analyzer statistics name**

In this release, voipout is a new keyword in this command to support detection of the Skypeout calls of Skype application.

```plaintext
show active-charging analyzer statistics name p2p duration voipout
```

### Performance Indicator Changes

**show active-charging analyzer statistics name p2p verbose**

In support of the new voipout sub-classification, the following new fields are added:
- Skype voipout
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts

**show active-charging analyzer sessions summary**

In support of the new voipout sub-classification, the following new field is added:
- Current skype voipout Sessions

**show active-charging analyzer sessions summary type p2p**

In support of the new voipout sub-classification, the following new field is added:
- Current skype voipout Sessions
CSCUl82665 - Support for Kik messenger in p2p plugin

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

Feature Changes

Support for Kik Messenger Application Detection

With this release, the support for detection of traffic originating from the Kik Messenger application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols.
With this release, the kik-messenger keyword is added to this command:

```
configure
  active-charging service service_name
    [ no ] p2p-detection protocol kik-messenger
  end
```

p2p protocol

This command enables detection of specific P2P protocols for charging purposes.
With this release, the Kik Messenger protocol is supported.

```
configure
  active-charging service service_name
    ruledef ruledef_name
      [ no ] p2p protocol = kik-messenger
    end
  end
```

clear active-charging analyzer statistics

A new keyword kik-messenger is added to this command to clear the analyzer statistics of the Kik Messenger protocol.

```
clear active-charging analyzer statistics name p2p application kik-messenger
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the kik-messenger keyword is added to the P2P list:
show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the **kik-messenger** keyword is added to the P2P list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the **kik-messenger** keyword is added to the P2P list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for **kik-messenger** as part of the plugin. If detection of the Kik Messenger P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-kik-messenger-group
- p2p-kik-messenger-uplnk-bytes
- p2p-kik-messenger-dwlnk-bytes
- p2p-kik-messenger-uplnk-pkts
- p2p-kik-messenger-dwlnk-pkts
- p2p-kik-messenger-duration

show active-charging analyzer statistics name p2p

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.
With this release, the following fields have been added to the output of this command:

- Kik-messenger:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging analyzer statistics name p2p protocol-group verbose

With this release, the following fields have been added to the output of this command:
• Communicator-kik-messenger:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

• Current kik-messenger Sessions

**CSCum56566 - P2P performance optimization - impact to be less than 10%**

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

**Feature Changes**

**ADC Performance Optimization**

In this release, performance overhead of the ADC component is optimized to improve the performance. Integration of ADC with A-ECS framework will help in further optimization of ADC.

---

**Important:** CSCuq09162 is an unresolved issue in ASR5500 that is being tracked for this enhancement.

**CSCum56575 - P2P to be integrated and optimized with A-ECS effort**

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

**Feature Changes**

**Interworking of ADC and A-ECS**

Accelerated-ECS feature speeds up the processing of certain types of flows such that the packet-actions and charging applicable to packets from those flows is done in a fast manner. The throughput in terms of PPS (Packets Processed per Second) is improved by caching rule matching results for a flow for selected flows so as not to incur the lookup penalty for a large number of packets in that flow.

In this release, P2P flows will be optimized and accelerated using A-ECS. ADC when enabled with A-ECS improves P2P performance considerably.

*Previous Behavior:* P2P flows are not accelerated by A-ECS.

*New Behavior:* P2P flows are accelerated by A-ECS. Accelerated packet count is added in P2P analyzer statistics.
**Important:** A-ECS accelerates P2P flows for most P2P protocols except for the protocols/apps listed below. A-ECS works partially or does not work for some protocols.

- Bittorrent
- Edonkey
- Winny
- Soulseek
- Zattoo
- Ares
- DirectConnect
- PPlive
- Iskoot
- Thunder
- Tunnelvoice
- Scydo
- ThunderHS
- Blackberry

**Command Changes**

```
show active-charging analyzer statistics
```

The `wide [ all ]` keyword is added to this command to displays all available P2P statistics in a single wide line, and also to display the accelerated packet count. The `all` keyword displays all available P2P statistics without suppressing zeroes.

```
show active-charging analyzer statistics [ name p2p [ application p2p-list | protocol-group group_list | duration [ audio | video ] ] [ wide [ all ] ]]
```

**CSCup36140 - Support for telegram in ADC**

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

**Feature Changes**

**Support for Telegram Application Detection**

With this release, the support for detection of traffic originating from the Telegram application is added.
Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols. With this release, the **telegram** keyword is added to this command:

```
configure
active-charging service service_name
   [ no ] p2p-detection protocol telegram
end
```

p2p protocol

This command enables detection of specific P2P protocols for charging purposes. With this release, the Telegram protocol is supported.

```
configure
active-charging service service_name
    ruledef ruledef_name
    [ no ] p2p protocol = telegram
end
```

clear active-charging analyzer statistics

A new keyword **telegram** is added to this command to clear the analyzer statistics of the Telegram protocol.

```
clear active-charging analyzer statistics name p2p application telegram
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the **telegram** keyword is added to the P2P list:

```
show active-charging analyzer statistics name p2p application p2p_list
```

show active-charging flows type p2p

This command displays the information for the active charging flows. With this release, the **telegram** keyword is added to the P2P list:

```
show active-charging flows type p2p application p2p_list
```

show active-charging sessions summary
This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the **telegram** keyword is added to the P2P list:

```
show active-charging sessions summary type p2p application p2p_list
```

### Performance Indicator Changes

#### P2P Schema

New ADC bulk statistics are available in the P2P schema for **telegram** as part of the plugin. If detection of the Telegram P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-telegram-group
- p2p-telegram-uplnk-bytes
- p2p-telegram-dwlnk-bytes
- p2p-telegram-uplnk-pkts
- p2p-telegram-dwlnk-pkts
- p2p-telegram-duration

```
show active-charging analyzer statistics name p2p
```

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Telegram:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

```
show active-charging analyzer statistics name p2p protocol-group verbose
```

With this release, the following fields have been added to the output of this command:

- E-mail-telegram:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

```
show active-charging sessions summary
```

With this release, the following fields have been added to the output of this command:
Current telegram Sessions

CSCup36151 - Support for Didi in ADC

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

Feature Changes

Support for DiDi Application Detection

With this release, the support for detection of traffic originating from the DiDi application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols. With this release, the didi keyword is added to this command:

```
configure
  active-charging service service_name
  [ no ] p2p-detection protocol didi
end
```

p2p protocol

This command enables detection of specific P2P protocols for charging purposes. With this release, the DiDi protocol is supported.

```
configure
  active-charging service service_name
  ruledef ruledef_name
    [ no ] p2p protocol = didi
end
```

clear active-charging analyzer statistics

A new keyword didi is added to this command to clear the analyzer statistics of the DiDi protocol.

```
clear active-charging analyzer statistics name p2p application didi
```

show active-charging analyzer statistics name p2p
This command displays statistical information for protocol analyzers.
With this release, the didi keyword is added to the P2P list:

```
show active-charging analyzer statistics name p2p application p2p_list
```

**show active-charging flows type p2p**

This command displays the information for the active charging flows.
With this release, the didi keyword is added to the P2P list:

```
show active-charging flows type p2p application p2p_list
```

**show active-charging sessions summary**

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the didi keyword is added to the P2P list:

```
show active-charging sessions summary type p2p application p2p_list
```

### Performance Indicator Changes

#### P2P Schema

New ADC bulk statistics are available in the P2P schema for didi as part of the plugin. If detection of the DiDi P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-didi-group
- p2p-didi-uplnk-bytes
- p2p-didi-dwlnk-bytes
- p2p-didi-uplnk-pkts
- p2p-didi-dwlnk-pkts
- p2p-didi-duration

**show active-charging analyzer statistics name p2p**

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.
With this release, the following fields have been added to the output of this command:

- Didi:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets
show active-charging analyzer statistics name p2p protocol-group verbose

With this release, the following fields have been added to the output of this command:

- Communicator-didi:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary

With this release, the following fields have been added to the output of this command:

- Current didi Sessions

CSCup66475 - ADC Support For Xing

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

Feature Changes

Support for Xing Application Detection

With this release, the support for detection of traffic originating from the Xing application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols.
With this release, the xing keyword is added to this command:

configure

  active-charging service service_name

    [ no ] p2p-detection protocol xing

end

p2p protocol

This command enables detection of specific P2P protocols for charging purposes.
With this release, the Xing protocol is supported.

configure

  active-charging service service_name
ruledef  ruledef_name

[ no ] p2p protocol = xing
end

clear active-charging analyzer statistics

A new keyword xing is added to this command to clear the analyzer statistics of the Xing protocol.
clear active-charging analyzer statistics name p2p application xing

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the xing keyword is added to the P2P list:
show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the xing keyword is added to the P2P list:
show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the xing keyword is added to the P2P list:
show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for xing as part of the plugin. If detection of the Xing P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.
The following bulk statistics are added to the P2P schema:

- p2p-xing-group
- p2p-xing-uplnk-bytes
- p2p-xing-dwlnk-bytes
- p2p-xing-uplnk-pkts
- p2p-xing-dwlnk-pkts
- p2p-xing-duration
show active-charging analyzer statistics name p2p

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Xing:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging analyzer statistics name p2p protocol-group verbose

With this release, the following fields have been added to the output of this command:

- Social-nw-generic-xing:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary

With this release, the following fields have been added to the output of this command:

- Current Xing Sessions

CSCup66488 - ADC Support For Tagged

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

Feature Changes

Support for Tagged Application Detection

With this release, the support for detection of traffic originating from the Tagged application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols.

With this release, the tagged keyword is added to this command:

configure
active-charging service service_name
  [ no ] p2p-detection protocol tagged
end

This command enables detection of specific P2P protocols for charging purposes.
With this release, the Tagged protocol is supported.

configure

active-charging service service_name
ruledef ruledef_name
  [ no ] p2p protocol = tagged
end

clear active-charging analyzer statistics
A new keyword tagged is added to this command to clear the analyzer statistics of the Tagged protocol.
clear active-charging analyzer statistics name p2p application tagged

show active-charging analyzer statistics name p2p
This command displays statistical information for protocol analyzers.
With this release, the tagged keyword is added to the P2P list:
show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p
This command displays the information for the active charging flows.
With this release, the tagged keyword is added to the P2P list:
show active-charging flows type p2p application p2p_list

show active-charging sessions summary
This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the tagged keyword is added to the P2P list:
show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema
New ADC bulk statistics are available in the P2P schema for tagged as part of the plugin. If detection of the Tagged P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-tagged-group
- p2p-tagged-uplnk-bytes
- p2p-tagged-dwlnk-bytes
- p2p-tagged-uplnk-pkts
- p2p-tagged-dwlnk-pkts
- p2p-tagged-duration

**show active-charging analyzer statistics name p2p**

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Tagged:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging analyzer statistics name p2p protocol-group verbose**

With this release, the following fields have been added to the output of this command:

- Social-nw-generic-tagged:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

- Current tagged Sessions

**CSCup66573 - ADC Support For Friendster**

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

Support for Friendster Application Detection

With this release, the support for detection of traffic originating from the Friendster application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols. With this release, the friendster keyword is added to this command:

configure

   active-charging service service_name

   [ no ] p2p-detection protocol friendster

   end

p2p protocol

This command enables detection of specific P2P protocols for charging purposes. With this release, the Friendster protocol is supported.

configure

   active-charging service service_name

   ruledef ruledef_name

   [ no ] p2p protocol = friendster

   end

clear active-charging analyzer statistics

A new keyword friendster is added to this command to clear the analyzer statistics of the Friendster protocol.

clear active-charging analyzer statistics name p2p application friendster

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the friendster keyword is added to the P2P list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the `friendster` keyword is added to the P2P list:

```
show active-charging flows type p2p application p2p_list
```

```
show active-charging sessions summary
```

This command displays statistics for Active Charging Service (ACS) sessions. With this release, the `friendster` keyword is added to the P2P list:

```
show active-charging sessions summary type p2p application p2p_list
```

### Performance Indicator Changes

#### P2P Schema

New ADC bulk statistics are available in the P2P schema for `friendster` as part of the plugin. If detection of the Friendster P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- `p2p-friendster-group`
- `p2p-friendster-uplnk-bytes`
- `p2p-friendster-dwlnk-bytes`
- `p2p-friendster-uplnk-pkts`
- `p2p-friendster-dwlnk-pkts`
- `p2p-friendster-duration`

**show active-charging analyzer statistics name p2p**

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Friendster:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging analyzer statistics name p2p protocol-group verbose**

With this release, the following fields have been added to the output of this command:

- Social-nw-generic-friendster:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
• Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

• Current Friendster Sessions

---

**CSCuq07727 - Google Music detection by ADC**

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

**Feature Changes**

**Support for Google Music Application Detection**

With this release, the support for detection of traffic originating from the Google Music application is added.

**Command Changes**

**p2p-detection protocol**

This command enables detection of peer-to-peer (P2P) protocols.

With this release, the `google-music` keyword is added to this command:

```
configure

  active-charging service service_name

  [ no ] p2p-detection protocol google-music

end
```

**p2p protocol**

This command enables detection of specific P2P protocols for charging purposes.

With this release, the Google Music protocol is supported.

```
configure

  active-charging service service_name

  ruledef ruledef_name

    [ no ] p2p protocol = google-music

  end
```

**clear active-charging analyzer statistics**

A new keyword `google-music` is added to this command to clear the analyzer statistics of the Google Music protocol.
clear active-charging analyzer statistics name p2p application google-music

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the google-music keyword is added to the P2P list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows. With this release, the google-music keyword is added to the P2P list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions. With this release, the google-music keyword is added to the P2P list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for google-music as part of the plugin. If detection of the Google Music P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-google-music-group
- p2p-google-music-uplnk-bytes
- p2p-google-music-dwlnk-bytes
- p2p-google-music-uplnk-pkts
- p2p-google-music-dwlnk-pkts
- p2p-google-music-duration

show active-charging analyzer statistics name p2p

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Google-music:
  - Total Uplink Bytes
  - Total Downlink Bytes
• Total Uplink Packets
• Total Downlink Packets

**show active-charging analyzer statistics name p2p protocol-group verbose**

With this release, the following fields have been added to the output of this command:

- Streaming-google-music:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

- Current google-music Sessions

---

**CSCuq11023 - ADC Support For Idrive**

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

**Feature Changes**

**Support for IDrive Application Detection**

With this release, the support for detection of traffic originating from the IDrive application is added.

**Command Changes**

**p2p-detection protocol**

This command enables detection of peer-to-peer (P2P) protocols.

With this release, the `idrive` keyword is added to this command:

```bash
configure
active-charging service service_name
[ no ] p2p-detection protocol idrive
end
```

**p2p protocol**

This command enables detection of specific P2P protocols for charging purposes.

With this release, the IDrive protocol is supported.
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol = idrive
end

clear active-charging analyzer statistics

A new keyword \texttt{idrive} is added to this command to clear the analyzer statistics of the IDrive protocol.

clear active-charging analyzer statistics name p2p application idrive

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.

With this release, the \texttt{idrive} keyword is added to the P2P list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.

With this release, the \texttt{idrive} keyword is added to the P2P list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.

With this release, the \texttt{idrive} keyword is added to the P2P list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for \texttt{idrive} as part of the plugin. If detection of the IDrive P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-idrive-group
- p2p-idrive-uplnk-bytes
- p2p-idrive-dwlnk-bytes
- p2p-idrive-uplnk-pkts
• p2p-idrive-dwlnk-pkts
• p2p-idrive-duration

**show active-charging analyzer statistics name p2p**

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Idrive:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

**show active-charging analyzer statistics name p2p protocol-group verbose**

With this release, the following fields have been added to the output of this command:

- Cloud-Idrive:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

- Current idrive Sessions

---

**CSCuq11035 - ADC Support For Hike Messenger**

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

**Feature Changes**

**Support for Hike Messenger Application Detection**

With this release, the support for detection of traffic originating from the Hike Messenger application is added.

**Command Changes**

**p2p-detection protocol**

This command enables detection of peer-to-peer (P2P) protocols.
With this release, the **hike-messenger** keyword is added to this command:

```
configure
  active-charging service service_name
    [ no ] p2p-detection protocol hike-messenger
  end
```

**p2p protocol**

This command enables detection of specific P2P protocols for charging purposes.

With this release, the Hike Messenger protocol is supported.

```
configure
  active-charging service service_name
    ruledef ruledef_name
      [ no ] p2p protocol = hike-messenger
    end
```

**clear active-charging analyzer statistics**

A new keyword **hike-messenger** is added to this command to clear the analyzer statistics of the Hike Messenger protocol.

```
clear active-charging analyzer statistics name p2p application hike-messenger
```

**show active-charging analyzer statistics name p2p**

This command displays statistical information for protocol analyzers.

With this release, the **hike-messenger** keyword is added to the P2P list:

```
show active-charging analyzer statistics name p2p application p2p_list
```

**show active-charging flows type p2p**

This command displays the information for the active charging flows.

With this release, the **hike-messenger** keyword is added to the P2P list:

```
show active-charging flows type p2p application p2p_list
```

**show active-charging sessions summary**

This command displays statistics for Active Charging Service (ACS) sessions.

With this release, the **hike-messenger** keyword is added to the P2P list:

```
show active-charging sessions summary type p2p application p2p_list
```
Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for hike-messenger as part of the plugin. If detection of the Hike Messenger P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-hike-messenger-group
- p2p-hike-messenger-uplnk-bytes
- p2p-hike-messenger-dwlnk-bytes
- p2p-hike-messenger-uplnk-pkts
- p2p-hike-messenger-dwlnk-pkts
- p2p-hike-messenger-duration

show active-charging analyzer statistics name p2p

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.

With this release, the following fields have been added to the output of this command:

- Hike-messenger:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging analyzer statistics name p2p protocol-group verbose

With this release, the following fields have been added to the output of this command:

- Communicator-hike-messenger:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary

With this release, the following fields have been added to the output of this command:

- Current hike-messenger Sessions
CSCuq20947 - ADC support for Google push Notification

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

Feature Changes

Support for Google Push Application Detection

With this release, the support for detection of traffic originating from the Google Push application is added.

Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols.

With this release, the google-push keyword is added to this command:

```
class activate charging service service_name

[ no ] p2p-detection protocol google-push

end
```

p2p protocol

This command enables detection of specific P2P protocols for charging purposes.

With this release, the Google Push protocol is supported.

```
class activate charging service service_name

  ruledef ruledef_name

  [ no ] p2p protocol = google-push

end
```

clear active-charging analyzer statistics

A new keyword google-push is added to this command to clear the analyzer statistics of the Google Push protocol.

```
clear active-charging analyzer statistics name p2p application google-push
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.

With this release, the google-push keyword is added to the P2P list:
show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p
This command displays the information for the active charging flows. With this release, the `google-push` keyword is added to the P2P list:

```
show active-charging flows type p2p application p2p_list
```

show active-charging sessions summary
This command displays statistics for Active Charging Service (ACS) sessions. With this release, the `google-push` keyword is added to the P2P list:

```
show active-charging sessions summary type p2p application p2p_list
```

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for `google-push` as part of the plugin. If detection of the Google Push P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-google-push-group
- p2p-google-push-uplnk-bytes
- p2p-google-push-dwlnk-bytes
- p2p-google-push-uplnk-pkts
- p2p-google-push-dwlnk-pkts
- p2p-google-push-duration

show active-charging analyzer statistics name p2p
This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer. With this release, the following fields have been added to the output of this command:

- Google-push:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging analyzer statistics name p2p protocol-group verbose
With this release, the following fields have been added to the output of this command:
• Untagged-google-push:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

• Current google-push Sessions

**CSCuq20978 - ADC support for Apple push Notification**

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

**Feature Changes**

**Support for Apple Push Application Detection**

With this release, the support for detection of traffic originating from the Apple Push application is added.

**Command Changes**

**p2p-detection protocol**

This command enables detection of peer-to-peer (P2P) protocols.

With this release, the **apple-push** keyword is added to this command:

```plaintext
configure

active-charging service service_name

[ no ] p2p-detection protocol apple-push

end
```

**p2p protocol**

This command enables detection of specific P2P protocols for charging purposes.

With this release, the Apple Push protocol is supported.

```plaintext
configure

active-charging service service_name

ruledef ruledef_name
```
[ no ] p2p protocol = apple-push
end

clear active-charging analyzer statistics
A new keyword apple-push is added to this command to clear the analyzer statistics of the Apple Push protocol.
clear active-charging analyzer statistics name p2p application apple-push

show active-charging analyzer statistics name p2p
This command displays statistical information for protocol analyzers.
With this release, the apple-push keyword is added to the P2P list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p
This command displays the information for the active charging flows.
With this release, the apple-push keyword is added to the P2P list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary
This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the apple-push keyword is added to the P2P list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema
New ADC bulk statistics are available in the P2P schema for apple-push as part of the plugin. If detection of the Apple Push P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.
The following bulk statistics are added to the P2P schema:
- p2p-apple-push-group
- p2p-apple-push-uplnk-bytes
- p2p-apple-push-dwlnk-bytes
- p2p-apple-push-uplnk-pkts
- p2p-apple-push-dwlnk-pkts
- p2p-apple-push-duration

show active-charging analyzer statistics name p2p
This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer. With this release, the following fields have been added to the output of this command:

- Apple-push:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging analyzer statistics name p2p protocol-group verbose**

With this release, the following fields have been added to the output of this command:

- Untagged-apple-push:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

With this release, the following fields have been added to the output of this command:

- Current apple-pushSessions
Chapter 3
ECS Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from ECS in StarOS 17 software releases.
ECS Enhancements for 17.4

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.

CSCus82709 - Multiple failures after VPC-SI upgrade build 56341 -> build 57028

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

**Feature Changes**

**Packet Processing for Null Content ID**

**Previous Behavior:** The packets were processed only if a valid content id was configured. The old implementation did not consider content-id 0 as a valid entry and hence DCCA did not generate CCR messages.

**New Behavior:** With this release, the rating group 0 is also treated as a valid rating group. If there is a charging-action with no rating group configured through the CLI command `content-id`, it will be considered as rating group 0 and will be used for various accounting mechanisms.

**Customer Impact:** Customers will see a lot of CCR-Us generated for content-id 0.

CSCuu43602 - Malformed Packet is passed from Gi to S5 without applying Quota of Gy

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

**Feature Changes**

**Dropping Malformed Packets at ECS**

When P-GW detects IP packets with invalid length/version, packets should be dropped ideally. However, the current implementation passes these invalid IP packets going out of ECS without applying the ECS charging action. In this release, all malformed packets will now be dropped.

**Previous Behavior:** Downlink malformed packets get forwarded without any rulematch.

**New Behavior:** Downlink malformed packets will now get dropped at ECS. New statistics are added to the output of the `show active-charging service statistics` CLI command.
Performance Indicator Changes

show active-charging service all

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

- Packets Dropped - Invalid Len in IP Hdr(Dwlink)
- Packets Dropped - Invalid Ver in IP Hdr(Dwlink)
ECS Enhancements for 17.3

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.

CSCue60917 - EDRs to include Rating Group and Service ID fields

**Applicable Products:** IPSG

**Feature Changes**

**Inclusion of Rating Group and Service ID Fields in EDRs**

**Previous Behavior:** In earlier releases, the Rating Group (RG), Service Identifier (ID) and charging action name attributes were not available in EDRs.

**New Behavior:** With this feature, the EDR attribute configuration has been extended to support these additional fields in the EDRs for billing purposes.

**Important:** This feature currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.

**Customer Impact:** When there is any mismatch in the subscriber billing, the customers can use these attributes in the EDR to relate back the EDR records with particular RG/Service ID that is mapped for the particular URL.

**Command Changes**

```plaintext
attribute

In support of this feature, these keywords “sn-rating-group”, “sn-service-id”, “sn-charging-action” have been introduced to the attribute command to enable configuring these attributes in the EDR format for static and predefined rules.

```
[ no ] attribute { sn-rating-group | sn-service-id | sn-charging-action }
  priority priority
end

Performance Indicator Changes

show active-charging edr-format all

With this feature enabled, the output of `show active-charging edr-format all` command will display these newly configured EDR attributes.

CSCur91211 - Quota not requested in CCR-I when preemptively in CA set (dynamic-only)

Applicable Products: GGSN

Feature Changes

Processing of Predefined Rules with Default Bearer QoS Change

**Previous Behavior:** In the case of default bearer QoS change, the predefined rules were buffered for processing later. As a result, the CCR-I message sent over Gy does not contain the rating-group of predefined rule.

**New Behavior:** Predefined rules on default bearer will now be processed along with the default bearer QoS change.

**Customer Impact:** Customers will be able to see CCR-I with predefined rule charging-action rating group if configured.

CSCus80666 - Dis-engage TRM when a flow moves from one bearer to another

Applicable Products: GGSN, P-GW, PDSN

Feature Changes

TRM Flows

The Transactional Rule Matching (TRM) feature enables the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified. With this enhancement, TRM/Accel path gets disengaged in case of any bearer movement for a particular flow.

**Previous Behavior:** When TRM/Accel path gets enabled for a flow on a particular bearer and if flow moves from one bearer to another, TRM would not get disengaged. As a result, packets were being matched to rules present on the previous bearer, and not on the current bearer.

**New Behavior:** When TRM/Accel path gets enabled for a flow on a particular bearer and if flow moves from one bearer to another, TRM will get disengaged. Packets will now be matched to rules present on the new bearer.
CSCus96377 - Reset Flow-Bearer mapping is missed in certain scenarios

Applicable Products: GGSN, P-GW, PDSN

Feature Changes

ACS Data Flow-Bearer Association

**Previous Behavior:** When a new bearer gets created from UE, ACS does not mark all existing data flow-bearer association invalid. ACS uses existing bearer mapping to send a new downlink packet. Secondly, when an uplink packet fails to match any rule on the bearer it came from, it is discarded and downlink packets for the same flow are also discarded.

**New Behavior:** When a new bearer gets created from UE, ACS marks all existing data flow-bearer association invalid. When a new downlink packet comes for the same flow, ACS queries SM for the correct bearer and sends the new downlink packet on the correct bearer. Secondly, when an uplink packet fails to match any rule on the bearer it came from, it is discarded and flow-bearer association is invalidated. If a downlink packet comes for the same flow, ACS now sends a bearer lookup query to SM and the packet goes on the correct bearer.
ECS Enhancements for 17.2

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.

CSCus12168 - [ECSv2]: Pop-Up Notification use case

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

**Feature Changes**

**Support for Predefined Rules Deactivation**

A capability is added in the ECSv2 to redirect traffic when quota for a user expires. When quota expires, PCRF will install a rule for the redirection. In the charging-action for this redirection rule, an action to disable the same rule is added to ensure one time redirection. A new keyword `deactivate-predefined-rule` is added under the Charging Action Configuration Mode as per this enhancement. This keyword, when configured, will ensure that the predefined rule gets deactivated after applying the charging-action. A charging-rule-report will be sent to PCRF indicating the PCC Rule Status as INACTIVE for the deactivated rule. Rule-Failure-Code sent is RESOURCE_ALLOCATION_FAILURE.

**Command Changes**

```
charging-action

A new keyword `deactivate-predefined-rule` has been added in this release to ensure that the predefined rule gets deactivated after applying the charging-action when configured. By default, the configuration is disabled. The no option will remove the configuration, and the default option is same as no.

The deactivation will apply only for predefined rules. If a static rule or a predefined group-of-ruledef is associated with the charging-action, it will not be deactivated.

configure

active-charging service service_name

charging-action charging-action_name

  [ default | no ] deactivate-predefined-rule

end
```
Performance Indicator Changes

show active-charging charging-action all

The following statistic is added to the output of this command to indicate whether predefined rule deactivation has been enabled or disabled.

- Predefined Rule Deactivation

show active-charging charging-action statistics name

The following statistic is added to the output of this command to display the number of predefined rules that are deactivated.

- Predef-Rules Deactivated

CSCus65449 - Rule Inheritance: Show CLI should use subscriber level flag

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

Rule Inheritance

With this enhancement, the show active-charging sessions full all CLI command will display the inheritance information only if both the rule-level and subscriber-level inheritance information are present.

Important: This enhancement is applicable to 17.1.2 and later releases.

Previous Behavior: Even if there was inconsistency in the recovery of Inheritance feature, the show active-charging sessions full all CLI used to show that the charging parameters of a dynamic rule are inherited, whereas the Rf records and Gy records would indicate that inheritance is not applied.

New Behavior: When inconsistency is detected in the Inheritance feature parameters, a new field “Inheritance is disabled for this subscriber - Error!” will be displayed in the output of the show active-charging sessions full all CLI command.

Customer Impact: This change provides more clarity in an error scenario where the Inheritance feature is not applied.

Performance Indicator Changes

show active-charging sessions full all

The following field will be displayed if rule information has inheritance parameters but the subscriber level information does not have inheritance enabled.

- Inheritance is disabled for this subscriber - Error!
ECS Enhancements for 17.1

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.

CSCul22770 - SFR - PSP algorithm modification

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

**Feature Changes**

**PSP Algorithm Modification**

Since Radius selects the policing to be applied including Bandwidth policy, validation of the policy before its application is critical. In case Bandwidth policy received from RADIUS is invalid, that is, absent in the configuration, a fallback mechanism is required to select another policy so that subscriber call remains active.

**Previous Behavior:** A single bandwidth policy was being sent from SM to ECS for validation. When invalid bandwidth policy was received from RADIUS, call used to get terminated.

**New Behavior:** Primary and fallback policies are sent from SM to ECS. When invalid bandwidth policy is received from RADIUS,

- When bandwidth policy is configured under APN and fallback mechanism is also enabled, then Bandwidth policy from APN is applied, if it is valid and call remains active.
- When no bandwidth policy is configured under APN or fallback mechanism is disabled under APN configuration, then Bandwidth policy from Rulebase is applied if it is valid and fallback mechanism is configured under rulebase and call remains active.

In case, both Primary and fallback policies are found to be invalid, the call is terminated.

**Customer Impact:** This will help to prevent termination of calls when incorrect bandwidth policy is sent through RADIUS.

**Command Changes**

**fallback-enabled**

A new keyword **fallback-enabled** has been added to the CLI **active-charging bandwidth-policy** to control the fallback bandwidth mechanism. This keyword fills the bandwidth policy value.

If fallback is enabled, both primary and secondary BW policy is filled with Bandwidth Policy configured in the APN.
If fallback is not enabled, then only primary BW policy is filled with Bandwidth Policy configured in the APN and secondary BW policy is filled with NULL.

```plaintext
configure
  context context_name
  apn apn_name
    [ default | no ] active-charging bandwidth-policy bandwidth_policy_name [ fallback-enabled ]
  end
```

Notes:

- **fallback-enabled**: Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

**Important**: This configuration option shall not be applicable when neither primary nor fallback policy names are received from SM. In this case, default policy in rulebase shall always be applied if it is configured irrespective of "fallback-enabled" option.

When there is a radius returned Bandwidth-Policy value, the APN configured Bandwidth-Policy is to be sent in Bandwidth-Policy-Secondary attribute. Therefore, a new variable is added to show Secondary Bandwidth Policy value while displaying subscriber AAA configuration in the `show subscribers aaa-configuration` CLI. This value shows the APN configured Bandwidth-Policy.

**fallback-enabled**

A new keyword `fallback-enabled` has been added to the CLI `active-charging bandwidth-policy` to control the fallback bandwidth mechanism. This keyword fills the bandwidth policy value.

```plaintext
configure
  active-charging service service_name
  rulebase rulebase_name
    [ default | no ] bandwidth default-policy bandwidth_policy_name [ fallback-enabled ]
  end
```

Notes:

- **fallback-enabled**: Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

When this keyword is used, bandwidth policy under rulebase is applied when bandwidth policy name received through class attribute is invalid and no fallback policy name is received. When this keyword is not used, bandwidth policy from rulebase shall not be applied in the same case. The CLI command `bandwidth default-policy <BW-Policy>` will reset fallback-enabled option if it is set. The command `[no] bandwidth default-policy` will remove bandwidth policy and reset fallback option.
Performance Indicator Changes

show apn name

The output of the command `show apn name apn_name` has been modified to include the following option:
  - bandwidth-policy fallback

show active-charging rulebase name <rulebase-name>

The output of the command `show active-charging rulebase name rulebase_name` has been modified to include the following option:
  - bandwidth-policy fallback

show active-charging sessions full all

The output of the command `show active-charging sessions full all apn_name` has been modified to include the following option:
  - Bandwidth Policy Fallback Applied

CSCuo23705 - per-rulebase bulkstats to show number of subscribers using that rulebase

Applicable Products: GGSN, P-GW

Feature Changes

New ‘rulebase’ Schema

A new bulkstat schema ‘rulebase’ has been introduced which displays the number of subscribers using that rulebase.

Performance Indicator Changes

rulebase Schema

A new schema ‘rulebase’ has been introduced through this feature. This schema has the following counters.

- `%ecs-rbase-name%` : Rulebase Name.
- `%ecs-rbase-upl_pkts%` : Total Uplink Pkts hitting this rulebase.
- `%ecs-rbase-upl_bytes%` : Total Uplink Bytes hitting this rulebase.
- `%ecs-rbase-dnl_pkts%` : Total Downlink Pkts hitting this rulebase.
- `%ecs-rbase-dnl_bytes%` : Total Downlink Bytes hitting this rulebase.
- `%ecs-rbase-sess-cur%` : Total active bearers using this rulebase.
- `%ecs-rbase-subscribers-cur%` : Total active calls using this rulebase.
CSCuo68909 - TCP flows modification (RFC 1122, Section 4.2.2.13)

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

Feature Changes

Modification of TCP Flows

In some scenarios, UE initiates a new TCP connection request (SYN) reusing the existing source port number, received within the 2MSL time frame of the existing flow. The data flow pertaining to this old connection gets deleted after 2MSL timeout, if configured and till then the new TCP connection traffic goes on the same data flow. The TCP analyzer is not able to reopen existing TCP flow, in response to UE's new behavior.

The TCP analyzer has been enhanced to support the optional behavior in RFC 1122, section 4.2.2.13. ECSv2 now clears the old data flow before 2msl timeout and creates a new data flow, for UE's new connection using same port number. It will also generate and send last ack packet if not already sent. New CLI command has also been introduced to control this feature at rulebase level. You can enable or disable this feature using the CLI command. The stats counters have also been modified to indicate the number of port reuse flows.

Command Changes

tcp 2msl-timeout

A new keyword port-reuse has been added to the command tcp 2msl-timeout at rulebase level to support the source port reuse.

configure

active-charging service service_name

rulebase rulebase_name

[ default | no ] tcp 2msl-timeout time_in_sec [ port-reuse ]

end

Notes:

- port-reuse: Allows the source port reuse to reopen the tcp flow in 2msl timeout.
- When port-reuse keyword is configured along with tcp 2msl-timeout, reuse of the same source port number within 2msl timeout of previous flow, is permitted (supported in code).
- When port-reuse keyword is not configured along with the tcp 2msl-timeout, reuse of the same source port number within 2msl timeout of the previous flow, is not supported and such a packet will be dropped.

Performance Indicator Changes

show active-charging rulebase

This command has been modified to include the following in the output:

- Port Reuse: [Yes/No]
**show active-charging rulebase statistics name**

This command has been modified to include the following in the output:

- TCP 2msl port reuse : n

### CSCup08420, CSCup49998, CSCur67850 - PGW (Gp) rejecting dynamic rule with Unknown Bearer ID cause

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

### Feature Changes

#### Handling of Rule Modification in UE Only Mode for EPS IP-CAN Bearer

**Previous Behavior:** Earlier rule binding was getting rejected.

**New Behavior:** Now, the binding of PCEF rules will be successful when BCM mode is set to UE-only for EPS IP-CAN bearer without “bearer-ID” in the PCRF messages such as RAR or CCA-U.

**Customer Impact:** Rule binding in the 3G to 4G handover scenario will be successful in UE-only mode and any filter (and related info) changes because of this modification/installation/removal will not be notified to UE as updates in UE only mode cannot be sent to UE.

These rules are only considered for charging and the expectation is that the same rules are again modified in 4G (if handover is done) so that the filters (and related info) can be notified to UE.

### CSCup30908 - Incl X-header for IPv4 Unique Identity with “128bit-string” IPv6 address

**Applicable Products:** P-GW

### Feature Changes

#### Support for Insertion of New X-Header

Support has been added to insert attribute sent in the RADIUS access-accept message for Header Enrichment (HE). This RADIUS attribute received in access-accept message should be in 128 bit string format and ECS will insert it in the X-header, as is, in string format. This 128 bit string can be either IPv4 or IPv6 address assigned to the subscriber.

### Command Changes

**x-header format**

A new keyword `radius-string` has been added to the command `insert <xheader_field_name> variable bearer radius-string.`

configure
active-charging service service_name

xheader-format <xheader_format_name>

insert <xheader_field_name> variable bearer radius-string

end

Notes:

• radius-string: SN-Transparent-Data Attribute received in RADIUS ACCESS ACCEPT message.

CSCup31650 - Req29 - PCEF supervision-maintenance KPIs (phase 2)

Applicable Products: GGSN, P-GW

Feature Changes

Support for New Bulkstats Variables

New bulkstats variables are added to ECS schema to periodically track the following:

• number of interim EGCDR generation caused by Volume threshold
• number of interim EGCDR generation caused by Time threshold
• number of interim EGCDR generation caused by QHT
• number of final CDRs generated

Performance Indicator Changes

ECS Schema

The following new bulkstat variables are added to the ECS schema.

• egcdrs-generated-vol
• egcdrs-generated-time
• egcdrs-generated-qht
• egcdrs-generated-final

CSCup48750 - [ECS] UDR enhancement to support NEMO MR Hosts

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

Extending FDR/EDR and UDR for NEMO Sessions

As part of this feature, these configurable attributes are added to FDR/EDRs and UDRs to support the NEMO sessions.

- sn-subscriber-ipv4-address
- sn-subscriber-ipv6-address
- sn-vrf-name
- nemo-prefix-list
- num-nemo-prefix

**Important:** The “nemo-prefix-list” and “num-nemo-prefix” attributes are available only with NEMO license. The attributes “sn-vrf-name”, “nemo-prefix-list” and “num-nemo-prefix” are customer-specific.

These attributes will not be present in FDR/EDRs and UDRs unless explicitly configured. An additional trigger “nemo-prefix-update” is added for UDR generation on receiving a NEMO update event.

These attributes are required to populate the VRF-name and NEMO MR prefixes in UDR. The format in which these will be populated in UDRs is “<VRF-name>:<NEMO MR Prefix>”.

Command Changes

**attribute**

A new attribute “sn-vrf-name” is added to EDR format to support NEMO sessions.

**configure**

  require active-charging

  active-charging service service_name

  edr-format format_name

  [ no ] attribute sn-vrf-name priority priority_value

  end

Notes:

- **sn-vrf-name:** This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.

**attribute**

Five new attributes are added to UDR format to support NEMO sessions.

**configure**

  require active-charging
active-charging service service_name

udr-format format_name

[ no ] attribute { nemo-prefix-list | num-nemo-prefix | sn-subscriber-ipv4-address | sn-subscriber-ipv6-address | sn-vrf-name } priority priority_value

end

Notes:

- nemo-prefix-list and num-nemo-prefix keywords are available only with NEMO license.
- sn-vrf-name: This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.
- nemo-prefix-list: This attribute contains the various VRF names and NEMO MR Prefixes associated with them. This is a customer-specific attribute.
- num-nemo-prefix: This attribute indicates the number of NEMO MR Prefixes. This is a customer-specific attribute.
- sn-subscriber-ipv4-address: This attribute indicates the IPv4 address of the subscriber.
- sn-subscriber-ipv6-address: This attribute indicates the IPv6 address of the subscriber.

udr trigger

nemo-prefix-update is a new keyword in this command and this trigger is added for UDR generation during NEMO update event.

configure

require active-charging

active-charging service service_name

rulebase rulebase_name

[ default | no ] udr trigger nemo-prefix-update

end

Notes:

- The nemo-prefix-update keyword is available only with NEMO license.
- On configuring this keyword/trigger, UDRs will be generated in case a NEMO update event is received. If this trigger is not configured UDRs will not be generated even if a NEMO update event is received from session manager. If the “no” or “default” option is used, it will disable the UDR trigger for nemo-prefix-update.

Performance Indicator Changes

show active-charging rulebase name

The following field is newly added to the output of this show command to support NEMO sessions.
• NEMO Prefix Update Trigger

**show active-charging rulebase statistics**

The following field is newly added to the output of this show command to support NEMO sessions.

• UDRs generated for NEMO prefix update

**show active-charging udr-format all**

The output of this show command will include information on these newly added attributes in the UDR format.

**CSCuq30619 - active-charging cli need to be removed from ecs mode**

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

**Feature Changes**

**Cosmetic Changes to CLI**

**Previous Behavior:** The existing CLI command “active-charging test-prepaid-auth” in exec mode has been removed.

**New Behavior:** A new CLI command “debug active-charging test-prepaid-auth” has been introduced in exec debug mode. This is a hidden CLI, it is visible only when “cli test-commands” is enabled.

Additionally, the CLI “active-charging service” has been disabled in exec mode. Now one can enter this CLI only under the config mode.

**CSCuq45238 - Different disconnect reason is required for PCRF unreachable case**

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

**Feature Changes**

**Value Change for Diagnostics AVP in Rf Record**

**Previous Behavior:** Earlier, only one disconnect reason used to come from session manager to ECS, and there was no other way to differentiate between IMS Authorization failure and PCRF unreachable scenarios.

The Diagnostics AVP used to have the value as PCRF_INITIATED_SESSION_TERMINATION even when PCRF was unreachable.

**New Behavior:** Session manager will now send the detailed disconnect reason in Diagnostics field. The Diagnostics field in Rf record will have separate values when PCRF initiates termination and when PCRF is unreachable.
CSCur31337 - vrf-name attribute in EDR and UDR

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

Feature Changes

UDR Enhancement to Support NEMO Hosts

New attribute is added to FDR/EDR and UDR formats to populate the vrf-name associated with the base session of NEMO setup.

The VRF name attribute in the FDR/EDR and UDR will enable the customer to correlate the NAT binding records with the FDR/EDR and UDR in the gateway.

Command Changes

attribute

A new attribute “sn-vrf-name” is added to EDR format to support NEMO sessions.

configure

require active-charging

active-charging service service_name

edr-format format_name

[ no ] attribute sn-vrf-name priority priority_value

end

Notes:

• sn-vrf-name: This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.

attribute

A new attribute “sn-vrf-name” is added to UDR format to support NEMO sessions.

configure

require active-charging

active-charging service service_name

udr-format format_name

[ no ] attribute sn-vrf-name priority priority_value

end

Notes:
• **sn-vrf-name**: This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.

**CSCur47328 - PGW-CDR issues for WiFi calls & in LTE-WiFi & WiFi-LTE Handoffs**

**Applicable Products:** P-GW

**Feature Changes**

**Generation of CDRs During LTE<->WiFi Handoff**

**Previous Behavior:** In a scenario where LTE->WiFi handoff happens, CDR was not generated. But in the case of WiFi->LTE handoff, CDR was generated.

**New Behavior:** Now, when the TCP in-order packets are received, the list is checked for any pending packets. If there are any pending packets in the list, the timer is extended so that packet in list can get configured time for reordering.

**CSCur56899 - ECS rule matching wrong for app "Mon Réseau"**

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

**Feature Changes**

**Handling of pipelined HTTP HEAD response**

**Previous Behavior:** Message body with HTTP head response was leading to wrong rule match.

**New Behavior:** Now, any content-length or transfer-encoding in HTTP HEAD response is ignored and next downlink packet is considered as a new HTTP head response in case of pipelined HTTP HEAD request and response scenario.

**Customer Impact:** Customer would be able to see proper rule matching for pipelined HTTP HEAD request/response.
ECS Enhancements for 17.0

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.

---

**CSCub32971 - GGSN/PGW support Customer's customized processing on Gy interface**

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

**Feature Changes**

**Gy Interface Function Enhancement**

For a custom procedure to be undertaken for handling failure on Gy interface, a new GTPP dictionary “custom47” is defined for PGW-CDRs.

The same custom behavior for Gy failure condition is also supported in the existing custom21 dictionary for GGSN.

**CSCuf55484 - Support of ULI as X-header field in HE feature**

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

**Feature Changes**

**Support of User Profile and ULI as x-Header field**

The existing x-Header Enrichment (HE) feature has been enhanced to accept the following fields as an additional x-header field.

- **User Profile**—The value of this field will be dynamically provided by the PCRF over Gx interface.
- **User Location Information**

**Previous Behavior:** x-Header framework did not have User-Profile and ULI as x-Headers

**New Behavior:** You can now insert User-Profile and ULI as x-Headers.

**Customer Impact:** Customers now have the additional functionality to insert User-Profile and ULI as x-Headers.
CSCuh60799 - Remove memory fair usage feature

Applicable Products: P-GW

Feature Changes

Memory Fair Usage Feature Deprecated

The Memory Fair Usage feature has been removed and is no longer available. The following options under `fair-usage` CLIs have also been deprecated.

- Under active charging service:
  - adjust-factor
  - cpu-only
  - cpu-param
  - deact-margin
  - inline-memory-share
  - memory-only
  - threshold-percent

**Important:** The command `fair-usage tcp-proxy [ max-flows-per-subscriber | memory-share ]` has been retained and continues to work as before.

- Under Rulebase: The CLI `session-waiver-percent` under `rulebase` has also been deprecated and is ignored.

Command Changes

`fair-usage`

The CLI `fair-usage` under `active-charging service` has been deprecated and is ignored. The following CLI command options would no longer work.

- adjust-factor
- cpu-only
- cpu-param
- deact-margin
- inline-memory-share
- memory-only
- threshold-percent

Only `fair-usage tcp-proxy` option has been retained.
The CLI `fair-usage session-waiver-percent` under `rulebase` has been deprecated.

**CSCui88377 - Removal of Rule-deactivation-time not working**

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

**Feature Changes**

**Gx Activation/Deactivation Time for Predefined Rules**

**Previous Behavior:** If “Rule-Deactivation-Time” AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis.

**New Behavior:** If Rule-Deactivation-Time AVP for a predefined rule is omitted in a CCA or RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

---

**Important:** This behavior change is applicable only to predefined rules.

**Customer Impact:** If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

**CSCuj14841, CSCum33077 - Flow Aware Packet Acceleration (FAPA)**

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

**Feature Changes**

**Flow Aware Packet Acceleration (FAPA)**

Accelerated ECS Packet feature will be supported when TRM FastPath is enabled on the Rulebase.

The Flow Aware Packet Acceleration feature improves the throughput in terms of PPS, by caching rule matching results of a flow for selected flows so as not to incur the lookup penalty for a large number of packets in that flow. This new accelerated path is capable of performing a full range of basic functions including handling charging, modification of packet headers and incrementing various counters. The accelerated path dynamically evaluates the current flow state and reverts back to the slow path when the flow cannot be handled on the fast path.

The acceleration is applied to specific flows without affecting any external interfaces related to Billing, CLI, interfaces, and so on. This feature is an extension of the TRM/FastPath that was introduced in R15.0 for ASR5500 platform. TRM FastPath works on approximately 50-65% of all packets, including VoLTE, Encrypted and HTTP, in the system today for any given call model, with the control path left intact. New changes are in the data path after TRM has cached the rule matching results. Accelerated ECS packet path can efficiently process 50+% of data packets in the system, yielding a significant performance gain on ECS data path.

TRM/FP support has been extended beyond rule-matching. Qualifying packets avoid much of the ECS stack for N bytes of volume for a given flow. Only the packets requiring minimal work are qualified for the accelerated path. The work...
needed for each packet include a subset of flow actions, QoS enforcement, L3/L4 header inspection, tcp sequence number validation, and applicable charging methods.

The Accelerated ECS function identifies packets that need only a small amount of processing, and performs only those necessary tasks on these packets. Only those packets that do not require DPI are allowed to enter the Accelerated path. VoLTE, encrypted, HTTP, and plain TCP/UDP traffic where L7 analysis is not enabled, etc. are all the flows that will get accelerated.

The Flow Aware Packet Accelerated ECS is controlled by the FAPA license, and a CLI at active-charging service. The CLI is visible only if the license is present and is available only on ASR5500 and QvPC platforms. The FAPA path will be functional, only if TRM/FP is enabled and the CLI is configured.

This feature provides the operator with additional capacity on deployed systems without any HW addition. The operators could get 30-40% of the system capacity based on their traffic pattern and deployed call models.

**Important:** Flow Aware Packet Acceleration license is required on ASR5500 and QvPC platforms.

### Command Changes

**accelerate-flow**

A new CLI `accelerate-flow` has been added.

```
configure

    active-charging service <service_name>

        [ no ] accelerate-flow

    end
```

### Performance Indicator Changes

#### AECS Schema

The following bulkstats are available for FAPA feature:

- ip-accel-pkts
- udp-accel-pkts
- tcp-accel-pkts
- http-accel-pkts
- https-accel-pkts

### CSCum33088 - Simplification of retransmitted pkt charging Phase 2

Applicable Products: P-GW
Feature Changes

Deprecation of ‘retransmissions-counted’ command

The CLIs `retransmissions counted` and `no retransmissions counted`, introduced in release 16.0, when configured at rulebase level governed the charging of retransmitted packets. This CLI when configured overrides the following CLIs configured at charging-action level or rulebase level or service level.

From 17.0 release, the following CLIs have been deprecated:

- At the charging action level, the CLI `retransmissions-counted`
- At the rulebase, the CLI `edr sn-charge-volume count-retransmitted-units`
- At the service level, the CLI `policy-control retransmissions-counted`

Command Changes

`retransmissions-counted`

At the charging action level, the CLI `retransmissions-counted` has been deprecated.

`edr sn-charge-volume count-retransmitted-units`

At the rulebase level, the CLI `edr sn-charge-volume count-retransmitted-units` has been deprecated.

`policy-control retransmissions-counted`

At the service level, the CLI `policy-control retransmissions-counted` has been deprecated.

CSCum52646, CSCum52657, CSCum52650 - ECS Support for Override Control

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

Feature Changes

Support for Override Control

Important: Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Inheritance feature does not support enabling the feature at Rule level and charging action level. In order to provide this flexibility and also have a generic capability on chassis, Override Control feature is introduced. This feature will define a set of custom AVPs that will enable the PCRF to override charging and policy parameters for a specified set of rules or charging actions.

The override values should be sent by PCRF over Gx using the custom AVPs. Override Control provides this capability while addressing the limitations with Inheritance feature like rule level control, charging action level control, different override values to be specified for a subscriber, etc. So, the Override Control feature will replace the Inheritance feature.
**Important:** In this release, both Inheritance and the Override Control features will be supported. Note that both these two features should not be enabled simultaneously.

The Gx interface is updated to include custom AVPs for the PCRF to send override values to P-GW. These override values may be sent for a specific rule(s) or for charging action(s). In case the override values are sent for a charging action, a rule or some of the rules may be excluded from using the override values by sending the rules names in the Gx message. The override values will be check pointed and recovered in case of either standalone recovery or ICSR.

This Override Control feature is expected to maintain existing active calls using inheritance post upgrade. Inheritance feature and Override control should not be enabled simultaneously. It is necessary that Inheritance feature be turned off once Override Control feature is enabled.

**Customer Impact:** Override Control feature allows the customer to dynamically modify the parameters of static or predefined rules with parameters sent by PCRF over the Gx interface.

**Command Changes**

**override-control**

This is a new command to enable or disable Override Control feature. This feature is available at the rulebase level and is license controlled. The Diameter capability exchange message should indicate support for Override control feature when this CLI command is enabled.

```
configure

    require active-charging

    active-charging service service_name

    rulebase rulebase_name

       [ default | no ] override-control

end
```

Notes:

- This CLI command will be visible only when the license to configure the Override Control feature is installed.
- By default, this feature is disabled. If this command is configured, the Override Control feature will be enabled. When this feature is enabled, it is necessary to turn off the Inheritance feature.

**Performance Indicator Changes**

**show active-charging sessions full all**

The output of this show command is changed to indicate how many Overrides were received and how many are currently active for the subscriber.

The following fields are new in this release:

- Override Control
  - Installs Received
• Installs Succeeded
• Installs Failed
• Total Override Control

show active-charging subscribers callid <call_id> override-control

This is a new show CLI command for displaying the override being applied for the subscriber:

show active-charging service all

The following fields are newly added to the output of this show command:
• Override Control
  • Supported parameters
    • Charging Parameters
    • Policy Parameters

CSCum52736 - Dual Factor Authentication – Radius Based (MPN)

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

**Feature Changes**

**RADIUS Based Dual Factor Authentication For Mobile Private Network**

Dual Factor Authentication has been implemented for Mobile Private Network’s (MPN’s) mobile devices, most typically for terminals like lottery machine devices, ATMs, and so on. For security reasons, this DFA procedure is followed before traffic can flow normally. The first level authentication happens as part of call setup using RADIUS. While the call is established, the pre-DFA-rulebase that has the configuration to allow only RADIUS and ICMP traffic is used; rest of the traffic is dropped. Until then all the normal traffic is denied and is resumed only after the additional RADIUS based authentication is successful.

The success of RADIUS authentication is determined by a RADIUS analyzer. This analyzer understands the authentication requests and responses especially ‘Access-Request’ and ‘Access-Accept’. Whenever the RADIUS ‘Access-Request’ message is matched with ‘Access-Accept’ message, the rulebase is changed to new rulebase called Post-DFA-rulebase and the existing dedicated bearers are deleted and the same is informed to PCRF. The RADIUS analyzer does not analyze any other message but only the ‘Access-Request’, ‘Access-Accept’, and the ‘Access-Reject’.

**Command Changes**

**radius**

This is a new command to configure the RADIUS analyzer. This command is available at the charging ruledef level.

**configure**

  **require active-charging**
active-charging service service_name

ruledef ruledef_name


end

Notes:
- **radius**: RADIUS related configuration.
- **any-match**: This command allows you to define rule expressions to match all RADIUS packets.
- **error**: This command allows you to define rule expressions to match for errors in RADIUS packets and errors in the RADIUS analyzer.
- **state**: This command allows you to define rule expressions to match the current state of an RADIUS session.

route priority

A new keyword “radius” has been added to the **route priority** command. This keyword specifies the radius protocol analyzer.

configure

  require active-charging

  active-charging service service_name

  rulebase rulebase_name

  route priority route_priority ruledef ruledef_name analyzer radius [ description ]

  end

Notes:
- The new keyword **radius** determines the route to light weighted RADIUS protocol analyzer.

**Performance Indicator Changes**

**show active-charging analyzer statistics**

The output of this show command has been changed to include the radius information in the analyzer stats to indicate the number of pkts, "Access Requests", "Access Accepts", "Access Rejects".

**show active-charging flows type radius**

The output of this show command has been changed to include the radius flow type information.

**show active-charging flows full**
The output of this show command has been changed to include the radius state, radius IDs in the list, radius code received information.

**show active-charging analyzer statistics name radius**

The output of this show command has been changed to include the ACS RADIUS Session Statistics.

**clear active-charging analyzer statistics name radius**

This command clears the ACS RADIUS Session Statistics.

**clear active-charging analyzer statistics**

This command clears the radius information in the analyzer stats that indicate the number of pkts, "Access Requests", "Access Accepts", "Access Rejects".

**show active-charging subsystem all [ rulebase name xxxx | debug-only ]**

The output of this show command has been changed to include the total radius flows and current radius flows.

**CSCum59452, CSCum88067 - Enhanced DNS for IPv6 (MPN)**

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

**Feature Changes**

**Enhanced DNS for IPv6 (MPN)**

DNS redirection server redundancy is enhanced to include hierarchy based approach in addition to round-robin approach, helping the operator to specify list of DNS servers in the order of preference.

The Enhanced FQDN based DRE (DNS Readdressing enhancement) feature for IPv4 addresses enables MPN to redirect DNS requests, which are a part of the FQDN white list to a different server than the one specified in the APN for enterprise DNS servers for unique functionalities on IPv4 address space. When an enterprise receives IPv6 pool addresses, they use the enhanced FQDN based DRE on IPv6 that supports server redundancy.

Further, if readdress server list was configured then round-robin approach was selected for server selection. This feature also allows hierarchy based server selection. In hierarchy based approach, queries are redirected as per primary, secondary, and tertiary selection. The hierarchy approach is extended to support IPv4 addresses also. With this feature, both round-robin and hierarchy based server selection approaches would be applicable for both IPv4 and IPv6 based servers. An additional CLI is provided that enables you to select from hierarchy or round-robin approach for server selection.

**Previous Behavior:** Earlier DRE was available only for IPv4 addresses.

**New Behavior:** Support is enhanced for IPv6 address for DNS readdressing. Additionally, readdressing is supported for other protocols as well over TCP/UDP. New hierarchy approach is also provided for selecting the server in case of server list configured. This approach is provided for IPv4 and IPv6 addresses.

**Customer Impact:** Readdressing has been enhanced for IPv6 addresses. If the server-list is configured, the server can also be selected.
CSCum62403 - Support of Simultaneous Create Bearer Request and Update Bearer Request

Applicable Products: MME, P-GW, S-GW

Feature Changes

Support for Simultaneous Handling of Create Bearer Request and Update Bearer Request

Previous Behavior: When P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW.

New Behavior: When modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

CSCum67974 - Enhance CLI to display summary of active sessions per rulebase

Applicable Products: GGSN

Feature Changes

CLI to Get Summary of Active Sessions per Rulebase

The output of existing CLI `show active-charging sessions summary rulebase name <rulebase_name>` has been modified to display the summary of the total number of active sessions per rulebase. Earlier this command displayed a lot of other information such as the redundant flow counts.

Performance Indicator Changes

`show active-charging sessions summary rulebase name <rulebase_name>`

The CLI `show active-charging sessions summary rulebase name <rulebase_name>`, has been modified to display the summary of the total active sessions for the given rulebase. Earlier, this command displayed a lot of other information such as the redundant flow counts.

CSCum79237, CSCum79229, CSCum85815 - ECS support for Configurable Micro Checkpoint Syncup Timer

Applicable Products: GGSN, P-GW
Feature Changes

Support for Configurable Micro Checkpoint Sync-up Timer

Micro Checkpoint Sync-up timer is an internal timer utilized by Rf and Gy modules to check point corresponding billing information.

Previous Behavior: Earlier, micro checkpoint sync-up timer was not configurable and was hardcoded with a value of 18 seconds for ICSR and 8 seconds for Session Recovery (SR).

New Behavior: This enhancement reduces this timer value to ensure the accurate billing information during the ICSR switchover event. Micro Checkpoint Sync-up timer is now made configurable with an expectation that it be set at a value as low as 4 seconds.

Customer Impact: This provides the operator with the flexibility to provision timer for accurate billing information in case of session recovery or ICSR switchover. However, this is a performance impacting feature and the impact of the micro checkpoint sync timer reduction needs to be carefully considered by the operator before provisioning a lower value.

Command Changes

check-point accounting sync-timer

This is a new command at service level to configure the micro checkpoint sync-up timer to as low as 4 seconds and max 60 seconds.

configure

require active-charging

active-charging service service_name

   check-point accounting sync-timer { icsr | sr } timer_value [ sr | icsr ]

   timer_value

   no check-point accounting sync-timer { icsr | sr }

end

Notes:

- sr: Micro check-pointing for Session Recovery (SR)
- icsr: Micro check-pointing for ICSR
- timer_value: Time configured will be in multiples of 2 seconds. The default timer value will be 18 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

check-point accounting sync-timer

This is a new command at rulebase level to configure the micro checkpoint sync-up timer to as low as 4 seconds and max 60 seconds.

configure

require active-charging
active-charging service service_name

rulebase rulebase_name

check-point accounting sync-timer { icsr | sr } timer_value [ sr | icsr ]
timer_value

no check-point accounting sync-timer { icsr | sr }
end

Notes:
- sr: Micro check-pointing for Session Recovery (SR)
- icsr: Micro check-pointing for ICSR
- timer_value: Time configured will be in multiples of 2 seconds. The default timer value will be 18 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

CSCum88267 - MVG: URL Based Readdressing

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

Feature Changes

URL Based Re-addressing Feature

In this release, URL-based Re-addressing can be enabled based on L7 matching, particularly for HTTP URLs. Re-addressing charging action can also be applied based on L3/L4 matching. CLI and Statistics support are provided for this feature. The url-readdress keyword is added to the flow action command in the ACS Charging Action Configuration Mode.

Command Changes

flow action

The url-readdress keyword is added to the flow action command in the ACS Charging Action Configuration Mode to configure the URL server to re-address for the specified charging action.

configure

active-charging service service_name

charging-action charging_action_name

flow action url-readdress server ipv4_address [ port port_number ]

no flow action
end
Performance Indicator Changes

ECS Schema

The following new bulk statistics are added in this release:

- url-flow-readdress-success
- url-flow-readdress-failure

show active-charging charging-action statistics name

The following new counters are added to the output of this command:

- URL-Redressing:
  - Requests URL-Readdressed
  - Total Charging action hit - Req. Readdr
  - Proxy Disable Success
  - Flows connected to URL Server
- URL Readdressing Error Conditions:
  - Total connect failed to URL Server
  - URL Readdress - pipelined case
  - URL Readdress - Socket Mig. failed
  - Proxy Disable Failed

show active-charging rulebase statistics name

The following new counters are added to the output of this command:

- URL-Redressing:
  - Requests URL-Readdressed
  - Total Charging action hit - Req. Readdr
  - Proxy Disable Success
  - Flows connected to URL Server
- URL Readdressing Error Conditions:
  - Total connect failed to URL Server
  - URL Readdress - pipelined case
  - URL Readdress - Socket Mig. failed
  - Proxy Disable Failed

CSCum88678 - RF charging should be supported for flows accelerated by

Applicable Products: GGSN, HSGW, P-GW, S-GW
Feature Changes

Rf Accounting Support for FAPA

Rf is supported for Flow Aware Packet Acceleration (FAPA) feature and it provides improved performance for HTTP traffic if the traffic flow is FAPA eligible.

CSCum88705 - FDR/EDR should be supported in A-ECS

Applicable Products: GGSN, P-GW

Feature Changes

FDR/EDR Support for FAPA

FDR/EDR is supported for Flow Aware Packet Acceleration (FAPA) feature and it provides improved performance for HTTP traffic if the traffic flow is FAPA eligible.

CSCun17417 - Discontinue support for charge-volume variants except ip, constant

Applicable Products: P-GW

Feature Changes

Discontinuation of CLI Configuration Options in Charging Action

The other charge-volume protocol variants except IP and constant, in charging-action configuration has been removed and would no longer be available. For example, if you have a HTTP GET request with total packet length 100 bytes, out of which 20 bytes is the IP header, 20 bytes is the TCP header, and 60 bytes are the HTTP headers, ECSv2 provided a mechanism to charge for total 100 bytes (IP-and-above) or just 80 bytes (TCP-and-above) or just 60 bytes (HTTP-and-above), which of these three applied to a given packet was decided by the charge-volume protocol variant in the charging-action CLI config. With this feature, only IP packet is being charged and the granularity has been removed.

Previous Behavior: Earlier, bytes could be charged according to protocol specified in charging-action CLI.

New Behavior: Currently, only entire IP packet is charged and the granularity has been removed. All other charge-volume protocol variants except IP and constant have been removed.

Command Changes

charge-volume

All options in charge-volume command under charging-action have been removed except IP and constant.

charge-volume ip

The option packet-length has been removed from the command charge-volume ip under charging-action.
CSCun81110 - Expand HTTP URL field in EDR from 256 to 2000+ characters

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Support for Increases HTTP URL Field Length

- Previous Behavior: The limit for the length of HTTP URL in EDR was 1-255.
- New Behavior: The maximum length for HTTP URL in EDR is changed to 1-4095.
- Customer Impact: URL with larger length can now be accommodated fully in EDR. This may avoid truncation of records.

Command Changes

rule-variable

The size argument range for HTTP URL is now extended from 1-255 to 1-4095.

configure

  require active-charging
  
  active-charging service service_name
  
  edr-format format_name
  
  rule-variable http url length length_value priority priority

end

Performance Indicator Changes

show active-charging edr-format statistics all

The output of this show CLI command includes the following new statistic to track the truncated EDRs.

- Total edrs truncated

CSCun83874 - [A-ECS] Support post-processing rules in Accelerated Path

Applicable Products: P-GW

Feature Changes

Support for Post Processing Rules in Accelerated Path

Support for post processing rules have been added in accelerated path.
Previous Behavior: Transactional Rule Matching functionality was limited only to the charging rule match bypass. Also, Accelerated ECS support for post-processing actions was not present.

New Behavior: The Transactional Rule Matching functionality has been extended to bypass post-processing rule matching as well.

Customer Impact: Accelerated ECS will work for post-processing as well.

CSCup28989 - PGW session mgr memory usage increased in 17.0

Applicable Products: P-GW

Feature Changes

Limitation on Rules Recovery

Previous Behavior: There was no limit set for the number of Override Control (OC) rules / CA / exclude rules to be recovered.

New Behavior: In this release, only 15 OC rules/ CA / exclude rules will be recovered.

CSCup48914 - wsp user-agent ends-with is not getting optimized

Applicable Products: PDSN

Feature Changes

Optimization of WSP User-Agent Rules

Previous Behavior: There were several customer deployments using host based and http referrer based rules. Also there were quite a large number of rules used with ‘ends-with’ operator for matching the URL, URI, user-agent or host strings. Such types of rules were unoptimized and were matched with brute-force. This incurred a significant cost during rule matching.

New Behavior: To improve the rule-matching performance, already existing DFA optimizer has been extended to handle the optimization of these types of rules. As a result, user-agent based rules are now optimized and hence faster.

CSCup73278 - Incorrect ruledef match for frag traffic with reassembly timeout

Applicable Products: P-GW

Feature Changes

Incorrect RuleDef Match

Flow identification:

Previous Behavior: TCP layer info was not extracted for fragments earlier. Thus, for a fragment a new ads with src/dest port = 0 was created. Subsequent fragments (which timeout) on this flow would continue to match this new ads.
**ECS Enhancements for 17.0**

**ECS Changes in Release 17**

**New Behavior:** Now, if 1st fragment for this frag-chain is received and has tcp header, tcp src/dest ports are extracted. This fragment will now be mapped to the existing flow (if it exists). If 1st fragment is missing or does not have tcp header, a new ads with src/dest port = 0 is created. This fragment is sent for rule-matching. The newly created ads is immediately destroyed once the fragment is processed. This is followed for all such subsequent packets.

**Rule-matching:**

**Previous Behavior:** Dnl fragments on reassembly timeout, matched the rule on default bearer.

**New Behavior:** Dnl fragments which map to the existing bearer (returned by flow identification), now match rules installed on flow bearer. For example: If a flow is established and packets start coming on dedicated bearer, then flow bearer will be dedicated. Now when a dnl fragment comes, it will match the dedicated bearer rules.

**CSCup86339 - Assert sessmgr_ipv4.c:10235 : sessmgr_ipv4_process_user_pkt_part2()**

*Applicable Products: GGSN, P-GW*

**Feature Changes**

**Processing of Data Packets in S2b Handoff for Dormant Bearer**

**Previous Behavior:** During S2b handoff, DCCA was trying to send the buffered data packets to session manager even for a dormant bearer. Such dormant bearer existed only at ECS and not at session manager, and thereby resulting in system crash.

**New Behavior:** With the current implementation, after OCS response is received, it is verified to determine if the bearer is in dormant state at ECS. If the bearer is found to be in dormant state, then such buffered packets will be dropped.

**CSCuq20248 - Fail planned switchover when OC batch processing is in progress**

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

**Feature Changes**

**SRP Switchover Event During Batch Processing for Override Control**

When SRP switchover is initiated and the session manager is batch processing the subscribers for Override Control (OC), the switchover event will fail. Administrator will have to retry the switchover later.

**CSCuq30728 - PGW:Assertion failure at process_bearer_binding_rsp**

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

Installation of PCRF Bound Predefined Rule Based on Access Side Signaling

**Previous Behavior:** If a PCRF bound predefined rule is sent for installation, there was no check to determine if there was any access side signaling that was pending for the same predefined rule.

**New Behavior:** A check is now made available to verify if the predefined rule exists in pending rules list before binding it to the bearer. If the rule exists, a failure is indicated to PCRF.

**Customer Impact:** PCRF bound predefined rules can fail to get installed/updated if there is any access side signaling pending for the same rule.

CSCuI50221 - P4: show active-charging service all prints ICMP w/out v4/V6 details

**Applicable Products:** P-GW

Feature Changes

Change in display of ‘show active-charging service all’ command

**Previous Behavior:** The CLI command `show active-charging service all` was printing the message “ICMP Flow Idle Timeout : 300 (secs)” twice, once for IPv4 and once for IPv6.

**New Behavior:** The CLI command `show active-charging service all` now prints the message “ICMP Flow Idle Timeout : 300 (secs)” only once.

Command Changes

`show active-charging service all`

The CLI command `show active-charging service all` now prints the message “ICMP Flow Idle Timeout: 300 (secs)” only once.
Chapter 4  
ePDG Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from ePDG in StarOS 17 software releases.
ePDG Enhancements for 17.2

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 *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 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

---

**CSCus30276, CSCus30296 - Support for tunnel endpt ip in SWm interface**

**Feature Changes**

**Passing on UE tunnel Endpoint Address over SWm**

With this release ePDG to supports passing on UE tunnel Endpoint Address over SWm or S2b.

The provisioning of UE Tunnel Endpoint-IP (IKEv2 tunnel endpoint incase of NAT) to AAA server will help the operator to identifying the UE’s location at AAA server. The operator uses this information to control the access or to decide the UE connections. Operator can lookup the GeoIP database (GeoDB) against the UE tunnel endpoint IP to identify the country from where the UE is connecting from. Based on this information operator can allow the call or reject it(using auth-failure) according to the policy configured. Lets say the policy dictates that the VoWiFi calls are allowed only for UEs connecting from home country but not allowed while roaming outside the country, they can save the revenue leakage using this information.
ePDG Enhancements for 17.1

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 *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 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

---

**CSCur47221 - PGW reselection attempts to be made configurable**

**Feature Changes**

**PGW Reselection Optimization**

With this release ePDG supports PGW Reselection Optimization, ePDG attempts to select alternate PGW when the first PGW has rejected the call with the below error causes.

- EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCUPIED (0x54)
- EGTP_CAUSE_NO_RESOURCES_AVAILABLE(73)
- EGTP_CAUSE_SERVICE_DENIED (0x59)
- EGTP_CAUSE_PEER_NOT_RESPONDING-(100)
- EGTP_CAUSE_SERVICE_NOT_SUPPORTED (0x44)
Maximum alternate PGW selection attempts (0-64) can be configured per APN profile using CLI, default is 3.

CSCub02436 - EMERGENCY PDN- ePDG

Feature Changes

PDN support for UICC

With this release ePDG to support emergency PDN for the UICC authenticated UEs only. The procedure is not defined in 3GPP spec (TS 33402-a00), new standards are defined.

CSCup38875 - [ePDG] Non UICC device support EAP-MSCHAPV2/EAP-TLS/EAP-TTLS support

Feature Changes

EAP-TLS/EAP-TTLS based authentication support

Previous Behavior: For NON UICC devices, certificate based device authentication is supported by ePDG.
New Behavior: EAP-TLS/EAP-TTLS based authentication is also supported for NON UICC devices.

CSCur03639 - [ePDG] P-CSCF IPv4 address support in ePDG

Feature Changes

P-CSCF IPv4 address support in ePDG

Previous Behavior: Only IPv6 P-CSCF supported in ePDG.
New Behavior: Both IPv4 and IPv6 P-CSCF supported in ePDG.

CSCur47280 - ePDG need to set HO flag set when v4 IP addr is zero from UE

Feature Changes

HO flag setting when V4 IP address is zero from UE

Previous Behavior: ePDG does set HO flag when v4 IP address is zero from UE.
New Behavior: ePDG sets HO flag when v4 IP address is zero from UE.
ePDG Enhancements for 17.0

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 *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 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**

---

**CSCtz75077 - ASR5500 Support for ePDG**

**Feature Changes**

**ASR5500 Support for ePDG**

This feature supports ePDG/IPSec subscriber mode in ASR5500.

**Previous Behavior:** Users NPUSIM in data path and data takes multiple hops in INGRESS

**New Behavior:** NPU is used in chassis instead of NPUSIM. NATT / Migration support is added as well as data INGRESS path is more optimized.
CSCum39855 - [ePDG]- Support local configuration as preferred PGW selection mechanism

Applicable Products: ePDG

Feature Changes

PGW Selection Mechanism

With this release local configuration can be used as the preferred PGW selection mechanism with ePDG.

CSCum45189 - [ePDG] Crypto performance - Scale improvement on ASR5500

Feature Changes

Crypto performance

ASR5500 introduces a new CLI require ipsec-large which will allow to scale the tunnels to 3.5M. Throughput of 25GBPS on 6 ACTV DPCs.

Previous Behavior: This CLI and associated changes are not present

New Behavior: New CLI require ipsec-large added to enable scale the tunnels to 3.5M.

Customer Impact: More tunnel density available, but SM memory is reduced to accommodate the same.

Command Changes

require ipsec-large

As part of Crypto performance scale improvement on ASR5500 a new command require ipsec-large is introduced.

configure

require ipsec-large

end

CSCum67523 - Initiate Session Checkpoint upon Session Creation.

Applicable Products: ePDG

Feature Changes

Session Checkpoint

With this release sessions are check pointed to the standby chassis upon creation.
CSCum84927 - [ePDG] - No need to retransmit the CSR if the prev resp parsing failed

Applicable Products: ePDG

Feature Changes

CSR Retransmission

With this release ePDG retransmitting CSR if the previous response parsing failed is addressed.

CSCum87789 - Trap for failed Diameter or Radius peer success after XGW/PGW/HA/ePDG failover

Applicable Products: XGW, PGW, HA, ePDG

Feature Changes

Trap for failed Diameter

New trap is introduced to report SRP switchover.

Previous Behavior: No trap to indicate SRP switchover.

New Behavior: New trap “starSRPSwitchoverOccured” generated when SRP switchover happens.

CSCuo23369 - [ePDG]:Intelligent graceful PDN disconnection during maintenance-mode

Feature Changes

Graceful PDN disconnection during maintenance-mode

In maintainence mode ePDG will automatically delete the VoLTE calls. When the VoLTE bearer gets teared down or subscriber will become non-VoLTE after deletion of all VoLTE bearers when operator uses the "clear subscriber all non-volte-call auto-delete" command.

Previous Behavior: “clear subscriber all non-volte-call" command deletes the non-VoLTE subscribers. when operator uses the same command at some interval to delete the VoLTE call when VoLTE call will become non-VoLTE.

New Behavior: Operator will use the "clear subscriber all non-volte-call auto-delete" command one-time only, service will delete the volte subscribers as well when it will become non-VoLTE.
Chapter 5
GGSN Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from GGSN in StarOS 17 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:

- GGSN Enhancements for 17.0
  - “CSCum88464 - Intelligent graceful PDN disconnection during maintenance-mode” - Corrected and enhanced description
GGSN Enhancements for 17.5

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

---

**CSCzn47162 - Routing Behind the Mobile Station on an APN**

**Feature Changes**

**Routing Behind the Mobile Station on an APN**

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDP context which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the “mobile router.” If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDP context.
**Command Changes**

`network-behind-mobile`

The following `network-behind-mobile` has been added to enable or disable a Network behind Mobile Station for APN.

```
config
  context context_name
  apn apn_name
    network-behind-mobile { max-addresses-behind-mobile max_addr | max-subnets max_subnets }
    { default | no } network-behind-mobile
end
```

**Notes:**

- **default**
  Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

- **no**
  Disables the network behind mobile station functionality on the APN.

- **max-addresses-behind-mobile max_addr**
  Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

- **max-subnets max_subnets**
  Specifies the maximum number of subnets that can be enabled for a call in the APN.
  `max_subnets` must be an integer from 1 through 16.
  Default: 10

**Performance Indicator Changes**

`show apn name <apn_name>`

The following fields have been added to this command.

- Network Behind Mobile Station: Enabled
- Maximum subnets behind Mobile station: 10
- Maximum Addresses Behind Mobile Station: 16777214
GGSN Enhancements for 17.3

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

---

**CSCus80195 - T3/N3 timer with 100 ms granularity**

**Feature Changes**

**Granularity Added to T3/N3 Timer**

This enhancement introduces the ability to configure T3/N3 timer in millisecond (ms) granularity. This helps reduce the possibility of “packet collision” between P-GW/S-GW/MME and so on by being able to configure a nearly identical second value separated by a few 100 ms.

The new T3 value is configured in 100 ms granularity, starting at 1000 ms (1 second). The previous range for T3 value was between 1 to 20 seconds, with a default of 5 seconds. The range for the new T3 value is 1000-20000 ms, with numbers going up by 100 ms.

**Previous Behavior:** The CLI command `retransmission-timeout` was operational. Timer granularity for T3/N3 timer was in seconds.
New Behavior: The CLI command `retransmission-timeout` is now obsolete; this CLI has been replaced by the CLI command `retransmission-timeout-ms`. Timer granularity for T3/N3 has been changed from seconds granularity to 100 milliseconds.

Command Changes

`retransmission-timeout-ms`

This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer.
The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure

calendar context context_name

  ggsn-service service_name

    retransmission-timeout-ms retransmit_time

    default retransmission-timeout-ms

  end
```

Notes:
- **default**: Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.
- **retransmit_time**: Specifies the amount of time, in milliseconds, that must pass without an SGSN response before the GGSN service retransmits GTP control packets. Must be an integer from 1000 to 20000, with increments of 100.
  Default: 5000

`retransmission-timeout-ms`

This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer.
The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure

  context context_name

  egtp-service service_name

    gtpc retransmission-timeout-ms retransmit_time

    default gtpc retransmission-timeout-ms

  end
```

Notes:
GGSN Changes in Release 17

GGSN Enhancements for 17.3

- **default**: Configures the default control packet retransmission timeout in GTP.
- **retransmit_time**: Specifies the GTP control packet retransmission timeout in milliseconds. Must be an integer from 1000 to 20000, with increments of 100.
  
  Default: 5000

**retransmission-timeout-ms**

This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer. The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure

  peer-profile service-type [ ggsn-access | pgw-access | sgw-access | sgw-network ] name peer_profile_name

  gtpc-service service_name

  gtpc retransmission-timeout-ms retransmit_time

  default gtpc retransmission-timeout-ms

end
```

Notes:
- **default**: Configures the default control packet retransmission timeout in GTP.
- **retransmit_time**: Specifies the GTP control packet retransmission timeout in milliseconds. Must be an integer from 1000 to 20000, with increments of 100.
  
  Default: 5000

**CSCus80582 - 3G call - All packets are dropped due to APN AMBR limiting**

**Feature Changes**

**Change in ‘apn-ambr rate-limit direction’ CLI Command**

In 17.3 release and onward, the CLI mentioned in Command Changes section below has been modified. The option `bytes` has been deprecated and can no longer be used. However, this command option is available in earlier releases.

**Previous Behavior**: The command option `bytes` was available in the CLI command `apn-ambr rate-limit direction`.

**New Behavior**: The command option `bytes` has been deprecated and is no longer available in the CLI command `apn-ambr rate-limit direction`.

**Command Changes**

```
apn-ambr rate-limit direction
```
This command has been modified. The command option **bytes** has been deprecated from this command. The new command reads as follows:

```
configure

calendar context context_name

apn apn_name

   apn-ambr rate-limit direction { downlink | uplink } [ burst-size { auto-readjust duration seconds } | violate-action { drop | lower-ip-precedence | transmit } ]

   [ default | no ] apn-ambr rate-limit direction { downlink | uplink }

end
```

Notes:

- **default**: Returns the selected command to it’s default setting of no APN-AMBR.
- **no**: Disables the selected command.
- **rate-limit direction { downlink | uplink }**: Specifies that the rate limit is to be applied to either the downlink (network to subscriber) traffic or the uplink (subscriber to network) traffic.
- **downlink/uplink**: Applies the AMBR parameters to the downlink/uplink direction.
- **burst-size**: This parameter is used by policing and shaping algorithms to permit short bursts of traffic in order to not exceed the allowed data rates. It is the maximum size of the token bucket.
- **drop**: Drops violating packets.
- **lower-ip-precedence**: Sets the DSCP value to zero ("best effort") for violating packets.
- **transmit**: Transmits violating packets. This is the default setting.
GGSN Enhancements for 17.1

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

---

**CSCuh06473, CSCuq23971 - Cause IE enhancement for Delete Bearer Request**

**Feature Changes**

**Cause IE enhancement for Delete Bearer Request**

Cause value in the Delete Bearer Request has been limited. The behavior impacted by this feature is:

- Delete Bearer Request/Delete PDP Context due to idle-timer/session-timer expiration
- Delete Bearer Request due to bearer inactivity of default bearer
- Delete PDP Context due to bearer inactivity of the last PDP context of PDN connection
- Delete Bearer Request/Delete PDP Context triggered by `clear subscriber` CLI command

Configuration has been added to set cause values and cause inclusion in the following scenarios:

- CLI-based trigger to disconnect
• per APN when P-GW initiated disconnection for above mentioned timer expiry

**Important:** Cause IE Enhancement for Delete Bearer Request is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Previous Behavior:**

1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, its cause-IE is not configurable.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, its cause-IE is not configurable.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, its cause-IE is not configurable.

**New Behavior:**

1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, the cause-IE to be used may optionally be specified by the operator in CLI. The CLI also allows the operator not to include cause-IE.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, the cause-IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, the cause IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.

**Customer Impact:** Cause-Code during PDN connection teardown may be modified.

**Important:** This feature allows operator to override existing behavior. Such overridden behavior may not be compliant with standards.

**Command Changes**

`clear subscribers`

When subscribers are deleted, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword `del-cause` is optional and can be combined with existing options to modify “Cause-IE” behavior.

```
clear subscribers all [ del-cause { reactiv-req | none } ] [ verbose ] [ -noconfirm ]
clear subscribers apn apn_name [ del-cause { reactiv-req | none } ] [ verbose ] [ -noconfirm ]
```

**Notes:**

- `del-cause`: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests generated for default bearer.
- `reactiv-req`: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- `none`: Omit GTP cause IE in DBR/DPC generated for default bearer.
GGSN Changes in Release 17

- The new behavior for Cause-IE will be effective only if the clear subscribers CLI results in the sending of a Delete Bearer Request for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**timeout**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword del-cause is optional and can be combined with existing options to modify “Cause-IE” behavior.

```plaintext
configure
  context context_name
    apn apn_name
      timeout absolute time [ del-cause { reactiv-req | none } ] | { exclude-default-bearer } | { timeout_value volume-threshold { downlink | total | uplink } Data_traffic_bytes } | { { gbr | non-gbr } { timeout_value volume-threshold { downlink | total | uplink } Data_traffic_bytes } | { default | no } timeout absolute del-cause
end
```

Notes:
- **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- By default, the del-cause option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**timeout bearer-inactivity**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword del-cause is optional and can be combined with existing options to modify “Cause-IE” behavior.

```plaintext
configure
  context context_name
    apn apn_name
      timeout bearer-inactivity del-cause { reactiv-req | none }
      { default | no } timeout bearer-inactivity del-cause
end
```
end

Notes:

- **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- By default, the **del-cause** option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**timeout idle**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword **del-cause** is optional and can be combined with existing options to modify “Cause-IE” behavior.

```
configure
  context context_name
    apn apn_name
      timeout idle idle_dur [ del-cause { reactiv-req | none } ]
      { default | no } timeout idle del-cause
end
```

Notes:

- **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- **del-cause reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- By default, the **del-cause** option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for Default Bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**operator-del-cause**

A new CLI **operator-del-cause** has been added to the existing configuration. This CLI will enable or disable the the Cause-IE feature for Delete PDP Context Request in GGSN.

The Cause-IE configuration for Delete PDP Context Request is given in the APN configuration and is also available in **clear subscribers** CLI. When this new CLI is enabled, the feature will be applied to GGSN based on the APN configuration or the **clear subscribers** CLI. This new CLI will be disabled by default.
configure
context context_name

    ggsn-service service_name

    { default | no } gtpc operator-del-cause

end

Notes:

• **operator-del-cause**: Enables or Disables Operator Cause-IE Behavior Feature for Delete PDP Context Request sent to delete the last PDP Context of the PDN connection. This CLI is disabled by default.

**CSCuo89377 - Different Credit-Control Treatment at Gy for Out-roamers**

**Feature Changes**

**Enhancement in Number of Home PLMN**

In order to define more Home PLMNs under ggsn/pgw-service, the allowed PLMN limit under ggsn/pgw-service has been increased to more than 512 PLMNs. With this increased limit, the defined PLMN would be treated as Home PLMN, while the undefined PLMNs such as International SGSN or PLMN, would be automatically treated as Foreign PLMNs. Additionally, an option is provided to define just the MCC portion of the PLMN under GGSN-Service/PGW-Service for Home PLMN definition. In this case, Home PLMN qualification will be done solely based on MCC value and MNC portion will be ignored for these particular MCCs (Mobile Country Code).

**Previous Behavior:**

1. The number of Home PLMNs configured under GGSN/PGW service was limited to 5 PLMNs.
2. Both MCC and MNC had to be configured for Home PLMN definition.

**New Behavior:**

1. The number of Home PLMNs configured under GGSN/PGW service has been increased to 512.
2. An option has been provided to define just the MCC portion of the PLMN under ggsn-service/pgw-service for Home PLMN definition. In this case, Home PLMN qualification will be done solely based on MCC value, and MNC portion will be ignored for these particular MCCs (Mobile Country Code).

**Customer Impact:** 512 PLMNs can be configured for Home PLMN definition under GGSN/PGW service.

**Command Changes**

```
plmn id mcc [ mnc ]
```

In the below CLI, the number of PLMN ids that can be configured under the PGW/GGSN service would be increased from 5 to 512.

Currently MNC is the mandatory parameter, this would be made as an optional parameter so that we can configure both MCC and MNC value, or just the MCC portion for Home PLMN definition.
ggsn-service  ggsn-service

plmn  id  mcc  plmn_mcc_id_number  [  mnc  plmn_mnc_id_number  ]

end

Notes:
- **id**: Configures the PLMN identifier for the GGSN service. This command must be followed by the MCC command, whereas the MNC command is optional.

**CSCup14481 - P-CSCF discovery mode on ggsn output can be made more transparent**

**Feature Changes**

**Change in Output of P-CSCF Discovery Mode**

The P-CSCF Discovery Mode output is Enhanced to cover the details about the source of the FQDN in case the Discovery Mode is DNS. The source for the FQDN sting can be either S6B Server or the APN Configuration.

**Previous Behavior**: Earlier, the output shown in the Discovery Mode of the P-CSCF Address Information was restricted.

Following is the output shown earlier:

**P-CSCF Address Information: Discovery Mode: Addresses received from DNS**

Restricted Discovery mode information

**New Behavior**: Now, the output shown in the Discovery Mode of the P-CSCF Address Information is more detailed.

Following is the modified output:

**P-CSCF Address Information: Discovery Mode: Addresses received from DNS (APN based FQDN) OR (S6B based FQDN)**

Detailed Discovery Mode Information

**Performance Indicator Changes**

**Show Sub Full All**

The output of the command **show sub full all** has been modified to display the Discovery Mode address in more detailed way. The previous and current output has been described in the previous and new behavior sections.
CSCup59406 - sesstrc task in over state during longevity/aggravator run

Feature Changes

Configuring Session Trace File Type

To address the issues caused when the sesstrc task allocates memory over the allotted limit, under a random subscriber session trace load tests on P-GW/S-GW, support for B-type XML files is introduced in addition to the A-type files already supported.

Previous Behavior: The file type was A-type XML file and the type could not be changed.

New Behavior: The CLI has been modified (see Command Changes section) to allow the operator to select the file type generated by session trace. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

Command Changes

circuit trace network-element

The new optional file-type keyword enables the operator to determine which type of XML file is generated by the session trace:

configure

  session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw } [ file-type { a-type | b-type } ] [ collection-timer | tce-mode ]

  no session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw }

end

Notes:

- Default file-type is a-type.
- To keep the syntax simple, the optional file-type keyword must be entered before entering either of the other optional keywords.
- To modify the session trace network-element configuration, you must first enter the no session trace network-element form of the command to remove the session trace configuration.
CSCuq35259 - [17.0 FCS] ARP value not in synch with ACS n SESSMGR for secondary bearer

Feature Changes

NRUPC Seen Towards Access Side

Previous Behavior: Earlier, if the CCA-U coming from PCRF to PGW has a dynamic rule whose QCI/ARP has changed from the original QCI/ARP, then a NRUPC request towards access side was not initiated.

New Behavior: Now, if the CCA-U coming from PCRF to PGW has a dynamic rule whose QCI/ARP has changed from the original QCI/ARP, then the NRUPC request towards the access side is initiated.

Customer Impact: NRUPC is seen towards access side in a scenario when a CCA-U coming from PCRF to PGW has a dynamic rule whose QCI/ARP has changed from the original QCI/ARP.

CSCur19546 - AccTermCause User_Request if session disconnec Invalid-source-IP-address

Feature Changes

Change in Termination Cause Value

Previous Behavior: Radius ACCT stop Termination cause value was 'User-Request'.

New Behavior: Radius ACCT stop Termination cause value is now 'Admin-Request'.
GGSN Changes in Release 17.0

This chapter identifies features and functionality added to, modified for, or deprecated from GGSN in StarOS 17 software releases.

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

---

**CSCtr45924 - root privileges for ftp-user, no restriction to specific ftp-directory**

**Feature Changes**

**Root Privileges to FTP Users**

File accessing privileges for individual users have been modified to the file-directory where billing files are located.

**Previous Behavior:** Earlier, user could do SFTP to any directory.

**New Behavior:** Administrator now can optionally assign user a root directory with either read-write or read-only privilege. Once assigned, the user can only SFTP to its root directory with assigned privilege.

**Customer Impact:** The command fields are optional. There is no impact if a customer does not choose to use.
CSCui40177 - GGSN to send micro chkpt for ue initiated and network initiated update

Feature Changes

Micro Checkpointing support for ue and network initiated updates

Currently GGSN uses full checkpoints when any bearer parameter like QoS change, SGSN change, or RAT change happens. In such cases GGSN shall use micro checkpoints for the parameters that are changed. This change is needed for session recovery checkpoints as well as ICSR checkpoints.

For GGSN -- UE initiated update and network initiated update (excluding inter tech handoff and coa ) should send microcheckpoint.

CSCui17195 - GTP echo and GTP message retry shall be configured separately

Feature Changes

Separate Configuration for GTP-C Echo and GTP-C Non-echo Messages

**Previous Behavior:** Previously, GTP echo and GTP message retry “timer” could be configured separately. However, the `max-retry number` configuration was the same.

**New Behavior:** Now, `max-retry number` can be configured separately for GTP echo and GTP message, similar to “timer” configuration.

**Customer Impact:** This new behavior allows different configurations for GTP-C echoes as compared to the non-echo messages.

See CSCum66168 for additional changes.

CSCum17169 - Per APN, and QCI, GTP-C v2 responses

Feature Changes

Per APN and QCI GTP-C v2 Response

This feature collects the eGTP-C cause codes as bulkstats and categorizes them to Per APN per QCI. Operator can derive KPI based on the bulkstat counters per QCI for a particular APN (for example: IMS APN and VoLTE APN).

Supporting more granular statistics/bulkstats on APN (up to 2,000 APNs are supported) has an impact on system performance and this occurs for bulkstats. Stats need to be obtained at regular intervals for a few minutes. Each of these retrievals can lead to gigabytes of information to be gathered and consolidated. Due to this issue, a restricted/controlled usage of granular bulkstats is introduced. If the operator uses the configuration, then it is possible to enable which APN is used to collect granular statistics and in those granular statistics which particular statistics are collected.

**Previous Behavior:** In general, the current bulkstats APN configuration gathers the bulkstat data for the all APNs. There is no option to restrict gathering of bulkstats for selective APN(s).
**New Behavior:** A new CLI is introduced to selectively enable an APN candidate list for the new bulkstat schema “apn-expansion”. The eGTP-C cause codes as bulkstats will be collected for those APN(s) which are configured through this CLI only.

**Customer Impact:** This feature allows operators to collect more granular GTP-C statistics on per APN per QCI level to monitor certain KPIs based on these statistics.

**Command Changes**

*egtpc-qci-stats*

This new command enables/disables an APN candidate list for the apn-expansion bulkstat schema.

```plaintext
configure
   context context_name
      apn apn_name
         [ no ] egtpc-qci-stats { all | qci1 | qci2 | qci3 | qci4 | qci5 | qci6 | qci7 | qci8 | qci9 }
    default egtpc-qci-stats
end
```

**Notes:**
- Refer to the *APN Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information about this command.

**Performance Indicator Changes**

**APN-expansion schema**

A new schema has been added to categorize bulkstats per APN QCI.

- cresessrespaccept
- cresessrespdeniedCtxNotFound
- cresessrespdeniedInvalidMsgFormat
- cresessrespdeniedInvalidLength
- cresessrespdeniedMandIEIncorrect
- cresessrespdeniedMandIEMissing
- cresessrespdeniedNoResourcesAvl
- cresessrespdeniedPrefPdnTypeUnsupported
- cresessrespdeniedAllDynamicAddrOccupied
- cresessrespdeniedServiceDenied
- cresessrespdeniedUserAuthFailed
- cresessrespdeniedApnAccessDenied
- cresessrespdeniedRequestRejected
- cresessrespdeniedCondIEMissing
- cresessrespdeniedApnRstTypeIncompatible
- cresessrespdeniedImsiNotKnown
- cresessrespdeniedOtherCause
- crebearNorsp
- crebearrespaccept
- crebearrespdeniedCtxtNotFound
- crebearrespdeniedSvcNotSupported
- crebearrespdeniedInvalidMsgFormat
- crebearrespdeniedMandIEIncorrect
- crebearrespdeniedMandIEMissing
- crebearrespdeniedCondIEMissing
- crebearrespdeniedNoResourcesAvl
- crebearrespdeniedSemanticErrinTFT
- crebearrespdeniedSyntacticErrinTFT
- crebearrespdeniedSemanticErrinPktFltr
- crebearrespdeniedSyntacticErrinPktFltr
- crebearrespdeniedUnableToPageUE
- crebearrespdeniedUENotResponding
- crebearrespdeniedUnableToPageUeSuspend
- crebearrespdeniedUERefuses
- crebearrespdeniedRequestRejected
- crebearrespdeniedInvalidLenPiggybkMsg
- crebearrespdeniedInvalidRemotePeerReply
- crebearrespdeniedPeerNotResponding
- crebearrespdeniedTempRejDueToHOProgress
- crebearrespdeniedDeniedInRat
- crebearrespdeniedOtherCause
- modbearerrespaccept
- modbearerrespdeniedCtxtNotFound
- modbearerrespdeniedInvalidMsgFormat
- modbearerrespdeniedInvalidLength
- modbearerrespdeniedMandIEIncorrect
modbearerrespdeniedMandIEMissing
modbearerrespdeniedNoResourcesAvl
modbearerrespdeniedServiceDenied
modbearerrespdeniedRequestRejected
modbearerrespdeniedCondIEMissing
modbearerrespdeniedOtherCause
delsessrespaccept
delsessrespdeniedInvalidMsgFormat
delsessrespdeniedMandIEIncorrect
delsessrespdeniedMandIEMissing
delsessrespdeniedNoResourcesAvl
delsessrespdeniedOtherCause
delbearerNorsp
delbearerrespaccept
delbearerrespdeniedCtxtNotFound
delbearerrespdeniedInvalidMsgFormat
delbearerrespdeniedMandIEIncorrect
delbearerrespdeniedMandIEMissing
delbearerrespdeniedCondIEMissing
delbearerrespdeniedNoResourcesAvl
delbearerrespdeniedRequestRejected
delbearerrespdeniedUnableToPageUeSuspend
delbearerrespdeniedInvalidRemotePeerReply
delbearerrespdeniedPeerNotResponding
delbearerrespdeniedTempRejDueToHOPrivate
delbearerrespdeniedOtherCause
updbearNorsp
updbearerrespaccept
updbearerrespdeniedCtxtNotFound
updbearerrespdeniedInvalidMsgFormat
updbearerrespdeniedMandIEIncorrect
updbearerrespdeniedMandIEMissing
updbearerrespdeniedNoResourcesAvl
updbearerrespdeniedSemanticErrinTFT
- updbearrespdeniedSyntacticErrinTFT
- updbearrespdeniedSemanticErrinPktFltr
- updbearrespdeniedSyntacticErrinPktFltr
- updbearrespdeniedUENotResponding
- updbearrespdeniedUERefuses
- updbearrespdeniedUnableToPageUE
- updbearrespdeniedRequestRejected
- updbearrespdeniedUnableToPageUeSuspend
- updbearrespdeniedCondIEMissing
- updbearrespdeniedInvalidRemotePeerReply
- updbearrespdeniedPeerNotResponding
- updbearrespdeniedTempRejDueToHOProgress
- updbearrespdeniedOtherCause

show apn name

The following new field has been added:
- APN QCI Stats

CSCum17370 - PDN session handling for Invalid IMEI & IMSI-less devices

Feature Changes
PDN Session Handling for Invalid IMEI and IMSI-less Devices

Due to legacy devices in the network which are configured with invalid IMEI or provide invalid IMEI to the network, it is possible that different UEs may report the same IMEI, resulting in duplicate IMEI in the network. In other scenarios, it is possible that IMEI is completely missing. In most scenarios, when IMSI is available and valid, the network can handle the subscriber session. For UEs that do not have valid IMSI and attach to the network for emergency PDN, a duplicate IMEI could be an issue because a unique index is not available for MME, S-GW, and P-GW to identify the user.

CSCum17389 - Dependency to support Per APN, and QCI, GTP-C v2 responses

Feature Changes

eGTP-C Statistics Enhancements

New counters and bulk statistics have been introduced to collect more granular GTP-C statistics on per APN QCI level to monitor certain KPIs.

See CSCum17169 for additional information.
Customer Impact: This feature allows operator to collect more granular GTP-C statistics on per APN per QCI level to monitor certain KPIs based on these statistics.

CSCum17434 - AAA provide Restoration Priority Indicator to PGW

Feature Changes

Restoration Priority Indicator Support

In order to distinguish VoLTE Capable IMS PDN connections from Non-VoLTE capable IMS PDN connections, support has been added for AAA provided priority value via a new S6b AVP during authentication.

Previous Behavior: Earlier restoration priority indicator was not available from AAA.

New Behavior: Restoration Priority indicator is now received from AAA across the s6b interface. Corresponding stats are maintained, and the relevant values can be seen through CLI.

Customer Impact: The customer will now be able differentiate the Volte subscriber from non-volte subscriber based on the value of restoration priority.

Command Changes

show pdn-connection-count

This new command displays the current number of PDN connections for each of the Restoration-Priority-Level values (1 to 8).

show pdn-connection-count restoration-priority-level (priority_level | all)

Notes:

- restoration-priority-level: Restoration priority associated with PDN connection.
- priority_level: Restoration priority value. Must be an integer from 1 through 8.
- all: Displays number of PDN connections associated with all restoration priorities.

Performance Indicator Changes

<name> Schema

<Brief description then list new/modified/deprecated stats>

show subscribers ggsn-only full all

Following new variables has been added in the output of the above command to display the specified restoration priority

- Restoration priority level: Identifies the restoration priority value associated with the PND connection.
• **Total subscribers matching specified criteria**: Identifies the total number of subscribers matching criteria for restoration priority value associated with the PND connection.

**show bulkstats variables**

The show bulkstats variables statistics are modified to display the following new variables for SAEGW schema in case of colocation with GGSN.

- `ggsn-pdns-restore-priority-1`
- `ggsn-pdns-restore-priority-2`
- `ggsn-pdns-restore-priority-3`
- `ggsn-pdns-restore-priority-4`
- `ggsn-pdns-restore-priority-5`
- `ggsn-pdns-restore-priority-6`
- `ggsn-pdns-restore-priority-7`
- `ggsn-pdns-restore-priority-8`

The new variable in the show bulkstat variables schema for displaying the associated schema.

- `current-pdn-restore-priority-1`

**CSCum42664 - Bit Rate mapping across Gx and GTP based interfaces**

**Feature Changes**

**Bit Rate Mapping Across Gx and GTP-based Interfaces**

Bit rate granularity provided by different interfaces was not aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

With this feature, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up.

**Previous Behavior**: Previously, rounded-down kbps bitrate (AMBR, MBR, BGR) values were being sent towards the Access side.

**New Behavior**: Bitrate granularity is still maintained per the current interface specifications but 3GPP provides explicit guidance that whenever the conversion from bps to kbps results in decimal values, the node converting should round the value up.

Introduced a new CLI command under GGSN service `[no] gtpc bit-rates-rounded-down-kbps` to control the behavior of rounding-up. The CLI command will enable/disable the old behavior of rounding down. By default, this CLI command is configured to use rounded-up bitrate values. Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value will be sent on GTP interface towards the Access side.

**Customer Impact**: This feature provides for more consistent behavior and ensures correct bandwidth is allocated for bearers.
CSCum51838 - GGSN Support for PCSCF Discovery

Feature Changes

GGSN Support for PCSCF Discovery

<description>

**Previous Behavior:** The Existing code for GGSN supported P-CSCF address discovery based on only the IMSA based table lookup. The other P-CSCF discovery mechanisms like DNS query are not supported.

**New Behavior:** To ensure parity between PGW and GGSN, implementation for deriving P-CSCF addresses from the various interfaces/local configuration has been done. Following is the desired order of sequence in which P-CSCF address is to be fetched and returned:

- P-CSCF info from S6b FQDN based DNS query
- P-CSCF info from Config FQDN based DNS query
- P-CSCF info from IMSA configured table
- P-CSCF info from APN config

P-CSCF Discovery would be performed inline with respect to the Call establishment Handoff Procedure and could refer to the stored FQDN information. In addition to the above enhancements, following points have also been supported:

- Storing of discovered P-CSCF IPv4 and IPv6 addresses
- SR/ICSR Recovery of P-CSCF IP addresses
- Persistence of FQDN information
- Persistence of P-CSCF values across gngp handoff
- Unification of the P-CSCF Address Element

CSCum56817 - Use of well-known APN for Customer-specific 4G subs

Feature Changes

Use of Well-known APN for 4G Subscribers

This feature is supported through virtual APN feature.

CSCum66168 - DHCPv6: IPv6 default pregfix AAA and Delegated Prefix Corelation

Feature Changes

AAA and Prefix Delegation DHCP Correlation
Currently at the DHCP server, DHCPv6 does not provide any mechanism to correlate allocated IPv6 (/64) prefix to a particular subscriber. This feature correlates the default prefix allocated from AAA server with the delegated prefix allocated from external DHCPv6 server during the PDN connection setup.

New options to an existing CLI in DHCP Client Profile Configuration mode to enable GGSN to send USER_CLASS_OPTION in DHCPv6 messages to external DHCPv6 server during delegated prefix setup.

**Important:** This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Customer Impact:** This feature allows different configurations for GTP-C echoes as compared to the non-echo messages.

### Command Changes

#### enable

A new option `user-class-option` has been added along with some other options within it to configure whether imsi or msisdn should be sent in the user class option.

```plaintext
configure

context context_name

dhcp-client-profile profile_name

    enable user-class-option { imsi | msisdn }

end
```

**Notes:**

- **enable user-class-option imsi**: This CLI triggers sending the "User_Class_Option" with UE's IMSI in the DHCPv6 messages from PGW/GGSN to the external DHCPv6 server during DHCPv6 Prefix Setup.
- **enable user-class-option msisdn**: This CLI triggers sending the "User_Class_Option" with UE's MSISDN in the DHCPv6 messages from PGW/GGSN to the external DHCPv6 server during DHCPv6 Prefix Setup.

#### disable

A new option `user-class-option` has been added to disable sending the user class option in the messages from PGW/GGSN to the external DHCPv6 server during DHCPv6 Prefix Setup.

```plaintext
configure

context context_name

dhcp-client-profile profile_name

    disable user-class-option

end
```

**Notes:**
• disable user-class-option: This CLI disables sending the "User_Class_Option" in the DHCPv6 messages from GGSN to the external DHCPv6 server during DHCPv6 Prefix Setup.

CSCum88464 - Intelligent graceful PDN disconnection during maintenance-mode

Feature Changes

Intelligent Graceful PDN Disconnection During Maintenance Mode

When a gateway is in maintenance mode and new-call policy is enabled at a service or APN level, it only rejects new calls as the rejection is at the demux. For PDNs that have dedicated bearers, even though the APN is in maintenance mode, since the default bearer is already up, network-initiated dedicated bearers will still be accepted by the gateway and thus block clearing of all PDNs. CLI has been added to clear the entire PDN when the last VoLTE dedicated bearer goes down.

Command Changes

clear subscribers

auto-delete is a new keyword that enables auto deletion when PDN connections that do not have an active voice call are disconnected.

clear subscribers apn apn_name non-volte-call auto-delete [ max-subscribers max_count ] [ uniform ]

clear subscribers all non-volte-call auto-delete [ max-subscribers max_count ] [ uniform ]

Notes:

• auto-delete: Clears the PDN/call when the last VoLTE dedicated bearer goes down for P-GW, S-GW, SAEGW, GGSN, and ePDG.

Calls will not be cleared when one of the calls in a multiple PDN scenario is a VoLTE PDN. When the VoLTE PDN goes down, all of the other PDNs found for the same IMSI are brought down, which will bring down the call automatically.

• max-subscribers: (existing keyword) The maximum number of subscribers to be cleared.

  max_count must be an integer from 0 through 20000000.

• uniform: (existing keyword) Subscribers will be cleared uniformly.

• This assumes that new call policy has been configured on the node to reject any new calls so that these new calls get directed to an alternate PDN before clear subscribers command is executed.
Performance Indicator Changes

**show session disconnect-reasons verbose**

The following disconnect reason is used to indicate the percentage of the total number of sessions that have been auto deleted.

- session-auto-delete(588)

**CSCum98092 - MS-to-MS traffic for Ipsec**

Feature Changes

**MS-to-MS traffic for IPSec**

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.

```
configure

context context_name
```
[ default | no ] ip guarantee framed-route local-switching variable
dend

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.

CSCun51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change

Feature Changes

Gn-Gp Handoff enhancement

Previous Behavior: UE support for BCM was unknown on HO from PGW to GGSN and so BCM would not be derived as expected.

New Behavior: With new changes even if PCO IE is not sent in HO indication to GGSN but previously sent to PGW during call setup, BCM will be derived based on UE support in PGW.

Customer Impact: BCM mode will be derived based on UE and SGSN support on HO rather than assuming BCM in PGW to be always by UE.

CSCun91294 - Inactivity timeout to be displayed under Session Release Reasons

Feature Changes

Inactivity timeout to display under Session Release Reasons

Currently stats for session disconnected due to inactivity timeout is maintained in field “idle timeout”, but their should be a separate field in Session Release Reasons from output of CLI show gtpc statistics verbose to maintain stats for session cleared due to inactivity timeout. Also, the same to be displayed under bulkstat files.

CSCuo77196 - NAS-Port-Id support on GGSN.

Feature Changes

NAS-Port-Id support on GGSN
Addition of some new RADIUS attributes has been done via some new CLIs.

**Previous Behavior:** Previously, as per the configuration guide, the attribute is mentioned as supported, but it was never sent as part of any RADIUS messages because the attribute was never supported in the first place. It was defined in starent.attr file only for encoding/decoding purposes.

**New Behavior:** Now, support has been provided for the NAS-Port-Id AVP in Access-request and Accounting-Start messages for both GGSN and PGW calls. Even then, the attribute is not sent by default, if any customer wants to send the attribute, the same should be explicitly enabled using "radius attribute" config.

**Customer Impact:** If the customer does not have GGSN session licence, there would not be any impact, as the CLI would not be visible and the AVP will not be sent in the messages.

Existing customers with GGSN session license who use starent dictionary or a custom dictionary which encompasses starent dictionary will not face any impact. If they need the AVP to be present in their RADIUS messages, they can do so by using the "radius attribute" CLI. The CLI will be displayed in verbose mode.

**CSCuo95634 - P-CSCF Info (PCO IE) for Secondary Context/ Update PDP Rsp**

**Feature Changes**

**P-CSCF Info for Secondary Context/ Update PDP Rsp**

GGSN Support for PCSCF Discovery refers to maintaining Parity between PGW and GGSN implementations as far as P-CSCF discovery is concerned. But there is an inherent difference between the message exchanges for the two services.

- The Create Bearer Request is Network driven for PGW against Create PDP Req (secondary context) which is Access side driven for GGSN. Thus the Create PDPReq(secondary context) can request for P-CSCF Address information which the Create Bearer Req (PGW) cannot.
- Similarly the Update Bearer Request is Network driven for PGW against Update PDP Req which is Access side driven for GGSN. P-CSCF Address information can be requested via Update PDP Req.

**Previous Behavior:** Following Test cases arise as a result:

- Verify GGSN behavior when Secondary PDP request from access side carries P-CSCF address request but the primary CPCQ did not
- Verify GGSN behavior when the Update PDP context from the access side carries P-CSCF request whereas CPCQ did not
- Check GGSN behavior when secondary pdp context requests for P-CSCF address of ipv6 type and primary was established with v4 CSCF address
- Check GGSN behavior when secondary pdp context requests for P-CSCF address of ipv4 type and primary also was established with v4 CSCF address

**New Behavior:** The P-CSCF discovery would be initiated ONLY as part of Initial Attach (PGW) and Create PDP Context (Primary) for GGSN. Subsequently, as part of Create PDP Context (Secondary) and Update PDP procedure, the P-CSCF Address information, if requested, would be returned as part of the corresponding Response procedure(PCO IE), provided the P-CSCF Address Information is ALREADY Discovered. In other words, a new P-CSCF discovery would NOT be triggered upon receiving P-CSCF Address request as part of Secondary context creation or Update PDP request. The existing discovered information would be returned appropriately.
CSCuo96798 - Counter type is not correct for all the variables of gtpc schema

Feature Changes

Output Change for GTPC Schema CLIs

Previous Behavior: Counter types were displayed “None” for most of the variables of GTPC schema
New Behavior: Appropriate type has been displayed for all the variables of GTPC schema.

CSCup51146 - Counter type is not correct for all the variables of apn schema

Feature Changes

show bulkstat variables apn output change

Output of the show bulkstat variables apn CLI has been updated to correct the counter type for all the variables of APN schema
Previous Behavior: Show CLI used to show most of the counter types as none.
New Behavior: show CLI will show appropriate counter types now.

CSCzn41068 - ICSR support for L2TP on GGSN/PGW

Feature Changes

ICSR support for L2TP on GGSN

This feature has been integrated in order to support the recovery of L2TP LAC sessions with ICSR on GGSN/PGW (chassis running GGSN/SGW/PGW combo).

CSCzn23942 - CLI: Content-insert does not take a string up to 1023 characters as men

Feature Changes

The size of string that can be inserted with the cli analyze priority 4 category TECH action content-insert <string> has been reduced

Previous Behavior: String of length 1023 could be inserted as content insertion action.
New Behavior: String of length 767 can be inserted as content insertion action.
Chapter 6
GTPP Changes in Release 17

This chapter identifies GTPP management features and functionality added to, modified for, or deprecated from GTPP in StarOS 17 software releases.
GTPP Enhancements for 17.3

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.

**CSCts50004, CSCum62796 - IPSG:EGCDR is not working with subscriber profile**

**Applicable Products:** IPSG

**Feature Changes**

**eG-CDR for CDMA Subscribers**

**Previous Behavior:** Support for eG-CDR generation for CDMA traffic was not available in the earlier releases.

**New Behavior:** IPSG now generates eG-CDR records for CDMA traffic with these additional fields:

- Subscriber profile name
- PDSN IP Address
- BSID (CDMA)
- Online Charging Flag
- Event Type (causeForRecClosing)

These fields are added to a newly defined GTPP dictionary “custom49” based on custom6 GTPP dictionary.

**Command Changes**

**gtpp group**

This is a new command added to the subscriber profile configuration to support eG-CDR generation for CDMA calls.

**configure**

```bash
context context_name

subscriber name subscriber_name

gtpp group group_name
```
CSCut59336 - Support for RAT-Type EUTRAN in eGCDRs

Applicable Products: IPSG

Feature Changes

Support for EUTRAN RAT-Type in eG-CDRs

**Previous Behavior:** The eG-CDRs were generated with RAT Type field as GERAN when RAT Type is eUTRAN.

**New Behavior:** Now, the RAT Type CDR field is populated with the value “eUTRAN” for eG-CDRs on IPSG when RAT Type is eUTRAN.
GTPP Enhancements for 17.0

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.

CSCub32971 - GGSN/PGW support customer’s customized processing on Gy interface

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

**Feature Changes**

**Customized Behavior for Handling Failure on Gy Interface**

A new GTPP dictionary “custom47” has been created and configured for P-GW CDRs for customizing the failure handling procedure when Gy link is down. This dictionary is used along with custom21 GGSN dictionary for a combo deployment of GGSN and P-GW.

The custom21 dictionary includes these additional customizations:

- Addition of PS-FCI field to CDRs
- Filling of custom values for free format data in the PS-FCI field.

**Important:** This feature is a customer-specific implementation.

CSCuf73716 - PI: The CLI "accounting-mode radius-diameter" is not for diameter

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

**Command Changes**

*accounting-mode*

This command is used only for RADIUS and GTPP accounting, and not for Diameter interfaces. So, the CLI command “accounting-mode radius-diameter” under APN configuration is modified as “accounting-mode radius”. 
configure

context context_name
   apn apn_name
      accounting-mode radius
   default accounting-mode
end

Notes:
- The existing keyword “radius-diameter” is concealed to support backward compatibility.

CSCul26544 - Incorrect pdpType for a ipv4v6 call in GCDR

Applicable Products: GGSN

Feature Changes

PDPType for IPv4v6 Calls

Previous Behavior: For an IPv4v6 call, G-CDR showed value of pdpType as IPv4v6 only if the CLI command “gtpp attribute served-pdp-pdn-address-extn” is enabled. If this CLI is not configured, G-CDR showed the value as IPv6 even though it was an IPv4v6 call.

New Behavior: For an IPv4v6 call, G-CDR shows the value of pdpType as IPv4v6 irrespective of the CLI being configured or not.

Customer Impact: pdpType in G-CDR will be ipv4v6 if it is an ipv4v6 call.

CSCum25831 - PI: Accounting mode GTPP and gtpp group config should be shown in apn

Applicable Products: GGSN, P-GW

Feature Changes

CLI Display Modification

The default configuration of accounting mode in APN is “accounting-mode gtp”. When “show configuration” is executed, if it is a default configuration, then the default value will not be displayed. As part of this enhancement, the accounting mode will always be displayed even if it is a default mode.

Previous Behavior: The default value of “accounting-mode gtp” was not displayed in the “show configuration” command. The value was only displayed in the output of “show configuration verbose” command.
**New Behavior:** Even for a default configuration of `accounting-mode` under APN, this will be indicated in “`show configuration`” both in verbose and non-verbose modes.

**CSCum59328 - GTPP requests should be sent to any available CGF server in a group**

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

**Feature Changes**

**Load Balancing of CGF Servers**

It has been verified that the gateway performs load balancing of the CDRs across all the available CGF servers. CDRs for a given session can be sent to any available CGFs. If one CGF goes down, the CDRs are distributed to all other available CGFs.

**CSCum75381, CSCuj46390, CSCuj46415, CSCuj46585, CSCuj46276, CSCuj46607, CSCuj46305, CSCuj46287, CSCum99212, CSCuo15607, CSCuo15880, CSCuo16109, CSCuo75689, CSCuo75713 - CDR module restructuring : Phase-II**

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

**Feature Changes**

**Redesign of CDR Module**

**Previous Behavior:**
- Dictionary-specific checks were present all over the code. For any new feature enhancements or incremental changes, code-changes were time-consuming and error-prone.
- The default GTPP dictionary is starent.
- In release 16.0, a new flexible and extensible framework was implemented to generate eGCDR and PGW-CDRs. Customer had to use “`gtpp egcdr new-path`” CLI command to use the new CDR framework.

**New Behavior:**
- This new framework has been extended to define a GTPP dictionary in a structured format using a “Dictionary Definition Language (DDL)”. Using this language, customers can clearly define fields, triggers and behaviors applicable for a particular GTPP dictionary.
  - DDL text file will be parsed at compilation time and metadata will be populated to generate eGCDR and PGW-CDR. This metadata makes the new framework more modular and maintainable. This will help in faster turnaround time in supporting any new enhancements.
- Customers should explicitly configure the dictionary as there will be no default dictionary. If no dictionary is configured, then eGCDR/PGW-CDR will not be generated.
From this release, all GTPP dictionaries shift onto the new CDR framework. “gtpp egcdr dynamic-path” CLI command is configured to use field-modified dictionary DDL.

**Customer Impact:** If customer wants to use new framework for customized/field defined CDR generation, customer should enable CLI “gtpp egcdr dynamic-path” in GTPP Group Configuration mode. This CLI command is used to support field modified dictionary DDL. “gtpp dictionary customXX” CLI command is operational as before for configuring the predefined GTPP dictionaries.

When customer wants to add/modify/remove a field, this information has to be updated in DDL. The DDL file is processed dynamically and the field reflects in CDR. This framework works only for eGCDR and PGW-CDR.

**Command Changes**

**gtpp egcdr dynamic-path**

dynamic-path is a new keyword in this command to enable field defined (customer created) eGCDR and PGW-CDR generation.

configure

context context_name

gtp group group_name

gtp egcdr dynamic-path ddl-path

{ default | no } gtp egcdr dynamic-path

dcl

Notes:

- **dynamic-path**: Enables the user to load the customized or modified dictionary. The dictionary configured through this CLI command takes precedence over the existing gtp dictionary CLI command.

- **ddl-path**: Specifies the path of dictionary DDL. The path must be a string of size 0 through 127. This is to support field-loadable DDLs. The DDL file will be parsed to populate metadata required to generate eGCDR/PGW-CDR.

- It is not recommended to enable gtpp egcdr dynamic-path when there are active calls.

**CSCum79565, CSCum47539, CSCum47494 - CDR support for including LAPI (signaling priority)**

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

**Feature Changes**

**Support for Low Access Priority Indicator in CDRs**

A new GTPP attribute “LowPriorityIndicator” is defined in CDR for custom35 and custom40 GTPP dictionaries as per the Release 10 3GPP specification of 32.298. If S-GW/P-GW receives Low Access Priority Indicator (LAPI) in GTPP
message, then the CDR will contain the LowPriorityIndicator attribute value. The LAPI Information Element (IE) is introduced in Create Session Request for indicating that the PDN is of low priority.

**Command Changes**

```plaintext
gtpp attribute

A new keyword “lapi” has been added to this command to control the presence of Low Access Priority Indicator (LAPI) attribute in S-CDRs.

configure

case context_name

gtpp group group_name

[ default | no ] gtpp attribute lapi

end
```

Notes:
- When UE indicates low priority connection, then only “lowPriorityIndicator” attribute will be included in the PGW-CDR.

### CSCum85305 - sponsor ID should be populated in the PGW-CDR

**Applicable Products:** P-GW

**Feature Changes**

**Configuration Support for Sponsor ID and Application Provider ID Attributes**

This feature aims at including the attributes “Sponsor ID” and “Application-Service-Provider-Identity” in PGW-CDR under LOSDV if the PCEF supports Sponsored Data Connectivity feature and the required reporting level is sponsored connectivity level as described in 3GPP TS 29.212. This feature can be enabled by configuring the CLI command “gtpp attribute sponsor-id” in GTPP Group Configuration mode.

This feature has been implemented to be in compliance with Release 11 3GPP specification for CDRs. So, this behavior is applicable only to custom35.

**Customer Impact:** Customer should use custom35 GTPP dictionary and configure the `gtpp attribute sponsor-id` command to include the Sponsor ID and Application Provider ID attributes in PGW-CDRs.

**Command Changes**

```plaintext
gtpp attribute

A new keyword “sponsor-id” has been added to this command to control the presence of Sponsor ID and Application Provider ID attributes in PGW-CDRs.
configure

context context_name

gtpp group group_name

[ default | no ] gtpp attribute sponsor-id

end

CSCum85499 - Support for LAPI bit in SCDR

Applicable Products: SGSN

Feature Changes

Encoding of LAPI in S-CDRs

This release provides support for Low Access Priority Indicator (LAPI) attribute in SGSN CDRs for custom24 GTPP dictionary. This attribute field indicates if the PDN connection has a low priority, i.e. for Machine Type Communication (MTC).

This attribute is required to support MTC feature in SGSN. This attribute will be included in SGSN CDRs only if the CLI command “gtpp attribute lapi” is configured.

Command Changes

gtpp attribute

A new keyword “lapi” has been added to this command to control the presence of Low Access Priority Indicator (LAPI) attribute in S-CDRs.

configure

context context_name

gtpp group group_name

[ default | no ] gtpp attribute lapi

end

Notes:

• When UE indicates low priority connection, then only “lowPriorityIndicator” attribute will be included in the SGSN-CDR.

CSCum85810 - Support for LAPI bit in SGWCDR

Applicable Products: S-GW
Feature Changes

LAPI in SGW-CDRs

As part of MTC feature support in S-GW, Low Access Priority Indicator (LAPI) attribute is supported in SGW-CDR. This field indicates if the PDN connection has a low priority, i.e. for Machine Type Communication. SGW-CDR for custom24 and custom35 GTPP dictionaries have information about LAPI if the CLI command “gtpp attribute lapi” is configured.

Command Changes

gtpp attribute

A new keyword “lapi” has been added to this command to control the presence of Low Access Priority Indicator (LAPI) attribute in SGW-CDRs.

configure

  context context_name

  gtp group group_name

    [ default | no ] gtpp attribute lapi

  end

Notes:

- When UE indicates low priority connection, then only “lowPriorityIndicator” attribute will be included in the SGW-CDR.

CSCun71456, CSCup62539 - Diff order of supportzone config causes stranded CDR stuck

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

Feature Changes

Changes to HDD Directory Structure

The directory name creation logic for GTPP HDD is changed. Previously, vpn-id is used as part of the directory name. This logic is changed to include the GTPP accounting context-name.

Previous Behavior: The CDRs were placed in the following directory paths for local mode:

RAM-disk: /records/cdr/<gtpp-group-name><vpn-id>
HDD: /hd-raid/data/records/cdr/<gtpp-group-name><vpn-id>

For GTPP streaming mode, the directory structure was as follows:

RAM-disk: /records/cdr/hdd_sec_stor_<gtpp-group-name><vpn-id>
HDD: /hd-raid/data/records/cdr/hdd_sec_stor_<gtpp-group-name><vpn-id>

**New Behavior:** The CDRs are now placed in the following directory paths for local mode:
- RAM-disk: /records/cdr/<gtpp-group-name>_<context-name>
- HDD: /hd-raid/data/records/cdr/<gtpp-group-name>_<context-name>
  
For streaming mode, the directory structure is as follows:
- RAM-disk: /records/cdr/hdd_sec_stor_<gtpp-group-name>_<context-name>
- HDD: /hd-raid/data/records/cdr/hdd_sec_stor_<gtpp-group-name>_<context-name>

**CSCuo75702 - CDR module restructuring : Integration changes**

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

**Feature Changes**

**Configuration Support for Direct Tunnel Attribute**

**Previous Behavior:** Earlier, the “gtpp trigger direct-tunnel” has been used to control the presence of Direct-Tunnel Record Extensions attribute in the CDR.

**New Behavior:** Now with the implementation of new CDR framework, a new CLI command “gtpp attribute direct-tunnel” has been introduced to control the presence of Direct-Tunnel Record Extensions attribute in the CDR.

**Customer Impact:** Customer will have to use “gtpp egcdr dynamic-path” CLI command to use the new CDR framework. Then, the customer should use the “gtpp trigger direct-tunnel” command to trigger CDR for direct-tunnel, and the “gtpp attribute direct-tunnel” to display direct-tunnel in CDR.

**Command Changes**

`gtpp attribute`

A new keyword “direct-tunnel” has been added to this command to control the Direct-Tunnel attribute to be present in GGSN/P-GW CDRs.

configure

```
context context_name

  gtpp group group_name

    [ default | no ] gtpp attribute direct-tunnel

end
```

**CSCup04619 - PGW-Gz CDR HDD: CGF parse shows few AVPs incorrect**

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

Corrected CGF Parsing Errors

The following CDR attributes parsed through CGF have been modified to maintain them in sync with the output of monitor protocol command.

- p-GWAddress -> p_GWAddress
- servinggNodePLMNIdentifier -> servingNodePLMNIdentifier
- p-GWPLMNIdentifier -> p_GWPLMNIdentifier

CSCup08800 - gtpp egcdr new-path cli

Applicable Products: GGSN, P-GW

Feature Changes

CLI Support for New CDR Framework

In this release, the existing CLI command “gtpp egcdr new-path” is concealed to keep the release backward compatible and its functionality is now being supported using the CLI command “gtpp egcdr dynamic-path”.

Previous Behavior: The CLI command “gtpp egcdr new-path” was used to switch between old and new path for CDR generation.

New Behavior: From this release onwards there is only one flow at ECS, so no new path/old path for CDR generation. The CLI behavior is changed so that instead of working as switch for old path / new path for CDR generation, it acts as the medium to provide path for dynamic /customized ddl. The existing CLI command has been modified as “gtpp egcdr dynamic-path”.

Command Changes

gtpp egcdr dynamic-path

dynamic-path is a new keyword in this command to enable the new framework for eGCDR and PGW-CDR generation.

configure

context context_name

gtpp group group_name

gtpp egcdr dynamic-path ddl-path

{ default | no } gtpp egcdr dynamic-path

end

Notes:
- **dynamic-path**: Activates the new framework for eGCDR/PGW-CDR generation.
- **ddl-path**: Specifies the path of dictionary DDL. The path must be a string of size 0 through 127. This is to support field-loadable DDLs. The DDL file will be parsed to populate metadata required to generate eGCDR/PGW-CDR.
- It is mandatory to configure "gtpp dictionary ..." before enabling `gtpp egcdr dynamic-path` CLI command.
- It is not recommended to enable `gtpp egcdr dynamic-path` when there are active calls.

**CSCup52199 - cust21: incorrect encoding, tag 28 used for FCI and rATType**

_applicable products: GGSN_

**Feature Changes**

**New CDR Attributes in custom21 GTPP Dictionary**

*Previous Behavior*: RAT Type attribute field was not included in the GGSN CDRs. This behavior was as per the 3GPP TS 32.215 v4.5(R4) specification.

*New Behavior*: Now, the RAT Type, PS FCI and Diagnostics fields are added to the GGSN CDRs for custom21 GTPP dictionary.

**Important**: This new behavior is a customer-specific implementation.

**CSCuq21862 - Changing the default monpro to new routines from 17.0 onwards.**

_applicable products: GGSN, P-GW_

**Feature Changes**

**Record based Selection of Decode Routines**

*Previous Behavior*: For switching CDRs to new decode routines, an option “P” was selected from the output of `monitor protocol` command.

*New Behavior*: The option “P” is no longer selected for switching to decode routines. Now the decode routines will be automatically selected based on the record type.

**CSCuq44420 - qosInformationNeg is not seen in LOSDV with different service-id**

_applicable products: GGSN_
Feature Changes

QOS-Info IE in LOSDVs for Rel. 8 / Rel.10 Dictionaries

**Previous Behavior:** If in the CDRs there are multiple LOSDVs with same content-id and different service-identifiers, then QOS-Info Information Element (IE) was included only in the very first LOSDV and not in the subsequent LOSDVs unless its previous LOSDV was closed for QoS change.

**New Behavior:** The current implementation has been modified to include QOS-Info in all LOSDVs having different combination of service-id and content-id. Thus if there are multiple LOSDVs with same content-id but different service-id, QOS-Info will be present in every such LOSDV.

**Important:** This behavior change is applicable to Rel.8 and Rel.10 compliant GTPP dictionaries.
Chapter 7
HA Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from HA in StarOS 17.0 software releases.
HA Enhancements for 17.4

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.

---

**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 HA.

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

---

**CSCuu74619 - 3GPP2 CVSE GRE Key encoding for PMIP**

**Feature Changes**

**Support sending of GRE key in CVSE format by FA**

---

**Important:** This feature is a customer-specific enhancement. For more information, contact your Cisco account representative.

**Previous Behavior:** Cisco FA sends GRE key in proprietary NVSE format. CISCO HA used the same GRE Key in Downlink traffic and also did not send GRE Key in MIP Registration Reply message.
**New Behavior:** New configuration is added which can be enabled at FA to encode GRE Key in CVSE format. CISCO HA sends GRE Key back to FA in CVSE format, if MIP Registration Request is received with GRE Key in CVSE format. HA may send different value in GRE Key CVSE.

**Command Changes**

```plaintext
mobile-ip send

The 3gpp2-gre-cvse keyword is introduced in the mobile-ip send command, under the Subscriber Configuration Mode to support sending of GRE key in CVSE format by FA to HA in MIP RRQ.

configure

case context context_name

subscriber { default | name variable }

    mobile-ip send 3gpp2-gre-cvse

    [ default | no ] mobile-ip send 3gpp2-gre-cvse

end
```

**Notes:**
- By default this CLI will be disabled i.e. this CLI should be configured if the feature needs to be turned ON.
- This CLI is applicable for FA service only, and not for HA service.
Chapter 8
HeNBGW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 17 software releases.
HeNBGW Enhancements for 17.2

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HeNBGW 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 HeNBGW.

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

---

CSCuq12965 - DHCPv4 Proxy support for HeNBGW with IPSec

**Feature Changes**

**DHCP support**

The DHCPv4 proxy functionality on the SeGW integrated with HeNBGW is to update the DHCP messages with the HeNB Id in DHCP Option 61 (Client ID) and forward the DHCP messages to an external DHCP server.

1. The SeGW forwards DHCP requests from a LTE FAP to an external DHCP server during IPSec Setup.
2. The SeGW adds LTE FAP Id in the Client Identifier (CID) of the DHCP messages.
3. The PNR then receives these DHCP requests maintains a mapping between the LTE FAP ID and the assigned “Inner” IP Address
4. The RMS queries the PNR to get the LTE FAP inner IP Address, to use this inner IP Address to send TR-069 Connection Requests to the LTE FAP.
HeNBGW Enhancements for 17.1

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HeNBGW 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 HeNBGW.

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

---

**CSCuo53133 - [ePDG]: IPsec subsys needs enh to supp mul auth method for 1 crypo temp**

**Feature Changes**

**IPsec Sub System enhancement**

**Previous Behavior:** HeNBGW (SecGW) used to support any one type of IPSec Authentication scheme either PSK, EAP-AKA or Certificate based at any given point of time.

**New Behavior:** HeNBGW (SecGW) is able to support EAP-AKA, Certificates and PSK IPSec authentication simultaneously under the same Crypto template associated to HeNBGW Access service.

**Customer Impact:**
HeNBGW Enhancements for 17.0

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *HeNBGW 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 HeNBGW.

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

---

**CSCub79822 - HeNBGW: Support for TRACE procedure**

**Feature Changes**

**Support for TRACE procedure**

Trace procedure support on HeNBGW

**Previous Behavior:** HeNBGW support was not available for handling trace procedures.

**New Behavior:** HeNBGW supports relaying of S1AP Trace procedures to and from HeNBs/MME.

**Customer Impact:** HeNBGW will be able to forward trace procedures when received from MME/HeNB.
CSCu58078 - HeNBGW: nwsvc- not handling Overload Start Stop msg from MME

Feature Changes

Handling Overload Start Stop msg from MME

Overload start messages when received from MME(s) are sent to HeNBs using that Logical eNodeB as per received or configured Traffic Load Reduction value.

Overload Stop are sent to Henbs when received from MME(s) for which Start has been sent.

Previous Behavior: Overload messages used to get dropped on HeNBGW when received from MME.
HeNBGW will send HeNBGW GUMMEI to HeNB with S1 SETUP Response message to HeNB.

New Behavior: On receiving MME Overload Start message, HeNBGW shall use the Traffic Load Reduction Indication IE to determine the percentage of HeNBs (attached to the same logical eNB which receives the message) to which Overload Start message need to be relayed. If Traffic Load Reduction Indication IE is not present in the message, HeNBGW will relay the message to a configurable percentage of HeNBs.

HeNBGW also supports Automatic and Manual configuration to send Overload Stop if not received from MME.
HeNBGW will send aggregated GUMMEI list from all MMEs in a MME-pool of logical enodb to HeNB with S1 SETUP Response message to HeNB. Also GUMMEI list status changes for any MME (i.e. lost SCTP connection to MME, new MME connections is up or receive MME configuration Update message which changes GUMMEI list for a MME) shall be broadcasted to all HeNB attached to the logical eNB using MME configuration Update Message.

Customer Impact: Overload start and stop messages received from a MME are correlated as per received or configured TLR which reduces signaling towards that MME.

Command Changes

henbgw overload-control load-reduction-indicator Percentage_Value

This Command is used to configure load-reduction value in %ge of henbs if the Overload start message received from MME doesn't include TLR IE.

configure
lte-policy
   henbgw overload-control load-reduction-indicator Percentage_value
   [ default ] henbgw overload-control load-reduction-indicator
end

henbgw overload-control ochl-guard-time minutes

This configured timer after expiry automatically defines henbgw to send Overload Stop to all Henbs if not received from MME(s) irrespective from which start was received.

configure
lte-policy

    henbgw overload-control ochl-guard-time minutes

    [ default ] henbgw overload-control ochl-guard-time

    end

henbgw overload-control stop

    Manual way of sending Overload Stop to all henbs if not received from respective MME(s).

    henbgw overload-control stop

show lte-policy henbgw overload-control

    This command is used to view the configured Load-reduction-indicator and ochl-guard-time.

    show lte-policy henbgw overload-control

Performance Indicator Changes

SNMP MIB

As part of this release, the following new SNMP MIBs are added for starHENBGWMMEOverloadStart :

- starHENBGWServiceVpnName
- starHENBGWServiceServName
- starHENBGWServiceLogicalENBId
- starHENBGWServiceMMEServName
- starHENBGWServicePeerAddr
- starHENBGWServicePeerPort
- starHENBGWServiceTLRI

As part of this release, the following new SNMP MIBs are added for starHENBGWMMEOverloadStop :

- starHENBGWServiceVpnName
- starHENBGWServiceServName
- starHENBGWServiceLogicalENBId
- starHENBGWServiceMMEServName
- starHENBGWServicePeerAddr
- starHENBGWServicePeerPort

show henbgw-network-service mme-association full all

    This command introduces the following new parameters:

    - Served GUMMEI list
- Rat ID
- Served MMECs
- Served GROUP IDs
- Served PLMNs
- Last received overload start message
- Last received/configured TLRI (Percentage)

Currently there is support to display associated GUMMEI List for each Logical eNB and MME association and also the received time of Overload start message and TLR IE Percentage value.

**show henbgw-access-service henb-association full all**

This command also shows the Overload status of individual henb by setting it to True/False:

- MME Overload Start Msg Sent

**CSCum00843 - Cell Broadcast Support (CMAS)**

**Feature Changes**

**Cell Broadcast Support (CMAS)**

Broadcast Delivery of warning messages to relevant Henbs connected to Henbgw based on Warning Area List IE.

**Previous Behavior:** Write-Replace Warning/Kill procedures were not handled on HeNBGW.

**New Behavior:** Write-Replace-Warning and Kill procedures handling are supported on HeNBGW.

**Customer Impact:** HeNBGW will be able to support Write-Replace-Warning and Kill procedures to and from MME/HeNBs.

**Command Changes**

**public-warning-system**

Configuration of PWS feature under HeNBGW network service.

```bash
configure

context context_name

henbgw-network-service henbgw_network_service

[ no ] public-warning-system variable

[ default ] pws warning-request-timeout | kill-request-timeout

end
```
Performance Indicator Changes

<name> Schema

<Brief description then list new/modified/deprecated stats>

•

show henbgw-network-service all

This command introduces the following new performance indicators:

• Public-Warning-System
• PWS-warning-request-timeout
• PWS-kill-request-timeout

CSCum10435 - KT SCTP/S1AP stats enhancement request

Feature Changes

KT SCTP/S1AP stats enhancement request

Support for Tx/Rx SCTP cause statistics available. S1AP cause Statistics support based on TAI also available on access service.

Previous Behavior: SCTP Cause statistics was not available.

New Behavior: SCTP Tx/Rx cause stats available for both henbgw access and network service level. Support for S1AP cause stats filtering based on TAI entries.

Customer Impact: Provides detailed statistics of SCTP Causes and S1AP causes at TAI level for analysis.

CSCum10546 - QoS enhancements

Feature Changes

QoS enhancements

Logging enhancements for diagnosing faults under henbgw access and network service.

Logging enhancements during fault conditions such a SCTP aborts, Error handling, Handover Prep failures added for henbgw access and network service.

Customer Impact: Diagnosing fault conditions through Logs for various failures.
CSCum91014 - Need to increase mme-pool size from 8 to 32

Feature Changes

mme-pool size increased from 8 to 32

Increase in number of MMEs per pool from 8 to 32 MMEs.

**Previous Behavior:** Only 8 MMEs allowed per MME pool.

**New Behavior:** 32 MMEs are allowed per MME pool, thus allowing maximum of 256 S1MME associations for Network service.

**Customer Impact:** 32 MMEs support per MME pool allowing more S1MME associations.
Chapter 9
HSGW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from HSGW in StarOS 17 software releases.

Important: Correction: RoHC is not supported on the HSGW and was erroneously included in the past HSGW Administration Guide.
HSGW Enhancements for 17.1

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
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**CSCuc87249 - HSGW and PGW support RFC6275 (Checksum standard of S2a)**

**Feature Changes**

**HSGW and P-GW Support RFC6275**

There is a checksum field in the mobility header. The checksum is calculated from the octet string. This includes a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one's complement of the one's complement sum of this octet string. In RFC 3775, the next header value used in the pseudo header is 2. In RFC 6275, the next header value used in the "pseudo header" was changed to 135.

**Previous Behavior**: For incoming messages, both RFC 3775 and RFC 6275 based checksums are acceptable. For outgoing messages only RFC 3775 can be used to calculate the checksum.

**New Behavior**: For incoming messages, both RFC 3775 and RFC 6275 based checksums are acceptable. For outgoing messages, it is now possible to choose between RFC 3775 and RFC 6275 for calculating the checksum using a CLI based switch.
Command Changes

mobility-header-checksum

The following new keywords have been added: rfc3775 and rfc6275.

configure

context context_name

mag-service mag-service_name

mobility-header-checksum { rfc3775 | rfc6275 }

default mobility-option-type-value

end

Notes:

- **default**: Sets the command to the default value of rfc3775.
- **rfc3775**: Configures the ‘next header’ value to 2 as defined in RFC3775.
- **rfc6275**: Configures the ‘next header’ value to 135 as defined in RFC6275.
- Refer to the *Context Configuration Mode Commands I-M* chapter of the Command Line Interface Reference for more information about this command.
HSGW Enhancements for 17.0

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
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

CSCuo90236 - P-PGW Formulation of P-CSCF Output as part of show sub full all

**Feature Changes**

**Formulation of P-CSCF Address Output as part of show sub full all**

Simplified the P-CSCF Address Output as part of show sub full all output. The P-CSCF discovery mode specific information is SR/GR recovered.

**Previous Behavior:** Previously, the P-CSCF Address Output displayed the P-CSCF Address information separately for S6b based FQDN and for Radius or configured scenarios. It also restricted the S6b mode to only display the IPv6 Address Information. IPv4 information was not being displayed. Also, the earlier output did not support persistence across ICSR/Session Recovery for all the discovery modes. The previous behavior also maintained persistence across SR/ICSR. However, previously P-CSCF information was not persistent across inter technology handoffs (like LTE -> eHRPD, s2bGTP-> eHRPD, eHRPD-> LTE, eHRPD -> s2GTP, etc).
New Behavior:  In the new Output, a “Discovery Mode” field specifies the method of discovery followed by the actual P-CSCF Address Information. Also, the new Output displays both IPv4 and IPv6 address information as per applicability. The new Output remains persistent across ICSR/Session Recovery for all P-CSCF discovery modes. Additionally, the new behavior maintains the P-CSCF information persistency across inter technology handoffs (like LTE -> eHRPD, s2bGTP -> eHRPD, eHRPD -> LTE, eHRPD -> s2bGTP, etc.)

CSCuq06604 - PGW does not initiate dns query to resolve p-cscf addr after epdg-ehrpd ho

Feature Changes

P-GW Did Not Initiate DNS Query to Resolve P-CSCF Address after ePDG-eHRPD Handoff

Previously, P-CSCF address resolution during ePDG to eHRPD Handoff was not supported.

Added support to resolve P-CSCF Address during s2b to eHRPD Handoff if it is not resolved earlier as part of the ePDG call setup.

Important:  P-CSCF address resolution during Handoff only occurs if it was not resolved in the initial call setup.
This chapter identifies features and functionality added to, modified for, or deprecated from IPSG in StarOS 17 software releases.
IPSG Enhancements for 17.0

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 *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 IPSG.

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

---

**CSCum62821 - IPSG should respond for Acct-Stop with non-existing session**

**Feature Changes**

**IPSG Reply To Accounting-Request Stop For Failed Cases**

In earlier releases, the IPSG service responds to a Radius Accounting-Stop message only if the session exists. Otherwise, the packet is dropped.

With this release, the IPSG service can be configured using a CLI command under the IPSG Radius Server Configuration Mode to respond to Radius Accounting-Stop messages even if a session does not exist. This feature is disabled by default.

**Previous Behavior:** IPSG does not respond to Accounting-Stop messages when the session does not exist.

**New Behavior:** Radius Acct_rsp is sent for an acct_stop message of a non-existing session.
Customer Impact: When this feature is enabled, acct_rsp is sent for a non-existing session. This is helpful when an IPSG service is reset and loses all active sessions. The GGSN that is unaware of this sends a radius acct_stop to disconnect the call, for which the IPSG service sends a response. This is one use case.

Command Changes

respond-to-non-existing-session

In support of this feature, the respond-to-non-existing-session CLI command has been introduced to enable/disable IPSG from sending a response to a Radius accounting-stop message when the session does not exist.

configure

context context_name

ipsg-service service_name mode radius-server

[ default | no ] respond-to-non-existing-session

end

Notes:
- By default, this feature is disabled.

Performance Indicator Changes

IPSG Schema

The following bulkstats item is introduced in support of this feature:
- total_stop_non-existing_rsp_sent

show ipsg statistics

The following output field is introduced in support of this feature:
- Total Non-Existing STOP Rsp sent

CSCup07760 - SMOKETEST : IPv6 Ping timeout, uplink data packets are lost

Feature Changes

IPSG IPv6 Traffic

Previous Behavior: Enabling the ingress-mode configuration under the Ethernet Port Configuration Mode was not mandatory for IPSG to handle IPv6 traffic.

New Behavior: All IPv6 traffic requires the ingress-mode configuration to be enabled at the ingress context of IPSG.
**Customer Impact:** IPv6 traffic originating from the UE towards IPSG might be dropped if the `ingress-mode` configuration is not enabled at the ingress context of IPSG.
Chapter 11
L-ESS Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from L-ESS StarOS 17 software releases.
L-ESS Enhancements for 17.0

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 *L-ESS Administration Guide* for this release.

CSCum67352 - LESS should support pushing and pulling of files from servers over IPv6

**Feature Changes**

**IPv6 support in L-ESS**

L-ESS is used for pulling and pushing files from one or more remote/local server to one or more remote/destination servers.

**Previous Behavior:** L-ESS supports file transfer over IPv4.

**New Behavior:** With Release 17.0, L-ESS will also support file transfer over IPv6.

This feature change also includes the following:

- SNMP receiver will be IPv4 or IPv6 addressable.
- RedHat OS NTP package/utility will support IPv6.
- Veritas HA software works over IPv6.
Chapter 12
MME Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from the MME in StarOS 17 software releases.

Corrections have been made to the following items:

- In the 17.4 content, please look for changes identified for:
  - CSCuu51391
- In the 17.1 content, please look for changes identified for:
  - CSCum37443
  - CSCul07972
  - CSCup41525
MME Enhancements for 17.7

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

---

**CSCuv27053 - Purge-request towards only one HSS after sessmgr crash**

**Feature Changes**

**Purge Request Behavior**

**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.
CSCux33388, CSCur41900 - CLI Control for 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

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 TAUs 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-SSGN 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-SSGN will ignore the “target-access-restriction enabled” configuration and the source-SSGN 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.

```plaintext
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 ...
MME Enhancements for 17.5

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

CSCui60043 - Changing MME dictionary for LUR - feature list

Feature Changes

S6a Diameter Messages Sent without M-bit

Previous Behavior: The M-bit was included for Supported-Features AVP for standard and standard-r9 S6a dictionary.

New Behavior: The M-bit is removed for Supported-Features AVP for standard and standard-r9 S6a dictionary. So, now the MME sends out S6a Diameter Messages toward the HSS without Setting the M-bit for Supported-Features AVP.
CSCuu45609 - MME Misbehaves while S1-HO-SGW-REloc fails due to no response for MBreq.

Feature Changes

Reducing Signaling

**Previous Behavior:** Deactivate Bearer Request is sent to the UE after Detach Request is sent when Modify Bearer Request timed out in S1-HO with SGW relocation.

**New Behavior:** Because Deactivate Bearer Request is not required, it is not sent to the UE after Detach Request is sent to the UE when Modify Bearer Request timed out in S1-HO with SGW relocation. This results in reduced signaling.

CSCuv16974 - Cell Traffic Trace files to include eNodeBId eNodeBUeS1ApId

Feature Changes

Trace Extension for C Type Files

**Previous Behavior:** Earlier, the C Type file format only included IMSI and IMEI (SV) fields.

**New Behavior:** From this release onwards, the C Type file format is modified to include three additional fields—eNodeB ID, eNodeB UE S1 AP ID and MME UE S1 AP ID. The existing command `trace-extension` is modified to include these additional fields.

**Customer Impact:** The new CLI configuration allows the operator to view additional Cell Traffic Trace information from the additional fields—eNodeB ID, eNodeB UE S1 AP ID and MME UE S1 AP ID in the C Type files.

Command Changes

```
trace-extension
```

New keywords make it possible to trace additional fields:

```
configure

   template-session-trace network-element enb template-name cell-trace

   [ no ] trace-extension enb-id ue-slap-id

end
```

**Notes:**

- The `trace-extension` command defines the UE or eNodeB identity extension parameters for the C Type files.
- The `enb-id` keyword is an additional field in the C Type file that identifies the global eNodeB entry.
- The `ue-slap-id` keyword is an additional field in the C Type file that identifies the eNodeB UE S1AP identity and the MME UE S1AP identity.
Performance Indicator Changes

show session trace template network-element

The `show session trace template network-element` command allows the operator to verify the Cell Traffic Trace configuration. On executing the above show command, the following new field is displayed:

```
Cell Trace file Extension entries:   GLOBAL-ENB   ENB-UE-S1AP-ID   MME-UE-S1AP-ID
```

CSCuv68974 - EMM CC under CCP for SGS is incorrectly displaying as msi-unknown-in-hlr

Feature Changes

**imsi-unknown-in-hss**

MME CLI has been displaying an incorrect cause code mapping option.

**Previous Behavior:** The CLI keyword to configure the SGs cause code mapping for cause ‘IMSI unknown in HSS’ is `imsi-unknown-in-hlr`.

**New Behavior:** The CLI keyword to configure the SGs cause code mapping for cause ‘IMSI unknown in HSS’ is `imsi-unknown-in-hss`. The `imsi-unknown-in-hlr` keyword option has been deprecated from all instances in the StarOS command line interface. To maintain backward compatibility, all configurations using the deprecated keyword will load and a warning will be displayed to the user that the `imsi-unknown-in-hlr` keyword has been deprecated and the configuration has been internally reconfigured with `imsi-unknown-in-hss`.

**Customer Impact:** More intuitive user experience.

Command Changes

**sgs-cause-code-mapping**

To enable the customer to more easily configure SGs to EMM cause code mapping for ‘IMSI unknown in HSS’, one keyword is deprecated - `imsi-unknown-in-hlr` - and replaced with a new keyword `imsi-unknown-in-hss`.

```
configure

call-control-profile profile_name

   sgs-cause-code-mapping imsi-unknown-in-hss emm-cause-code imsi-unknown-in-hss

end
```

**Notes:**

- If a configuration using the old keyword is loaded, a warning message will be displayed: `Warning: imsi-unknown-in-hlr CLI keyword has been deprecated, imsi-unknown-in-hss is used instead`. The operator is not required to perform any action when the message is displayed.
Performance Indicator Changes

show configuration

The replacement keyword `imsi-unknown-in-hss` is visible in all situations where the deprecated keyword `imsi-unknown-in-hlr` was previously visible. For example:

```
show configuration
.
.
.
call-control-profile <profile_name>
  qos ue-ambr max-ul 120000 max-dl 130000
  qos ue-ambr prefer-as-cap both-hss-and-local minimum
  sgs-cause-code-mapping imsi-unknown-in-hss emm-cause-code imsi-unknown-in-hss
.
.
```

CSCu73207 - MME not compliance with 3GPP 24.301 CR 2098

Feature Changes

Cause Code in Attach Reject when EPS Subscription Not Present

**Previous Behavior:** 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.

**New Behavior:** 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.

**Customer Impact:** Reduced signaling between UE and MME because the UE does not retry the Attach.

Performance Indicator Changes

MME Schema

A new counter helps the operator to track Attach Rejects due to the subscriber not having an EPS subscription:

- `emmdisc-noepssubscription`
  - **Description:** Total number of 4G Attaches rejected because the subscriber did not have an EPS subscription.
  - **Triggers:** Counter increments when a subscriber without a subscription for 4G packet-oriented services tries to Attach to the MME.
• **Availability:** per MME service
• **Type:** Counter
• **Data Type:** Int32

**CSCuv87445 - During IRAT 3G to 4G iphone doesnt include APN, MME not req. apn from HS**

**Feature Changes**

**Handling PDN Connectivity Request with Missing APN**

The following behavior change was done to deal with PDN connectivity rejection, with cause missing or unknown APN, that occurs as a result of the Request not including the APN IE.

- **Previous Behavior:** When the UE does not include the APN IE in the PDN Connectivity Request then the MME rejects the request with cause missing or unknown APN.
- **New Behavior:** When UE does not include the APN IE in the PDN Connectivity Request then the MME processes the request with a default APN from the UE's subscription.
- **Customer Impact:** When the APN IE is not included in the PDN Connectivity Request from the UE, the MME will validate the PDN-Reconnect policy rather than blindly rejecting the PDN Connectivity Request.

**CSCuv88869 - MME to drop repeated IDRs from HSS**

**Feature Changes**

**Duplicate ISDR Rejection**

- **Previous Behavior:** Earlier, for every duplicate ISDR request, MME sends an ISDA message with the result code UNABLE_TO_COMPLY.
- **New Behavior:** From this release onwards, MME has been modified to drop ISDA messages for the incoming duplicate ISDR requests.

**CSCuw03805, CSCuw56073 - Increase the hss-peer-service limit in MME to 64**

**Feature Changes**

**More HSS Peer Services**

- **Previous Behavior:** The maximum number of HSS Peer Services that could be created and configured was 16 per MME chassis.
- **New Behavior:** The maximum number of HSS Peer Services that can be created and configured is now 64 HSS Peer Services per MME chassis. The HSS Peer Services are created with the `hss-peer-service` command in the Context configuration mode.
Important: In some cases, two diameter endpoints (S6a and S13) can be configured for a single HSS Peer Service. To ensure peak system performance, we recommend that the total of all Diameter endpoints should be taken into consideration and limited to 64 endpoints.

CSCuw21831 - MME Co location with SGSN in Pool Not Achieved

Feature Changes

Two Served GUMMEI Lists

Previous Behavior: The MME sends a single list of Served GUMMEI which contains all PLMN-ID(s), GROUP-ID(s) and MME-CODE(s) configured under both mme-service including the shared PLMN and inter-rat-nnsf configuration.

New Behavior: Per 3GPP TS 36.413 for S1 Setup, the MME can send two lists of Served GUMMEI. The MME’s first list for the LTE network contains information for all PLMN-ID(s), GROUP-ID(s) and MME-CODE(s) configured as part of the MME Service configuration, including the shared PLMN. The MME’s second list, for non-LTE RAT, contains a list of all PLMN-ID(s), GROUP-ID(s) and MME-CODE(s) configured for inter-RAT handovers when the MME is co-located with an SGSN (inter-rat-nnsf configuration) as part of the MME Service configuration.

Another facet of the MME’s new behavior, the operator can configure a range of MME-CODES for a particular PLMN-ID - Group-ID combination. This MME-CODES range makes it easier for the operator to configure and also allows the operator to configure more than 16 MME-CODES under a particular PLMN-ID - Group-ID combination.

Command Changes

inter-rat-nnsf

A new keyword, mme-code-range, has been added to the inter-rat-nnsf command to enable the operator to more easily define a range of served MME codes for a specific PLMN-ID - MME Group ID combination for non-LTE RAT service GUMMEI. The identified MME codes under the non-LTE served GUMMEI in S1 SETUP response facilitate MME selection for inter-RAT handovers when the MME is co-located with an SGSN.

configure

context context_name

mme-service mme_service_name

[ no ] inter-rat-nnsf collocated-mme plmn-id mcc mcc_value mnc mnc_value group-id mme_group_id { mme-codes mme_codes | mme-code-range first_mme_code to last_mme_code }

end

Notes:

- For all pre-existing keywords and variables, please refer to your Command Line Interface Reference for keyword descriptions and variable information.

- mme-codes mme_codes - Enter up to 16 MME codes, for a particular PLMN-ID and Group-ID combination. mme_codes must be ascending integers from 0 through 255 with a single blank space between each code; for example: 2 3 4.
**mme-code-range first_mme_code to last_mme_code** - Identify an unlimited number of MME codes, for a particular PLMN-ID and Group-ID combination, as a range of MME codes. *first_mme_code* must be the first MME code in the range and it must be an integer from 0 through 255. *last_mme_code* must be the last MME code in the range and it must be an integer from 0 through 255 and must be an integer greater than the value for *first_mme_code*.

**CSCuw33845 - Deletion of Notify Messages in PGW-initiated Bearer Deactivation**

**Feature Changes**

**MME Initiated Notifications to HSS – Removed**

**Previous Behavior:** When a UE moves from a LTE network to a WLAN network, MME receives a delete bearer request from PGW. MME initiates a notification request to HSS to delete the bearer information. Due to deletion of the bearer information from the HSS, the UE will not be able to connect to the same PGW when it switches back to LTE from a WLAN network.

**New Behavior:** The MME is modified to not initiate notification requests to HSS, when a delete bearer request is received from the PGW, during UE network switch. With this modified behavior, the UE can switch between LTE and WLAN networks being connected to the same PGW.

**Customer Impact:** Because delete notification requests are not initiated form the MME, message exchanges are significantly reduced in the network.
MME Enhancements for 17.4

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.

---

**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

---

**CSCur41900 - TAU Reject with EMS Cause #15 mapping instead of #19**

**Feature Changes**

**Target Access Restricted for the Subscriber Cause Code**

This enhancement is a 3GPP TS (29.274 and 29.060) release compliance enhancement. As per 3GPP TS 29.274 and TS 29.060, the source-serving node (MME/SGSN) is allowed to reject SGSN Context Request (GTPv1) and Context Request (GTPv2) mobility management messages with “Target Access Restricted for the subscriber” cause if target access is restricted for the subscriber based on the Access-Restriction-Data in the subscription profile. The target node (MME/SGSN) is allowed to reject RAU/TAU with anyone one of the following NAS Causes:

- #15 "No suitable cells in tracking area", or
- #13 "Roaming not allowed in this tracking area", or
- #12 "Tracking area not allowed"
New statistics have been introduced under "show egtpc statistics verbose" and "show sgtpc statistics verbose" to reflect the context response sent and received with the new reject cause "Target Access Restricted for the subscriber".

For more information refer to the 3GPP TS 29.274 (section 7.3.6), TS 29.060 (section 7.5.4), TS 29.060 Annex B (Table B.5: Mapping from Gn/Gp to NAS Cause values – Rejection indication from SGSN) and TS 29.274 Annex C (Table C.5: Mapping from S3/S16 to NAS Cause values – Rejection indication from MME/S4-SGSN)

**Previous Behavior:** In earlier releases:
- The target node (SGSN/MME) does not send the target RAT type in SGSN Context request to the source node.
- The target node (SGSN/MME) rejects RAU/TAU with cause “No suitable cells in Location/Tracking Area” only after ULA/ULR is received with target RAT restricted for the subscriber in Access-Restriction-Data.

**New Behavior:** From this release onwards:
- The target node (SGSN/MME) sends the target RAT Type in SGSN Context request to source node.
- The source node (SGSN/MME) rejects the SGSN Context Request/Context Request with the cause “Target Access Restricted for the subscriber” if target RAT is restricted for the subscriber as per Access-Restriction-Data received in ULA/ULR using RAT Type received in SGSN Context request/Context request.
- The target node (SGSN/MME) sends RAU/TAU reject after Context Response/SGSN Context Response received with EGTP/GTP cause “Target Access Restricted for the subscriber”.

**Customer Impact:** Rejecting RAU/TAU much early in call cycle results in reduced signaling.

### Performance Indicator Changes

#### `show sgtpc statistics verbose`

New statistic is added to this show command to display Target Access Restricted statistics for GTPv1 mobility management messages.
- Target Access Restricted

#### `show egtpc statistics verbose`

New statistic is added to this show command to display Target Access Restricted statistics for GTPv2 mobility management messages.
- Target Access Restricted

### CSCus24510 - MME support for EMERGENCY_CALL_RELEASE event in lcs service

### Feature Changes

**MME Notifies GMLC of Emergency Call Release**

*Important:* This functionality was initially available in 17.3 as Lab Quality but in Release 17.3.2 it was made available as fully qualified Deploy Quality.
The call release event enables the GMLC to clear the cache for existing calls and to correctly log the duration of an emergency call. Without call release facilitating the clearing of the cache, the location platform could send the old (erroneous) location information in response to a new location request for an E-911 call.

**Previous Behavior:** The GMLC was not notified when the MME performed an Emergency Call Release as part of a location service procedure.

**New Behavior:** In compliance with 3GPP TS 29.172, the MME LoCation Services (LCS) feature supports sending the EMERGENCY_CALL_RELEASE event in a subscriber location report (SLR) request message, to the GMLC to notify the GMLC of the call release, when an emergency call is released or when an emergency PDN is disconnected at the MME.

Note, this is not configurable functionality.

**Customer Impact:** Notifying the GMLC of the emergency call release event allows the GMLC to delete all information previously stored for the emergency call in accordance with regulations.

---

**CSCus32369, CSCuv66398 - wrong type of list TAI list IE sent in ATTACH/TAU Accept**

**Feature Changes**

**TAI List IE Value Encoding**

**Previous Behavior:** Tracking Area Identity (TAI) list IE, sent in ATTACH/TAU Accept from MME are incorrectly encoded. As per 3GPP TS 24.301 (clause 9.9.3.33), three different values are possible for encoding the TAI list:

- "000", list of TACs belonging to one PLMN, with non-consecutive TAC values
- "001", list of TACs belonging to one PLMN, with consecutive TAC values
- "010", list of TAIs belonging to different PLMNs

The MME sends incorrectly encoded Tracking Area Identity (TAI) list IE in ATTACH/TAU Accept messages. Irrespective of the TAC (Tracking Area Code) values and the PLMN configuration, the type of list value used is "010". Based on the 3GPP TS 24.301 options listed above, this encoding is incorrect when consecutive or non-consecutive TAC values, belonging to the same PLMN, are configured.

**New Behavior:** The MME now encodes the TAI list IE value per the 3GPP TS 24.301 so that the MME automatically encodes "000", "001", or "010" depending upon the TAC values and PLMN configuration.

This change is applicable for releases 17.4 and forward. A new CLI (PR CSCuv66398) ensures backward compatibility with previous releases, as it disables this behavior change (PRCSCus32369). This new CLI command, `legacy-tai-list-encoding`, is introduced under the MME Service configuration mode to configure the encoding for the TAI list value as "010" for list of TAIs belonging to different PLMNs.

---

**Command Changes**

`legacy-tai-list-encoding`

This new command is added to enable the MME to override the new default behavior and to specify the "010" encoding value for the TAI (Tracking Area Identity) list IE. If this command is not used for the configuration, then the MME uses the default function to encode the TAI list value for the IE based on the list of TACs belonging to one PLMN, with consecutive or non-consecutive TAC values configured in the TAI entries.
configure

context context_name

mme-service service_name

[no] legacy-tai-list-encoding

end

Notes:
- By default, the TAI list value is encoded based on PLMN and TAC values of TAI entries.
- The operator can use this command to configure the encoding of TAI list values to "010" irrespective of PLMN and TAI values.

CSCus57109 - MME Not Incrementing any Paging Stats for DDN Without EBI

Feature Changes

Enabling Paging Statistics using Active Bearers

Previous Behavior: The Paging Statistics for paging requests were not accounted when the DDN from the SGW is received without an EPS Bearer ID (EBI). The QCI values acquired using the EBI is primarily required for accounting paging statistics. Since, the EBI field was made available only from release 10 onwards, the DDN was received from SGW without the EBI and therefore, the Paging Statistics could not be accounted.

New Behavior: In case the DDN from SGW is received without EBI, the configuration is modified such that the QCI values are taken from all available active bearers of the UE. The QCI values from these active bearers will be used to account for Paging Statistics.

CSCus68029 - Configurable wait time value for ISDA reqd for state/location retrieval

Feature Changes

Configurable ISDA Guard Timer

Previous Behavior: The Insert Subscription Data Answer (ISDA) timer was hardcoded to a value of 25 seconds.

New Behavior: With this release, the operator can configure the ISDA guard timer to any value from 1 to 100 seconds. Upon expiry of this wait timer, the MME sends the ISDA with the last-known location of the UE if the MME receives the Insert Subscriber Data Response (ISDR) with both the location flags set (current and last-known locations). Only when the ISDR is received with both flags set is the ISDA guard timer started. In situations where the MME receives the ISDR with only the last-known location flag set, then the MME immediately sends the ISDA with location information - no delay and this timer is not started even if configured.

Customer Impact: This timer is separate from the paging timer and configuration of the ISDA guard timer can reduce the overall delay before sending the ISDA.
Command Changes

**isda-guard-timeout**

This new command in the MME Service configuration mode enables the operator to set the number of seconds the MME waits for current location information for the UE. If the current location is not learned before expiry, because there is no paging response or location reporting control from the eNB, then the MME sends the ISDA with the last-known location upon expiry of this timer.

```
configure
  context context_name
    mme-service service_name
      [ no ] isda-guard-timeout seconds
    end
```

Notes:

- **no** at the beginning of a command disables any configuration for this timer and resets the wait time to the default of 25 seconds.
- Only when the ISDR is received with both location flags (current and last-known locations) set is the ISDA guard timer started. Upon expiry of this wait timer, the MME sends the ISDA with the last-known location of the UE.
- In situations where the MME receives the ISDR with only the last-known location flag set, then the MME immediately sends the ISDA with location information - no delay and this timer is not started even if configured.
- When the ISDA guard timer expires, the paging procedure does not stop until the page timer expires but the MME ignores the paging timer and sends the ISDA with the last-known location if the ISDR was received with both location flags set and the UE is in EMM-idle mode.
- While the MME is serving the ISDR (where both location flags are set) from the HSS, if the HSS tries to send another similar request then the MME responds to the HSS with DIAMETER_UNABLE_TO_COMPLY.

Performance Indicator Changes

**show mme-service all**

A new field has been added to the output generated by this command to show the configuration for the ISDA guard timer. The following is an example of the display if the timer were configured for 2 seconds:

- **Isda guard timeout** : 2s
CSCuu29470 - Counter esm-msgtx-pdncon-rej not equal to the sum of all esm-ms

Performance Indicator Changes

MME Schema

Two new stats have been added under the category of PDN connectivity reject causes.

- Variable name: %esm-msgtx-pdncon-rej-mul-pdn-not-allowed-for-apn%
  - Description: Total number of ESM messages sent by the MME indicating that the PDN connection has been rejected because the APN does not allow multiple PDN connections.
  - Triggers: This type of message is sent when the MME rejects a received PDN Connection Request for an APN which already has an existing PDN of the same PDN-type.
  - Availability: per MME service
  - Stat Type: Counter, Proprietary
  - Data Type: Int32

- Variable name: % esm-msgtx-pdncon-rej-other-reasons %
  - Description: Total number of ESM messages sent by the MME indicating that the PDN connection has been rejected for a cause other than one of those listed in the output generated by the ‘show mme-service statistics esm-only’ command.
  - Triggers: This type of message is sent when a PDN connection is rejected due to causes other than those mentioned under the already existing PDN Connectivity Reject section of the output generated by the ‘show mme-service statistics esm-only’ command.
  - Availability: per MME service
  - Stat Type: Counter, Proprietary
  - Data Type: Int32

show mme-service statistics esm-only

These two new counters correlate to the two bulk stats mentioned in the section above.

Two new counter fields have been added to the generated output to ensure that the sum of all the causes listed under PDN Connectivity Reject should be equal to the PDN Connectivity Reject Total. The two new fields are:

- Multiple PDN conn not allowed:
- Other Reasons:

The following is a sample of the possible output:

```
[local]asr5000# show mme-service statistics esm-only
...
Total ESM Control Messages:
...
```
CSCuu48619 - MME Rejects UBR During a Handover Collision between S10-HO and X2-HO

Feature Changes

Enable TAU to Continue on Receiving X2 HO

Scenario:

- After SRNS handover from 3G, the MME rejects a received Update Bearer Request with the following failure cause: EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS.
- Then the QoS from the HSS is not applied to the subscriber.
- After the SRNS handover from 3G is performed, when the UE does a TAU, the MME waits to receive a TAU Complete message from the UE. But the MME only receives an X2/S1 HO.

Previous Behavior: If the MME received X2 HO /S1 HO while TAU Accept was being retried, then after completion of inbound MME relocation the TAU Accept retries were aborted and not retried after X2 HO/ S1 HO. Also, if X2/S1 HO occurred before TAU Complete was received then the HSS-provided subscribed QoS is not applied.

New Behavior: If the MME receives X2 HO /S1 HO while TAU Accept is being retried, then after completion of inbound MME relocation the TAU Accept retries will proceed after completion of S1 HO / X2 HO provided the HO happens from the same TAI as the TAU. Also, if X2/S1 HO occurred before TAU Complete was received then the HSS-provided subscribed QoS are applied.

CSCuu51391 - Scaling support for Cell Tracing

Feature Changes

Cell Traffic Trace
The Cell Traffic Trace feature provides a 3GPP standard-based cell trace function for tracing all calls in a single cell or multiple cells. Cell Tracing provides the capability to log on to data on any interface at a call level for a specific user or mobile type or a service initiated by a user. In addition, Cell Tracing provides instantaneous values for a specific event.

When Cell Traffic Trace is activated in the monitored cell(s) of E-UTRAN, the eNodeB starts a Trace Recording Session for new calls/session and also for existing active calls/session. A Trace Recording Session Reference (TRSR) is allocated by eNodeB for each of the monitored call/session. The TRSR includes the TRSR reference along with the Trace Reference and Trace Collection Entity (TCE) address in the CELL TRAFFIC TRACE message to the MME over S1 connection.

Cell Traffic Trace Procedures are used at the MME to assist the TCE Server in correlating the Trace Reference (generated by EM) and Trace Recording Session Reference (generated by the eNodeB) with the IMSI, IMEI (SV) corresponding to the traced session as the eNodeBs only have access to temporary UE identities and not permanent identities (IMSI, IMEI (SV)).

Trace Files management - Creation of Trace files, renaming and moving trace files to respective directories, compression and archiving of trace files. The configuration for this process is discussed in the Configuring Cell Traffic Trace section.

The Cell Traffic Trace feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Previous Behavior:** Compression of archived trace files was not provided in the earlier Cell Trace configuration.

**New Behavior:** From this release onwards, the Cell Traffic Trace configuration is modified to support compression of the archived trace files. The present configuration also supports compression of C Type files based on the configurable parameters.

### Command Changes

**session trace network-element**

**Local Storage**

`enb` is a new keyword that is configured as part of the Cell Traffic Trace feature. The Cell Traffic Trace feature is configured in the Global Configuration mode.

A global template configuration for Cell Traffic Trace with network element as eNodeB, allows the operator to decide the total disk size for storing C-type files and also the archive directory parameters (disk limit, number of files, size and timer) before the C-type files are compressed.

To store the trace files locally, use the following configuration:

```
configure

    session trace network-element enb tce-mode none collection-timer timer_value

[ no ] session trace network-element enb

end
```
MME Changes in Release 17

MME Enhancements for 17.4

Notes:
All parameters are new to the Cell Traffic Trace feature. For information on these parameters refer to the session trace command in the Command Line Interface Reference.

TCE Storage
To store the trace file on a TCE server, use the following configuration:

```_configure
   session trace network-element enb tce-mode push transport sftp path server_path_name
   username user_name [ encrypted ] password user_password collection-timer timer_value

   [ no ] session trace network-element enb
   end
```

Notes:
All parameters are new to the Cell Traffic Trace feature. For information on these parameters refer to the session trace command in the Command Line Interface Reference.

template-session-trace

Archiving and Compressing Trace Files
This command creates a template with parameters that configure archiving and/or compression for the files generated by Cell Traffic Trace. Defining this template and archiving and/or compression of files is optional when setting up Cell Traffic Trace. The enb keyword is added to the template-session-trace command

```configure
   template-session-trace network-element enb template-name cell-trace

   [ no ] disk-limit disk_size

   [ no ] archive files number_of_files size size timer timer_value
   exit
```

Notes:
- cell-trace indicates the template name 'cell-trace' for storage of the eNB cell trace storage parameters. Note that you cannot define a template name - there is only one template and its name is 'cell-trace'.
- disk-limit disk_size is measured in megabytes (MB). This keyword defines the total space to be reserved on the hard disk. If disk-limit alone is configured then compression is not considered. The disk-limit size ranges from 1 MB to 20480 MB. If disk-limit is not configured, a default size of 200 MB is allocated in the hard disk for storing Cell Trace files.
- archive allows you to define the archive directory and the archive parameters.
  - files number_of_files defines the maximum number of files that can be archived in the directory. When the limit is reached, the archive closes. The range is an integer from 1 through 10000.
  - size size defines the directory limit in MB. The range is an integer from 1 through 10
• timer timer_value defines the number of seconds before the pending directories are archives. The range is an integer from 1 through 3600.

Performance Indicator Changes

**show session trace template network-element**

The `show session trace template network-element enb template-name cell-trace` allows the operator to verify the Cell Traffic Trace configuration. On executing the above show command, the following new fields are displayed:

- NE Type
- Storage Parameters for Archiving Cell trace files
- Disk Storage Limit
- Files per Archive Directory
- Total size per Archive directory
- Archive directory timeout

**show session trace statistics**

This show command allows the operator to monitor or troubleshoot the Cell Traffic Trace configuration. On executing the above show command, the following new fields are displayed:

- Total number of file generated
- Number of Cell Traffic Trace files generated
- Total archive files
- Average time in seconds, for archiving one directory
- Average time in seconds, for moving one C type file
- Average files per archive directory
- Frequency of Archiving Triggers:
  - Files
  - Size
  - Time-out

**CSCuu65408 - MME Write-Replace-Warning Request encoded incorrectly**

Feature Changes

**5-byte Encoding for Concurrent Warning Message**

**Previous Behavior:** The length indicator was not included in the ConcurrentWarningMessageIndicator IE of the Warning Write Replace Request. So the Concurrent Warning message indicator was encoded in 4 bytes as:

```
00 8e 00 00
```
New Behavior: 1 byte for the length indicator is added in the ConcurrentWarningMessageIndicator IE of the Warning Write Replace Request. So the Concurrent Warning message indicator is encoded in 5 bytes (per ITU ASN.1 specification) as:

00 8e 00 01 00

CSCuu67762 - Enforce license for MTC functionality

Feature Changes

License Control for MTC Functionality

Previous Behavior: The feature specific license was not enforced to use the commands and functionality related to the optional MTC feature functionality on the MME.

New Behavior: With Release 17.4, the MTC Feature license is now enforced to use MTC functions and related commands. Please speak with your Cisco Customer Representative if you have questions about the MTC Feature license.

For information on the MTC functionality supported by the MME, refer to sections CSCuh04641, CSCum37443, and CSCum37475 in the MME Enhancements for 17.0 in this document.

CSCuu82559 - MME doesn't send Charging Characteristics in EGTP_CREATE_SESSION_REQUEST

Feature Changes

Inclusion of Charging Characteristics IE

Previous Behavior: Earlier, after a handover occurs from GN/GP, the Charging Characteristics IE was not included in the EGTP_CREATE_SESSION_REQUEST during the following scenarios:

- When a subscriber moves from a 3G to a 4G network.
- When MME sends a GTP_SGSN_CONTEXT_REQ_MSG message to SGSN, and when SGSN replies with GTP_SGSN_CONTEXT_RES_MSG.
- When MME sends a CREATE_SESSION_REQUEST without including Charging Characteristics IE.
- When a 4G call is terminated.
- When SGW generates CDR with default Charging Characteristics 0x800.

New Behavior: In this release, during GN/GP handovers, MME is modified to include SGSN Charging Characteristics IE in the Create Session Request. The Charging Characteristics is included if:

- Peer-SGSN sends the Charging Characteristics or
- MME has a local configuration to include the Charging Characteristics
**CSCuu85658 - Support serving node and handover event for emergency call in LCS**

**Feature Changes**

**Emergency Call Support for Handovers**

EMERGENCY_CALL_RELEASE support was described earlier (see CSCus24510). With this, the MME has been sending EMERGENCY_CALL_RELEASE to the GMLC whenever an emergency call is released, including for handovers.

With support for EMERGENCY_CALL_HANDOVER event, the MME’s LCS functionality is further enhanced to ensure location continuity during IMS emergency call (PS to CS) handovers.

By supporting the EMERGENCY_CALL_HANDOVER event, the MME can send the Subscriber Location Report (SLR) to the configured GMLC** when the SRVCC handover procedure completes. The report includes the UE Identity (UE's MSISDN, IMSI, IMEI), the target service node ID, and the event type as handover.

Because MSC ID (expected target serving node ID) is not known to the MME, CLI has been added (see Command Changes) to map the serving MSC ID to the serving MSC IP-address information (already part of the MME Service configuration) to derive the needed ISDN number. This configuration is required to enable sending the target serving node ID for SRVCC handover to the GMLC. This ensures that the GMLC does not receive EMERGENCY_CALL_RELEASE for a handover event and that the GMLC is aware that the subscriber has moved from the source MME for location continuity.

The MME also includes the MSC identity in the target service node IE (per TS 29.172) as part of the Provide Subscriber Location Response (PSL), if an MT-LR procedure was in progress during SRVCC handover of an emergency call.

**The MME does not bind all the call events for an emergency call to a specific GMLC peer. As a result, if multiple GMLC peers are configured, the call events for a single emergency call can be sent to any of the configured GMLC peers.

For details about configuring MME’s use and configuration of Location Services, refer to the Location Services feature chapter in the MME Administration Guide.

**Command Changes**

**msc-mapping**

This new command creates a mapping between the MSC ISDN number and the MSC’s IP-address (either IPv4 or IPv6) to ensure location continuity for SRVCC handover. This mapping is required to include the MSV ID in the target service node IE for the Emergency_Call_Handover event.

configure

    context context_name
    mme-service service_name

    msc-mapping ip-address { IPv4_address | IPv6_address } isdn isdn_number

no msc-mapping ip-address { IPv4_address | IPv6_address }

end
Notes:

- The MSC IP address, key part of the mapping definition, is used to identify a specific mapping definition.
- `isdn_number`: Enter a numeric string upto 15 digits long.
- `no msc-mapping ip-address`: Identifies a specific MSC IP address mapping definition to remove from the MME Service configuration.
- MME Service supports a maximum of 24 MSC mappings.
- Use the `show mme-service` command to view configured mapping. The following is a sample of what the MSC mapping information would look like:

  MSC IP-Address and ISDN Mapping
  192.168.61.2 : 123456789012345
  192.168.61.3 : 123456789012346

CSCuu85922 - Problem with DNS query for APN with ‘gprs’ anywhere in APN Name

Feature Changes

APN-FQDN String Construction

**Previous Behavior:** Earlier, the ".gprs" substring was replaced by ".3gppnetwork.org" present at any position of the APN Network Identifier string, which is an undesired query function.

For example:

APN NI: "alwin.gprs.cisco.brussels"

DNS query output: alwin.apn.epc.mnc045.mcc456.3gppnetwork.org

**New Behavior:** Now, MME is modified to replace the ".gprs" substring if it is present only at the last label of the APN Network Identifier. The ".gprs" is replaced by using the default APN-Operator Identifier (APN-OI) as per 3GPP TS 23.003. The APN-FQDN is obtained by inserting "apn.epc" label between the APN-NI and APN-OI and replacing ".gprs" with ".3gppnetwork.org" label.

For example:

APN NI: cisco.com.gprs

DNS query output: cisco.com.apn.epc.mnc045.mcc456.3gppnetwork.org

**Customer Impact:** DNS query might fail if the existing APN-NI contains ".gprs" as a substring in any of the first two labels.
CSCuu88343 - Emergency PDN Connectivity Request Rejected by MME

Feature Changes

Emergency PDN connectivity Requests After Emergency PDN Connection De-activation

**Previous Behavior:** For every emergency pdn-connection from the UE, the MME maintains the state of the emergency session. Once an emergency pdn-connection gets de-activated, any subsequent pdn-connectivity request towards same APN are rejected by the MME with the cause “Multiple PDN connections not allowed”.

**New Behavior:** Once the emergency pdn-connection is de-activated, the session state is accordingly updated at the MME. PDN connectivity requests that arrive after emergency pdn-connection de-activation are validated and honored by the MME.

**Customer Impact:** The UE is not affected by recurrent emergency pdn-context creation and deletion towards same APN.

CSCuv02890 - Enforce license for MTC functionality

Feature Changes

License Control for MTC Functionality

**Previous Behavior:** The feature specific license was not enforced to use the commands and functionality related to the optional MTC feature functionality on the SGSN.

**New Behavior:** With Release 17.4, the MTC Feature license is now enforced to use MTC functions and related commands. Please speak with your Cisco Customer Representative if you have questions about the MTC Feature license.

For an idea of the MTC functionality supported by the SGSN, refer to the sections covering CSCum47774, CSCum50056 in the **SGSN Enhancements for 17.1** in this document. For detailed information about the SGSN’s MTC feature support, refer to the **MTC Congestion Control** chapter of the **SGSN Administration Guide**.

CSCuv21929 - Incorrect Feature-List Bit Set for S6a - ODB-all-OG

Feature Changes

3GPP TS 29.272 Version Compliance for Operator Determined Barring

**Previous Behavior:** The Operator Determined Barring for all outgoing calls (ODB-all-OG) bit is always set in the ULR from the MME to the HSS. This behavior is not expected from MME that is compliant with 3GPP TS 29.272 version 10.5.0. The HSS does not expect the ODB-all-OG bit to be present in the ULR from the MME which is 3GPP TS 29.272 version 10.5.0 compliant, as a result excess signaling is observed on the s6A interface from the HSS.

**New Behavior:** The Operator Determined Barring of all outgoing calls (ODB-all-OG) bit will not be present in the ULR from MME. This is a 3GPP TS 29.272 version 10.5.0 compliance change.

**Customer Impact:** Excess signaling on the s6a interface from HSS is reduced.
CSCuv41626 - Issues observed while compressing archived Cell Traffic trace files

Feature Changes

Compression of Trace Files

**Previous Behavior:** Earlier, only duplicate files were renamed by adding a unique suffix to it

**New Behavior:** Now, all C Type files are renamed by adding a suffix to it. The suffix ranges from 1 to 4294967295. On reaching the maximum suffix value, the renaming of subsequent file will restart from 1.
MME Enhancements for 17.3

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.

---

**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

CSCus24510 - MME support for EMERGENCY_CALL_RELEASE event in Ics service

**Feature Changes**

**MME Notifies GMLC of Emergency Call Release**

---

**Important:** This new functionality is released as Lab Quality.

The call release event enables the GMLC to clear the cache for existing calls and to correctly log the duration of an emergency call. Without call release facilitating the clearing of the cache, the location platform could send the old (erroneous) location information in response to a new location request for an E-911 call.

**Previous Behavior:** The GMLC was not notified when the MME performed an Emergency Call Release as part of a location service procedure.
New Behavior: In compliance with 3GPP TS 29.172, the MME LoCation Services (LCS) feature supports sending the EMERGENCY_CALL_RELEASE event in a subscriber location report (SLR) request message, to the GMLC to notify the GMLC of the call release, when an emergency call is released or when an emergency PDN is disconnected at the MME.

Note, this is not configurable functionality.

Customer Impact: Notifying the GMLC of the emergency call release event allows the GMLC to delete all information previously stored for the emergency call in accordance with regulations.

CSCus34861 - MME is not using NAPTR with least preference first for MSC selection

Feature Changes

Enabling Weight-based MSC Selection

Previous Behavior: By default, the MME selection of the peer MSC for the Sv interface is ‘weight’ based.

New Behavior: By default, the MME selection of the peer MSC for the Sv interface is now ‘preference’ based. A new CLI command has been provided to enable the operator to disable the default and use ‘weight’ based load balancing.

Customer Impact: The customer will need to explicitly configure weight-based selection to disable the new preference-based selection scheme.

Command Changes

peer-msc

This new command makes it possible for the operator to enable/disable weight-based selection of a peer MSC during MSC lookup. By default, this functionality is not enabled.

configure

    call-control-profile profile_name

    peer-msc interface-type sv weight

    remove peer-msc interface-type sv weight

end

Notes:

- remove removes the previously configured peer-MSC configuration and disables weight-based selection of a peer MSC.

Performance Indicator Changes

show configuration
When the default is overridden with the new `peer-msc` command, the output of the `show configuration` command will indicate:

- `peer-msc interface-type sv weight`

**CSCuu18023 - MME standards violation - IDA without Supported-Features AVP**

**Feature Changes**

**Supported-Features AVP Always for ISDA**

**Previous Behavior:** The MME sent the Diameter AVP Supported-Features in the Insert Subscriber Data Answer (ISDA), only if the Supported-Features AVP was present and matched with the MME’s Supported-Features AVP including the Vendor-ID and Feature-List-ID.

**New Behavior:** In compliance with 3GPP TS 29.272, now the MME always sends the Supported-Features AVP in ISDA messages, even if the Supported-Feature AVP is not present in the ISDR. And, if the Feature-List value in the ISDR differs from the MME’s Feature-List, then the Feature-List value in the ISDA will be the negotiated value.

Support for the Supported-Features AVP is documented in the *AAA Interface Administration and Reference* for Release 18 with M-bit information included in the *Diameter Attribute Quick Reference* table of that manual.
MME Changes in Release 17

MME Enhancements for 17.2

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.

---

**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

---

**CSCts45571, CSCun25145, CSCun47322, CSCun70096 - MME: eMBMS Support**

**Feature Changes**

**MME Support for e-MBMS**

---

**Important**: This feature is under development and will be fully documented at time of deployment. This section is intended as an advisory. When working with this release of StarOS, you may encounter some of the related functionality and see some of the commands listed below. This functionality and these commands are not yet qualified or supported for use beyond trial testing.

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
- scpt
- 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> }
```

**CSCue56502 - SRVCC: Partial HO- providing voice services when SGSN is not responsive.**

Feature Changes

**SRVCC Failure Handling**
**Previous Behavior:** During S1-based CS-PS SRVCC handover, the MME used to send “Preparation Failure” for below mentioned types of failures:

- Peer SGSN DNS query failed
- Fwd Relocation Response timeout
- Fwd Relocation Response was received with a failure cause

**New Behavior:** Now, in the above failure scenarios, S1-based CS-PS SRVCC handover will continue for CS calls if CS handover on Sv interface succeeds. This means that the S1 SRVCC handover will continue as partially successful and the hanover command message will not carry any bearer related information.

**Customer Impact:** S1-based CS-PS SRVCC handover will continue for CS even if the PS handover fails.

**Performance Indicator Changes**

**MME Schema**

New bulk statistics tracks the total number of successful circuit-switched (only) 4G to 3G/2G CSPS SRVCC handovers - E-UTRAN to UTRAN (Iu mode) - using the Sv interface.

- `s1-ho-4gto3g-cspsv-sv-success-cs-only`

**show mme-service statistics verbose**

A new counter has been added to the output generated by this command to indicate the number of CS - PS handovers for the Sv interface that were partial successes.

- Success CS Only:

**CSCuq86490 - Include IMEI and IMSI in traceRecording element in Cell Traffic trace**

**Feature Changes**

**Including IMEISV in the XML Trace File**

**Previous Behavior:** Only IMSI was added in the XML trace file generated during a normal attach call. For emergency calls, only IMEI was added in the XML trace file.

**New Behavior:** If the MME is aware of the IMSI and IMEI(SV) values, then the MME will include both IMSI and IMEI(SV) values in the generated XML trace file.

**CSCuq88194 - New Reject cause needs to be added under Bearer Alloc Reject ESM message**

**Feature Changes**

**Counter and Stats Added to Track Reject Cause**
**Previous Behavior:** The “EPS QoS Not Accepted” reject cause was not available for use in Bearer Alloc Reject ESM control messages.

**New Behavior:** The “EPS QoS Not Accepted” reject cause code is now supported for use in the Bearer Alloc Reject ESM control message. This cause code is received when UE-initiated dedicated bearer request is rejected by the MME as a result of the MME’s configuration settings in the APN Profile - ‘reject’ option set with the `dedicated-bearers { gbr | non-gbr }` command.

Corresponding counter and bulk statistic variable have been added to track the use of this cause code.

**Customer Impact:** Support for this cause code will assist customers to debug the reject cause for bearer allocation failures.

**Performance Indicator Changes**

**MME Schema**

Use of the “EPS QoS Not Accepted” reject cause code for bearer allocation failures, is tracked as a bulk statistic in the MME schema:

- `esm-msgtx-brralloc-rej-eps-qos-not-accepted`

**show mme-service statistics**

Use of the “EPS QoS Not Accepted” reject cause code for bearer allocation failures, is tracked with the following new output counter generated by the `show mme-service statistics` command:

- `EPS QoS Not Accepted`

**CSCuq98725 - MME sesstrc task goes to over state when cell trace traffic is ON**

**Feature Changes**

**Increase in Memory Allocation for Sesstrc at the SMC Card**

**Previous Behavior:** Consider a scenario where cell traffic trace is enabled for multiple subscribers. The sesstrc task enters an over state when cell trace traffic is sent continuously for subscribers. The local storage for C type XML files is only 40 MB and this limit is crossed leading to file deletions. These file deletions consume extra CPU time. The Sesstrc CPU usage and memory are at 15% and 28 MB respectively.

**New Behavior:** The issue is resolved by increasing the local storage for C type XML files to 100 MB. The Sesstrc CPU usage and memory updated to 90% and 100 MB respectively to accommodate the incoming rate of Cell Trace files.

**Customer Impact:** The sesstrc resides at the SMC card, more memory has been allocated to sesstrc.

**CSCur19886 - Sessmgr crash sess/mme/mme-app/app/mme_egtp_fw.c:1014**

**Feature Changes**

**Idle-mode Entry Allowed During Outbound Handover**
Previous Behavior: If an idle-mode entry event occurs during outbound handover (4G to 3G), then idle-mode entry is not triggered.

New Behavior: Idle mode entry during outbound handover (4G to 3G) is now allowed.

CSCur50736 - PDN Connectivity Reject : Incorrect ESM cause#27

Feature Changes

Configuring ESM Cause Code #27

In general, much of the UE behavior depends on factory configuration; for example, some operator-tied phones consider APN subscriptions as RAT specific. But many operators have configured APN as RAT agnostic. This behavior changes allows some operator flexibility to handle either type of UE configuration.

Previous Behavior: By default, the MME sent cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject messages when the UE requested APN was not subscribed for that subscriber.

New Behavior: As part of the MME’s local cause code mapping, a new cause code option can be configured - "Requested-Option-Not-Subscribed" cause code value #33. When the new option is configured, then the MME sends cause code #33 (Requested Service Option Not Subscribed) in the standalone PDN Connectivity Reject message whenever the UE-requested APN is not subscribed. If the option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

Command Changes

local-cause-code-mapping

The new keyword *apn-not-subscribed* is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for *apn-not-subscribed* is explicitly configured with requested-service-option-not-subscribed in *either* the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscribed" (cause-code #33) will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

```
configure

call-control-profile profile_name

  local-cause-code-mapping { apn-not-subscribed esm-cause-code requested-service-option-not-subscribed }

remove local-cause-code-mapping apn-not-subscribed

end
```

Notes:
- *remove* - deletes the local cause code mapping from the configuration.
The new keyword `apn-not-subscribed` is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for `apn-not-subscribed` is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscriber" (cause-code #33) is sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

**configure**

```
context context_name

mme-service service_name

  local-cause-code-mapping { apn-not-subscribed esm-cause-code requested-service-option-not-subscribed }

  default local-cause-code-mapping apn-not-subscribed

end
```

**Notes:**

- **Important:** `service_name` must be unique across all contexts.

- `default` - returns the local cause code mapping to the default of #27 (Unknown or Missing APN).

**Performance Indicator Changes**

**show call-control-profile full name**

A new field has been added to the output of this command to indicate the operators Call-Control-Profile configuration for this cause code mapping:

- APN not subscribed : Requested service option not subscribed

**show configuration**

A new field has been added to the MME-Service output section of this command to indicate the operators MME-Service configuration for this cause code mapping:

- local-cause-code-mapping apn-not-subscribed esm-cause requested-service-option-not-subscribed

**show mme-service name**

A new field has been added to the output of this command to indicate the operators MME-Service configuration for this cause code mapping:

- APN not subscribed : Requested service option not subscribed
CSCur97956, CSCun97512 - paging event causing failures (PSC3 only, DPC is not)

Feature Changes

Enabling Paging Optimization

Previous Behavior: The MME’s paging cache functionality was disabled.

New Behavior: It is now possible for the operator to use CLI commands to enable and control the MME’s paging cache functionality.

Command Changes

mme paging cache

The new mme paging cache keyword ranges for this command, in the LTE Policy configuration mode, enable the operator to more easily enable or disable caching of the MME’s paging.

configure

lte-policy

mme paging cache { size cache_size | timeout time }

default mme paging cache { size | timeout }

end

Notes:

- size cache_size: Enter an integer from 0 to 10000 to specify the maximum number of tracking area code (TAC) entries to be cached. Entering the ‘0’ value disables caching and should be followed by use of the mme paging cache clear command (see CSCus14148).

- timeout time: Enter an integer from 1 to 1440 to specify the number of minutes that each TAC entry remains valid. A lower cache timeout helps to refresh the cache frequently and enables this functionality to quickly adapt to changes in the network. We recommend the timeout value be less than the expected eNodeB flap frequency; for example, if the eNodeBs connected to the MME are expected to disconnect and reconnect every 10 minutes (due to network issues), then the timeout configuration should be less than 10 minutes.

- Defaults: cache size = 5000 TAC entries per SessMgr; timeout time = 5 minutes.

- Both size and timeout must be configured to enable paging caching optimization.
CSCus00927 - S1 and SGs associations not equally distributed across mmemgr tasks

Feature Changes

Configuring the MMEDEMUX

**Previous Behavior:** MMEDEMUX had insufficient waiting time to distribute the incoming traffic to the associated MMEMGRs because all MMEMGRs were not up and running on startup of the box.

**New Behavior:** A new CLI command is introduced in the MMEDEMUX system, which allows operators to configure the percentage of MMEMGRs to be associated, and the waiting time to process the incoming traffic. The MMEDEMUX distributes the incoming traffic to the associated MMEMGRs based on the percentage value and wait time configured in this command.

**Customer Impact:** The new configuration provides the following:
- By default, MME waits for ten minutes to check if 90% of the MMEMGRs have started.
- MMEDEMUX allows users to configure the waiting time up to 3600 seconds.
- MMEDEMUX allows users to configure from 1 to 100% of the available MMEMGRs.

Command Changes

**task facility mmedemux**

The new CLI command `mmedemux` allows users to configure the waiting time of the MMEDEMUX and the percentage of MMEMGRs associated with the MMEDEMUX

```
configure

task facility mmedemux mmemgr-startup-percentage percent_value [ mmemgr-startup-wait-time wait_time ]

[ default | no ] task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time

end
```

Notes:
- `mmemgr-startup-percentage` allows users to configure the percentage of MMEMGRs to be associated with the MMEDEMUX
- `percent_value` an integer from 1 to 100
- `mmemgr-startup-wait-time` allows users to configure the waiting time of MMEDEMUX
- `wait_time` an integer value from 300 to 3600
- `[ default | no ]` disables user defined configuration and replaces the configuration with default configuration values.
Performance Indicator Changes

show configuration

If the mmedemux command is used to configure the percentage of MME Managers and wait time of the MME Demux, the following configuration is displayed on executing the command `show configuration`

- `task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time`

show session subsystem facility mmedemux all

The following new statistics are displayed on executing the command `show session subsystem facility mmedemux all`:

- MMEDemux MMEMGR Startup Status
- Max MME Managers
- Desired MME Managers
- Current MME Managers
- MMEMGRs Start in Progress
- Time Left
- All Required MMEMGRs are UP
- Time taken

Notes:
The above are status indicators
- MMEMGRs Start in Progress
- Time Left
- All Required MMEMGRs are UP
- Time taken

CSCus14148 - Dynamic Paging cache size allocation through CLI

Feature Changes

Configuring Paging Cache Functionality

Previous Behavior: The MME’s paging cache size could be configured to vary from 100 to 10000 tracking area code (TAC) entries.

New Behavior: The MME now supports an enhanced range for configuring the size of the paging cache. The configurable range has been expanded to 0 to 10000 TAC entries. Entering the ‘0’ value disables caching and should be followed by use of the `mme paging cache clear` command.

Customer Impact: Change ensures increased flexibility for operator to disable and/or control paging cache functionality
Command Changes

*mme paging cache*

The new configurable values range for the *mme paging cache* command enables the operator to more easily enable or disable caching of the MME’s paging.

```plaintext
configure
  lte-policy
  mme paging cache { size cache_size | timeout time }
  default mme paging cache { size | timeout }
end
```

Notes:
- `size cache_size`: Enter an integer from 0 to 10000 to specify the maximum number of TAC entries to be cached. Entering the ‘0’ value disables caching and should be followed by use of the *mme paging cache clear* command.

*mme paging cache clear*

The new *mme paging cache clear* command, under the Exec mode, enables the operator to clear the paging cache for either a specific SessMgr or for all SessMgs:

```plaintext
mme paging cache clear { all | instance sessmgr_instance }
```

Notes:
- `all`: Instructs the MME to clear the paging cache for all Session Managers.
- `instance sessmgr_instance`: Enter an integer from 0 to 4294967295 to specify a single Session Manager.

*show lte-policy*

A new filter, *paging cache parameters*, has been added to the *mme* keyword in this command to display the current configuration cache parameters.

*show lte-policy mme paging cache parameters*

The command generates a display similar to the following:

```
[local]MME1# show lte-policy mme paging cache parameters
MME Paging Cache Timeout: 5
MME Paging Cache Size: 5000
```
CSCus18004 - MME rounds down max bitrate in VoLTE leading to packet loss

Feature Changes

Rounding Up Some Assigned QoS Values

MME rounded down the MBR and GBR values for both Uplink and Downlink in some scenarios. This behavior has been modified to support rounding up in place of rounding down - as described below.

**Previous Behavior:** MME rounded down the assigned QoS values if the requested QoS did not align in order of 8 (<576Kbit/s) or 64 (<8640Kbit/s) and in order of 100kbp(<16000Kbit/s), (<=128000Kbit/s)1Mbps and (<256000Kbit/s) 2Mbps increments for extended values. For example, if the requested QoS value is 78Kbps the MME rounded down the QoS to 72Kbps.

**New Behavior:** MME rounds up the assigned QoS values if the requested QoS is not aligning in order of 8 (<576Kbit/s) or 64 (<8640Kbit/s) and in order of 100kbp(<16000Kbit/s), (<=128000Kbit/s)1Mbps and (<256000Kbit/s)2Mbps increments for extended values. For example, if the requested QoS value is 78Kbps the MME rounds up the QoS to 80Kbps.

During 4G to 3G (S3 to S4-SGSN) RAU, the MME does not send rounded QoS value to the SGSN. The SGSN is left to make the decision to round up or round down.

CSCus36547, CSCur89572 - 'State/Location Information Retrieval' flag support in Feature-list AVP

Feature Changes

State/Location Information Retrieval' Flag

With this release, the MME now sends the “State/Location-Information-Retrieval” flag set in the Feature-List AVP of the Update Location Request (ULR) message over the S6a interface to the HSS at the time the UE attaches. With the “State/Location-Information-Retrieval” flag set, the HSS knows to set the “EPS User State Request”, “EPS Location Information Request” and “Current Location Request” bits in the IDR-Flags AVP in IDR messages towards the MME. This subscriber data provides the UE’s current location information needed in multiple service scenarios, such as VoLTE services on the IMS side.

**MME behavior for IDR-initiated Paging:** Upon receipt of an IDR message with the “Current Location Request” bit set in the IDR-Flags AVP, the MME behavior complies with Feature-List AVP, IDR-Flags AVP, and EPS-Location-Information AVP sections as specified in 3GPP TS 29.272 v11.9.0. So when the IDR messages are received with “EPS Location Information Request” and “Current Location Request” bits set in IDR-Flags AVP, the MME sends the UE's current location information or the UE's last known location information in the “EPS-Location-Information” AVP of the IDA message.

If IDR is received with “EPS Location Information Request” and “Current Location Request” flags set in IDR-Flags AVP, the the MME's IDA response depends on whether :

- the UE is in connected mode with Location Reporting active making location information available, then the MME sends the IDA message without “Current-Location-Retrieved” AVP in “EPS-Location-Information” AVP.
- the UE is in connected mode without Location Reporting active so location information is not available, then the MME sends a Location-Reporting-Control message to the eNB to get the ECGI and the TAI.
If the MME receives a Location-Report message, then the MME sends an IDA message without “Current-Location-Retrieved” AVP and the “Age-Of-Location-Information” is set to zero in the “EPS-Location-Information” AVP sent to the HSS.

If the MME does not receive a Location-Report message, then the MME sends IDA message with last known location information with “Age-Of-Location-Information” AVP and without “Current-Location-Retrieved” AVP to the HSS.

- the UE is in idle mode, then the MME pages the UE to bring the UE to connected mode.

- If paging is successful, then the MME sends an IDA message with "Age-Of-Location-Information" and "Current-Location-Retrieved" both set to zero in the "EPS-Location-Information" AVP to the HSS.

- If paging is not successful, then the MME sends IDA messages with last known location information with "Age-Of-Location-Information" AVP and without "Current-Location-Retrieved" AVP to the HSS.

Location Reporting Control messages allow the MME to request the eNB to report where the UE is currently located.

MME’s IDR-initiated Paging Process: If the UE is in ECM-IDLE and the MME receives IDR with "EPS Location Information Request" and "Current Location Request" flags set in IDR-Flags AVP, then the MME starts a timer for 25 seconds and triggers the paging procedure. If the MME receives a response from the eNB before the timer expires, then MME sends an IDA message with the UE’s current location information in the "EPS-Location-Information" AVP. Otherwise the MME sends an IDA message with the last known location information in "EPS-Location-Information" AVP when the IDR timer expires.

Paging initiation is similar to paging for signaling events. However, a separate event shall be used in this case and be processed. If the paging procedure is already running for that UE, then when IDR is received with both flags set the MME shall not trigger paging again. MME behavior depends on the precedence configuration under paging-map:

- If the paging procedure already running for the UE has a higher precedence than for IDR, then when IDR is received with both flags set and if the other paging is not successful, then the MME does not trigger IDR paging again.

- If the paging procedure already running for the UE has a lower precedence than for IDR, and if IDR is received with both flags set, then the MME stops the ongoing paging procedure and triggers an IDR paging procedure.

If the paging procedure completes before the IDR timer expires and a paging response is not received from the eNB, then the MME sends an asynchronous IDA response immediately without waiting for IDR timeout.

Previous Behavior: Precedence assignment was limited to 1 (highest) to 7 (lowest).

New Behavior: The range of possible precedence assignments has been extended, so that the precedence set can now be any integer from 1 (highest) to 19 (lowest).

Command Changes

precedence

A new option, idr, has been added as a paging trigger option to the signaling filter of the traffic-type keyword of the precedence command precedence enables the operator to apply a priority for different paging-profiles based on traffic type. When the MME service is associated with a paging map, the system checks the profile map to determine which paging-profile to adopt for a given paging trigger, such as an IDR.

Important: If precedence is not configured, then the lowest precedence is automatically assigned.
lte-policy

    paging-map paging_map_name
    precedence precedence traffic-type signaling idr paging-profile
    paging_profile_name
    no precedence precedence
    end

Notes:

- **no precedence precedence** removes the precedence configuration associated with the specified precedence value.
- **paging_map_name** must be an alphanumeric string of up to 64 characters to identify a unique paging map associated with the LTE Policy.
- **precedence** must be an integer from 1 (highest precedence) to 19 (lowest precedence) to specify the handling precedence for this particular configuration definition.
- **idr** selects IDR as the signaling traffic sub-type that triggers paging.
- **paging_profile_name** must be an alphanumeric string of up to 64 characters to identify a unique paging profile associated with the paging map and the LTE Policy.

Performance Indicator Changes

MME Schema

The following bulk statistics have been added to the MME schema to track paging initiated in response to IDR:

- signaling-idr-paging-init-events-attempted
- signaling-idr-paging-init-events-success
- signaling-idr-paging-init-events-failures
- signaling-idr-paging-last-enb-success
- signaling-idr-paging-last-tai-success
- signaling-idr-paging-tai-list-success

**show mme-service statistics**

New counters have been added, to the output generated by this command, to display quantitative data for successes and failures of paging initiated in response to IDR:

Paging Initiation for SIGNALING IDR Events:

Attempted: 0  Success: 0

Failures: 0

Success at Last n eNB: 0  Success at Last TAI: 0
show lte-policy paging-map

The `show lte-policy paging-map name map_name` command allows you to see the precedence information configured, for example:

```plaintext
asr5000# show lte-policy paging-map name pml
```

```
== Pager Map : pml ==
Precedence 1 : Signaling-IDR ; Paging is performed as per paging-profile pp1
```

show hss-peer-service statistics

In support of the new 'State/Location Information Retrieval' flag functionality, new counters have been added to the output generated by the `show hss-peer-service statistics` command:

- Asynchronous Message Stats:
- Asynchronous ISDR Req
- Asynchronous ISDA
- Asynchronous ISDA Dropped

**CSCus36908 - MME recovered stats should be displayed with cumulative count**

**Feature Changes**

**Showing Cumulative MME Statistics**

**Previous Behavior:** When the `show mme-service statistics recovered-values` command was issued, the generated output only displayed recovered backed-up statistical values.

**New Behavior:** When the `show mme-service statistics recovered-values` command is issued, the generated output displays the cumulative statistics, which includes both current + recovered backed-up statistical values.

**Important:** This behavior change is applicable to CSCup41525 introduced in 17.1.
CSCus50162 - QOS : Incorrect Reliability Class Mapping from QCI=5

Feature Changes

Improve Reliability Class Mapping

During handovers involving Inter-RAT, some UEs experienced issues with existing behavior, which required the UEs to be powered off/on (reboot) to acquire service. Those issues should be resolved with the behavior changes identified below.

**Previous Behavior:** In situations where the SDU error ratio = 10^-6, the MME and SGSN each implemented QoS mapping of reliability class =2.

**New Behavior:** The MME and SGSN behavior has been modified such that in situations where the SDU error ratio = 10^-6, the MME and SGSN each implement QoS mapping of reliability class =3.
MME Enhancements for 17.1

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:](image) 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

**CSCup41525, CSCur94789, CSCur89174 - MME to support back up of counters and to be recovered aftr smgr rcvry**

**Feature Changes**

**Backup and Recovery of Key KPI Statistics**

**Previous Behavior:** The counter values were not recovered after a session manager crash, hence the KPI values which depend on these counter values were affected. Backing up all possible counters is not feasible as this would have an impact on memory and also on session recovery time.

**New Behavior:** This feature allows the backup of a selected set of KPI counters for recovery of the counter values after a session manager crash.

Using the new `statistics-backup` commands, in the Global configuration mode, the operator can enable the feature and define the frequency of the backup; range 1-60 minutes.
In support of this new functionality, the new mme-bk schema has been defined with statistics, derived from the MME schema, that will be backed up for recovery.

**Command Changes**

**statistics-backup**

Using the new `statistics-backup` command, in the Global configuration mode, enables this new feature with a default backup interval of every 5 minutes.

```configure
statistics-backup { mme | sgsn } 
no statistics-backup { mme | sgsn }
end
```

**statistics-backup-interval**

Using the new `statistics-backup-interval` command, in the Global configuration mode, allows the operator to change the interval between backups.

```configure
statistics-backup-interval minutes ]
no statistics-backup-interval ]
end
```

Notes:
- `minutes` - Enter an integer from 1 to 60 to set the number of minutes between backups.
- `no` with the command removes the statistics-backup-interval from the configuration.

**Displaying Backed-up Statistics**

To view the recovered counter values, a new keyword has been added to the show commands - `recovered-values` keyword option:

- `show mme-service statistics [ recovered-values ] [ verbose ]`
- `show mme-service statistics emm-only [ recovered-values ] [ verbose ]`
- `show mme-service statistics esm-only [ recovered-values ] [ verbose ]`

Notes:
- When the new keyword is used, only the `recovered` values will be displayed.

---

**Important:** In 17.2 CSCus36908, this behavior is changed so that output includes both current + recovered backed-up statistical values.
• If no session manager crash has occurred, then the recovered variables will be 0 (zero).

**Important:** The above point has been corrected so that behavior for recovered variable is correctly identified.

The list of counters and statistics that will be backed up are listed in the *Performance Indicator Changes* section below.

**Clearing Backed-up Statistics**

To clear the backed-up counter values, use one of the following commands with the new `recovered-values` keyword option:

- `clear mme-service statistics [ recovered-values ]`
- `clear mme-service statistics emm-only [ recovered-values ]`
- `clear mme-service statistics esm-only [ recovered-values ]`

**Notes:**
- When the new keyword is used, only the `recovered` values will be cleared.

**Performance Indicator Changes**

**mme-bk Schema**

The following statistics will be backed up for recovery. They are derived from the MME schema and perform the same functions as the statistics of similar names minus the `recovered-` prefix. For example, the `recovered-epsattach-imsi-attempted` listed below performs the same functions as the `epsattach-imsi-attempted` statistic in the MME schema:

- vpnid
- vpnname
- servname
- recovered-epsattach-imsi-attempted
- recovered-epsattach-imsi-success
- recovered-epsattach-guti-local-attempted
- recovered-epsattach-guti-local-success
- recovered-epsattach-guti-foreign-attempted
- recovered-epsattach-guti-foreign-success
- recovered-epsattach-ptmsi-attempted
- recovered-epsattach-ptmsi-success
- recovered-epstauattach-guti-foreign-attempted
- recovered-epstauattach-guti-foreign-success
- recovered-epstauattach-ptmsi-attempted
- recovered-epstauattach-ptmsi-success
• recovered-combinedattach-imsi-attempted
• recovered-combinedattach-imsi-success
• recovered-combinedattach-imsi-success-eps
• recovered-combinedattach-guti-local-attached
• recovered-combinedattach-guti-local-success
• recovered-combinedattach-guti-local-success-eps
• recovered-combinedattach-guti-foreign-attempted
• recovered-combinedattach-guti-foreign-success
• recovered-combinedattach-guti-foreign-success-eps
• recovered-combinedattach-ptmsi-attempted
• recovered-combinedattach-ptmsi-success
• recovered-combinedattach-ptmsi-success-eps
• recovered-combinedtauattach-guti-foreign-attempted
• recovered-combinedtauattach-guti-foreign-success
• recovered-combinedtauattach-guti-foreign-success-eps
• recovered-combinedtauattach-ptmsi-attempted
• recovered-combinedtauattach-ptmsi-success
• recovered-combinedtauattach-ptmsi-success-eps
• recovered-emmevent-auth-attempt
• recovered-emmevent-auth-success
• recovered-tau-periodic-attempted
• recovered-tau-periodic-success
• recovered-tau-normal-attempted
• recovered-tau-normal-success
• recovered-tau-active-attempted
• recovered-tau-active-success
• recovered-tau-sgw-change-attempted
• recovered-tau-sgw-change-success
• recovered-ecmevent-ue-svcreq-attempt
• recovered-ecmevent-ue-svcreq-success
• recovered-ecmevent-nw-svcreq-attempt
• recovered-ecmevent-nw-svcreq-success
• recovered-emm-msgtx-attach-accept
• recovered-emm-msgtx-attach-reject
- recovered-emm-msgtx-illegal-ue
- recovered-emm-msgtx-illegal-me
- recovered-emm-msgtx-eps-not-allowed
- recovered-emm-msgtx-decode-failure
- recovered-emm-msgtximei-not-accept
- recovered-emm-msgtx-roaming-restrict-ta
- recovered-emm-msgtx-plmn-not-allow
- recovered-emm-msgtx-tau-no-suitable-cell-ta
- recovered-emm-msgtx-tau-no-eps-svc-plmn
- recovered-emm-msgrx-attach-req
- recovered-emm-msgrx-tau-req
- recovered-esmevent-defbearact-attempt
- recovered-esmevent-defbearact-success
- recovered-dedi-brr-activation-ue-attempted
- recovered-dedi-brr-activation-ue-success
- recovered-dedi-brr-activation-nw-attempted
- recovered-dedi-brr-activation-nw-success
- recovered-esm-msgtx-brralloc-rej
- recovered-esm-msgtx-brralloc-rej-svc-not-supported
- recovered-esm-msgtx-brralloc-rej-svc-not-subscribed
- recovered-emmevent-x2ho-attempt
- recovered-emmevent-x2ho-success
- recovered-emmevent-s1ho-attempt
- recovered-emmevent-s1ho-success
- recovered-in-tau-ho-4gto4g-s10-attempted
- recovered-in-tau-ho-4gto4g-s10-success
- recovered-in-s1-ho-4gto4g-s10-attempted
- recovered-in-s1-ho-4gto4g-s10-success
- recovered-in-tau-ho-2g3to4g-gngp-attempted
- recovered-in-tau-ho-2g3to4g-gngp-success
- recovered-in-tau-ho-2g3to4g-s3-attempted
- recovered-emm-msgtx-ta-not-allow
- recovered-emm-msgtx-eps-non-eps-not-allowed
- recovered-emm-msgtx-no-eps-svc-plmn
- recovered-emm-msgtx-tau-illegal-ue
- recovered-emm-msgtx-tau-illegal-me
- recovered-emm-msgtx-tau-eps-not-allowed
- recovered-emm-msgtx-tau-decode-failure
- recovered-emm-msgtx-tau-no-bearer-active
- recovered-emm-msgtx-tau-ue-identity-unk
- recovered-emm-msgtx-tau-imei-not-accept
- recovered-emm-msgtx-tau-roaming-restrict-ta
- recovered-emm-msgtx-tau-plmn-not-allow
- recovered-emm-msgtx-tau-ta-not-allow
- recovered-in-tau-ho-2g3gto4g-s3-success
- recovered-emm-msgtx-attach-accept-retx
- recovered-emm-msgtx-tau-accept
- recovered-emm-msgtx-no-suitable-cell-ta
- recovered-emm-msgtx-tau-reject

**CSCup59406 - sesstrc task in over state during longevity/aggravator run**

**Feature Changes**

**Configuring Session Trace File Type**

To address the issues caused when the sesstrc task allocates memory over the allotted limit, under a random subscriber session trace load tests on P-GW/S-GW, support for B-type XML files is introduced in addition to the A-type files already supported.

**Previous Behavior:** The file type was A-type XML file and the type could not be changed.

**New Behavior:** The CLI has been modified (see Command Changes section) to allow the operator to select the file type generated by session trace. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

**Command Changes**

`session trace network-element`

The new optional `file-type` keyword enables the operator to determine which type of XML file is generated by the session trace:

`configure`
session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw } [ file-type { a-type | b-type } ] [ collection-timer | tce-mode ]

no session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw }

end

Notes:
- Default file-type is a-type.
- To keep the syntax simple, the optional file-type keyword must be entered before entering either of the other optional keywords.
- To modify the session trace network-element configuration, you must first enter the no session trace network-element form of the command to remove the session trace configuration.

CSCuq63874 - Increase the number of APN in remapping table

Feature Changes

Increase APN Entries for Remap Table

Previous Behavior: 100 was the maximum number of remap entries that could be created in an APN remap table.
New Behavior: The APN remap table entries limit has been extended from 100 to 300. The operator can use the apn-remap command to create and configure up to 300 entries in a single APN remap table, with one APN Remap Table per operator policy and the possibility of 1000 operator policies per system.

CSCuq95642 - [QvPC-DI] unable to start GTPUMgr, insufficient unserved memory

Feature Changes

QvPC-DI System Capacity

Previous Behavior: All DI system capacities based on memory were treated in the same manner.
New Behavior: DI systems with memory less than 48Gb are treated as reduced capacity (Medium Model) systems.

CSCur38243 - MME discards EGTP_CREATE_INDIRECT_DATA_FORWARDING_TUNNEL_RSP

Feature Changes

Extended Validation Options for UL F-TEID during HO
Up Link - Fully qualified Tunnel End Point Identifier

**Previous Behavior:**
- The MME did not accept ‘up link fully qualified tunnel end point identifier’ (UL F-TEID) in a Create Indirect Data Forwarding Response and response was dropped).
- The MME would only accept a UL F-TEID in a Create Indirect Data Forwarding Response from the S-GW if the IE instance was 4 and the interface type was set at 28 (SGW GTP-U interface for UL data forwarding).

**New Behavior:** The validation process has been modified so that the MME now accepts UL F-TEID in a Create Indirect Data Forwarding Response during intra-EUTRAN handover. So, the MME does not drop the response if the IE of the UL F-TEID instance is 4 and the interface type is set to either 28 (SGW GTP-U interface for UL data forwarding) or 1 (S1-U SGW GTP-U interface).

**Customer Impact:** The MME will accept a broader range of responses from the S-GW.
MME Enhancements for 17.0

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 *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 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**

---

**CSCua06554 - MME sends update bearer response reject when collision with TAU**

**Feature Changes**

**New Reject Cause During UBR Collision**

The MME now uses a different reject cause code to handle such error cases so that the P-GW can retry the failed procedure.

**Old Behavior:** The MME was rejecting an Update Bearer Request from the P-GW with cause EGTP_CAUSE_NO_RESOURCES_AVAILABLE (0x49) when a Modify Bearer Request was already in progress.

**New Behavior:** During this scenario, the MME will now reject the Update Bearer Request with the new cause EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS. This instructs the P-GW to retry the Update Bearer Request.
CSCub06751 - NASTAR Cell tracing

Feature Changes

Subscriber Information for LTE Cell Traces

With this feature the MME is capable of sending trace information (IMSI, Trace reference, etc.) for all UEs to the TCE, in compliance with 3GPP TS 32.413, Release 10. Upon trace activation, the eNodeB sends the allocated Trace Reference and Trace Recording References in a Cell Traffic Trace message to MME over S1AP, which looks up the IMSI/IMEI associated with the corresponding S1 session and forwards the two references and UE ID to the Trace Collection Entity (TCE) indicated in the Cell Traffic Trace message.

This functionality assists the TCE in correlating the Trace Reference and Trace Recording Session Reference generated by the eNodeB with the IMSI/IMEI corresponding to the traced session, since the eNodeBs only have access to the temporary UE identities but not to the permanent ones.

With this enhancement, operators have better trace information, improving the management of UEs.

Command Changes

session trace

The TCE Connection parameter and credentials will be configured via the CLI, using the existing session trace mechanism. To allow the configuration of different sets of TCE Connection parameters for Cell Traffic Tracing reports and regular Session Tracing, as well as the ability to enable/disable Cell Traffic Tracing independently from regular Session Tracing, a new Network Element, eNB, has been introduced.

The existing mechanism and CLI syntax will be used to configure, process, store and manage TCE Connection parameters for the eNB Network Element.

configure

    session trace network-element { all | enb | mme | pgw | sgw | ggsn } [ collection-timer sec ] [ tce-mode { none | push transport sftp path string username name { encrypted password enc_pw | password password } } ]

   no session trace network-element { all | enb | mme | pgw | sgw | ggsn }

end

Notes:

- The TCE IP address provided in the Cell Traffic Trace messages must correspond to the configured TCE connection. It is the responsibility of the operator to ensure that the TCE transport is properly configured at the MME and eNodeB.

- Up to 8 TCEs are supported for each MME instance.

Performance Indicator Changes

MME Schema
The following new bulk statistic has been added to the MME schema to track the total number of Cell Traffic Trace messages received from all eNodeBs.

- `s1ap-recdata-celltrfctrc`

**show session trace statistics**

The following fields have been added to report the total number of received Cell Traffic Trace files generated and deleted:

- Number of Cell Traffic Trace files generated
- Number of Cell Traffic Trace files deleted
  - No space
  - TCE Timeout

**show mme-service statistics s1ap**

The following field has been added to report the total number of received Cell Traffic Trace signals for all MME services:

- Cell Traffic Trace

**CSCuf59965, CSCum41122, CSCum55668 - Customized Inter-MME/SGW S1-Handover & TAU Procedure for PS-LTE Support**

**Feature Changes**

**Customized Inter-MME/SGW S1-Handover & TAU Procedure for PS-LTE Support**

In the Public Safety LTE (PS-LTE) network, every MME is co-located with an S-GW and at least one P-GW, and the MME must always use the co-located S-GW and a co-located P-GW for all calls that it handles. This requires configuring the IP addresses of the S11 interface of the S-GW as part of the MME service configuration, and the S5/S8 interface of the P-GW as part of an APN profile configuration. An MME configured for PS-LTE network operation will not send any DNS queries for S-GW or P-GW lookups; it will only use the S-GW configured for PS-LTE operation and the P-GW configured in the matching APN profile, regardless of any other configuration present.

All intra-MME S1 and X2 handovers and all TAU Requests with a local GUTI will be serviced by the same S-GW that is configured for PS-LTE network operation with the P-GW(s) used at the time of the initial Attach or relocation to the MME. S-GW relocation is neither necessary nor supported for intra-MME handovers or intra-MME TAU Requests.

This feature allows the co-location of the MME, P-GW and S-GW nodes for Public Safety deployments.

This feature 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**

```
ps-lte
```
This new command enables PS-LTE network operation for the MME and provisions the co-located S-GW address which the MME service should use.

`configure`

```
context context_name

mme-service mme_svc_name

ps-lte sgw ip_address

[ no ] ps-lte

end
```

Notes:

- `ip_address` is an IPv4 or IPv6 address for the S11 interface of the co-located S-GW.
- The S-GW address configured in this command is the one which will always be used by the MME while in PS-LTE network operation. An MME configured for PS-LTE network operation will not send any DNS queries for S-GW or P-GW lookups; it will only use the S-GW configured in the CLI command for PS-LTE operation and the PGW configured in the matching APN profile, regardless of any other configuration present. All intra-MME S1 and X2 handovers and all TAU Requests with a local GUTI will be serviced by the same S-GW that is configured for PS-LTE network operation with the P-GW(s) used at the time of the initial Attach or relocation to the MME in question. S-GW relocation is neither necessary nor supported for intra-MME handovers or intra-MME TAU Requests.
- If this command is issued on an mme-service instance that is currently operating and that did not have PS-LTE network operation previously configured, any UEs that were previously attached or relocated under normal LTE network operation will continue to operate using normal LTE network behavior, rather than the PS-LTE network behavior described in this document. All UEs that attach or relocate to this network after this command is issued will operate using PS-LTE network behavior with the configured S-GW chosen for all new calls.
- If this command is issued on an mme-service instance that is currently operating and that did have PS-LTE network operation previously configured using a different S-GW address, any UEs that were previously attached or relocated under PS-LTE network operation will continue to operate using the S-GW that was configured at the time the UE either attached or relocated to this MME. All UEs that attach or relocate to this network after this command is issued will operate using PS-LTE network behavior with the newly configured S-GW chosen for all new calls.
- If the `no ps-lte` CLI command is issued on an mme-service instance that is currently operating and had PS-LTE network operation previously configured, any UEs that were previously attached or relocated under PS-LTE network operation will continue to operate using PS-LTE network behavior, with the S-GW that was configured at the time the UE either attached or relocated to this MME. All UEs that attach or relocate to this network after this command is issued will operate using normal LTE network behavior.

`ho-resource-release-timeout`

This new command configures the timer that is started when the source MME initiates a handover. This command is available for all MME services, regardless if the license for PS-LTE functionality is present.

`configure`

```
context context_name
```

Notes:
mme-service mme_svc_name

    ho-resource-release-timeout timeout

    [ default ] ho-resource-release-timeout

end

Notes:

- This is the amount of time in milliseconds that the MME will hold on to bearers and E-RABs after an S1-based handover has been initiated. When this timer expires, the source MME will send a UE Context Release to the source eNodeB. Refer to 3GPP TS 23.401 Section 5.5.1.2.2 for additional information about the use of this timer.
- timeout must be an integer from 500 through 15000.
- Default: 5000 (5 seconds).

Performance Indicator Changes

show mme-service all

The following fields have been added to the output of the show mme-service all command to display the configuration of the above commands:

- PS-LTE Operation
- SGW Address
- HO Resource Release Timeout

CSCuh04641 - Timers for congestion conditions

Feature Changes

Congestion Control Enhancements

This feature requires that a valid MME Resiliency license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

With this StarOS release, the MME supports several of the 3GPP TS23.401 R10 machine type communications (MTC) overload control mechanisms to be used in the handling of signaling bursts from machine-to-machine (M2M) devices. This feature set allows the operator to handle the signaling storm MTC devices can bring to the network thus ensuring a more robust network and more efficient resource utilization.

This feature enhances the MME product to support congestion control in better way so that MME can reject or drop requests based on the low priority of the subscribers or based on the APN.

When there is congestion in the system, MME detects it based on the already existing congestion detection techniques. Based on the level of congestion, the MME application running in session manager will apply the congestion action profile configured for that congestion level.

- **Congestion Control for LAPI Subscribers:** The current CLI configuration for congestion action profile has been enhanced to take action (reject or drop) for MTC subscribers with Low Access Priority Indication (LAPI).
If a specific EMM request is received when the MME is experiencing congestion, the MME will reject/drop requests for those which include LAPI indicator.

The MME decodes and stores in the UE context/default EPS bearer context, the presence of LAPI indication from device properties IE if this indicator is set to “MS is configured for NAS signaling low priority” in any of attach/extended service/TAU/bearer resource allocation/bearer resource modification/PDN connectivity requests. This is displayed in the output of `show mme session full` command. If the NAS signaling low priority indication is provided in a PDN CONNECTIVITY REQUEST message, the MME stores the NAS signaling low priority indication within the PDN context activated due to the PDN connectivity request procedure.

- **Congestion Control for Specific APNs**: The current CLI configuration for congestion action profile has been enhanced to take action (reject or drop) during congestion based on APN. Specific APNs can be configured under the Operator Policy configuration mode to be considered for APN-based congestion control. If a specific EMM request is received when the MME is experiencing congestion, the MME will reject/drop requests for those specific APNs.

  The existing APN configuration under Operator Policy has been enhanced to define specific APNs for congestion control.

  EMM and/or ESM requests coming from UEs with LAPI indication and/or which match the APNs configured under the Operator Policy for congestion control will be dropped/rejected if the corresponding request is configured to be dropped/rejected in congestion-action-profile.

  The Session manager uses the congestion level received from MME manager as part of new requests and uses it for selection of the appropriate congestion-action-profile (critical/major/minor).

  The MME has also been enhanced to allow mapping of specific diameter result codes to NAS cause code #42 (Severe Network Failure). Refer to the `diameter-result-code-mapping s6a` command in the following section for more information.

  Refer also to CSCum37475 - MTC Support : Reject causes with MM & SM back-off time in this document for more information about related EMM and ESM back-off timers related to congestion control.

### Command Changes

**drop**

This command has been enhanced to drop incoming packets based on LAPI (Low Access Priority Indication) or based on APN when a congestion control threshold has been reached. This functionality is configured using the new `lapi` and `apn-based` keywords.

Additionally, a new keyword, `brr-cntxt-mod-requests`, has been added to configure the MME to drop Bearer Context Modification Requests during a congestion condition.

```
configure

lte-policy

congestion-action-profile profile_name

  drop { addn-brr-requests | addn-pdn-connects | brr-cntxt-mod-requests | combined-attaches | handovers | ps-attaches | s1-setups | service-request | tau-request } [ lapi ] [ apn-based ]

end
```
Notes:

- When a congestion action profile is configured with the `drop <call-event> lapi` option, only LAPI requests will be dropped for those call-events during congestion. However, if the call-event is configured without the `lapi` option, all LAPI and non-LAPI requests will be dropped.

- If the congestion action profile is configured with the `drop <call-event> apn-based` option, only the requests for those APNs configured for congestion control in the Operator Policy will be dropped for those call-events during congestion. However, if the call-event is configured without the `apn-based` option, all requests will be dropped. Refer to the `apn` command later in this section to enable congestion control for a specific APN.

- If the congestion action profile is configured with both the `lapi` and `apn-based` options, the call-event will be dropped only if both conditions are matched.

reject

This command has been enhanced to reject messages based on LAPI (Low Access Priority Indication) or based on APN when a congestion control threshold has been reached. This functionality is configured using the `lapi` and `apn-based` keywords.

Additionally, a new keyword, `brr-ctxt-mod-requests`, has been added to configure the MME to reject Bearer Context Modification Requests during a congestion condition.

configure

```plaintext
lte-policy

congestion-action-profile profile_name

    reject { addn-brr-requests | addn-pdn-connects | brr-ctxt-mod-requests |
            combined-attaches | handovers | ps-attaches | s1-setups | service-request | tau-request } 

    [ lapi ] [ apn-based ]

end
```

Notes:

- When a congestion action profile is configured with the `reject <call-event> lapi` option, only LAPI requests will be rejected for those call-events during congestion. However, if the call-event is configured without the `lapi` option, all LAPI and non-LAPI requests will be rejected.

- If the congestion action profile is configured with the `reject <call-event> apn-based` option, only the requests for those APNs configured for congestion control in the Operator Policy will be rejected for those call-events during congestion. However, if the call-event is configured without the `apn-based` option, all requests will be rejected. Refer to the `apn` command later in this section to enable congestion control for a specific APN.

- If the congestion action profile is configured with both the `lapi` and `apn-based` options, the call-event will be rejected only if both conditions are matched.

apn

This command has been enhanced to enable Congestion Control for a particular APN network identifier using the new `congestion-control` keyword.

configure
operator-policy policy_name

[ no ] apn network-identifier apn_net_id congestion-control

end

Notes:
- During an Attach, all subscribed APNs will be checked to determine if any of them is configured for congestion. Attach request would be rejected if any of the subscribed APN is configured for congestion.
- During an Additional PDN, the requested APN will be checked to determine if it is configured for congestion. This congestion control enhancement also supports the APN remap table functionality. The APN to which it is remapped will be checked for the congestion-control configuration. For example, if APN abc.com is remapped to xyz.com and xyz.com has been configured for congestion-control, the MME can drop/reject these connection attempts.

diameter-result-code-mapping s6a

This command now includes a new keyword to map EMM NAS cause code #42, “Severe Network Failure” with s6a diameter result codes.

configure

call-control-profile profile_name

diameter-result-code-mapping s6a diameter_result_code mme-emm-cause severe-network-failure

remove diameter-result-code-mapping s6a diameter_result_code }

end

Notes:
- NAS cause code #42 (Severe Network Failure) can now be applied to any diameter result code using the new severe-network-failure keyword. For example: diameter-result-code-mapping s6a diameter-unable-to-comply mme-emm-cause severe-network-failure

Performance Indicator Changes

MME Schema

The following new MME Schema bulk statistics have been added to track congestion-related EMM reject causes. No new ESM statistics were introduced as the cause “insufficient resources” already existed.

- emm-msgtx-attach-reject-congestion
- emm-msgtx-attach-reject-severe-network-failure
- emm-msgtx-service-reject-congestion
- emm-msgtx-tau-congestion
- emm-msgtx-tau-severe-network-failure
- emm-msgtx-tau-intra-congestion
• emm-msgtx-tau-intra-severe-network-failure
• emm-msgtx-tau-inter-congestion
• emm-msgtx-tau-inter-severe-network-failure

show mme-service statistics

The following highlighted fields have been added to display statistics related to congestion-related EMM reject causes:

• Total EMM Control Messages
• Sent
• Attach Reject
• Congestion
• Severe Network Failure
• Service Reject
• Congestion
• TAU Reject Total
• Congestion
• Severe Network Failure
• TAU Reject Intra MME
• Congestion
• Severe Network Failure
• TAU Reject Inter MME
• Congestion
• Severe Network Failure

show congestion-control statistics mme full

The following highlighted fields have been added to provide statistics for the number of Bearer Context Modification Requests dropped or rejected during a congestion condition.

• Critical Congestion Policy Action
  • Brr-ctxt-mod-request
  • Rejected
  • Dropped
• Major Congestion Policy Action
  • Brr-ctxt-mod-request
  • Rejected
  • Dropped
• Minor Congestion Policy Action
  • Brr-ctxt-mod-request
show lte-policy congestion-action-profile name

The output of this command now displays the configuration of LAPI and APN-based congestion options. For example, the following output shows a congestion control profile which is configured to drop UE initiated bearer resource requests. The MME will drop only those subscribers which are subscribed to specific APNs (as defined in Operator Policy) and which are LAPI:

```
Congestion Action Profile 1
  none handovers
  none combined-attaches
  none ps-attaches
  none addn-pdn-connects
  drop addn-brr-requests lapi apn-based
...
```

show mme-service session full

The following highlighted fields have been added to display LAPI information for each session. LAPI indication can be received in any of attach/extended service/TAU/bearer resource allocation/bearer resource modification/PDN connectivity requests. If the indication is received in any of the above messages, it is displayed at the UE information level. If the indication is received in a PDN CONNECTIVITY REQUEST message, it is displayed at the PDN information level as well.

- **Low Access Priority Indication**: Yes/No
- **Initial UE establishment cause**: Delay Tolerant Access / High Priority Access / Emergency / MT-Access / Unknown
- **PDN Information**
- **Low Access Priority Indication**: Yes/No

show subscribers summary mme-service <name>

The following field has been added to this command to display the current number of LAPI devices.

- LAPI Devices

show subscribers mme-only

The following field has been added to this command to display the current number of LAPI devices.

- LAPI Devices

show mme-service session

The following field has been added to this command to display the current number of LAPI sessions.
- Total LAPI sessions

**CSCul07972 - Stats: Counting of failures where no REJECT or ACCEPT is send**

**Feature Changes**

**Statistics Enhancements**

New counters and bulk statistics have been introduced to track procedure failures (attach, intra-MME TAU, and inter-MME TAU) where no Reject or Accept is sent, such as during a detach and attach procedure collision. These counters and bulk statistics are collected at the MME service level, and at the eNodeB or TAI level.

Additional failure statistics have also been introduced to track failure reasons for a select set of procedures.

**Performance Indicator Changes**

| Important: Two corrections have been made in the ‘show mme-service statistics’ section - please look for the ‘Correction’ indication below. |

**MME Schema**

The following bulk statistics are provided to track attaches where no reject or accept is sent:

- emm-msgtx-attach-ue-initiated-detach
- emm-msgtx-attach-detach-in-progress
- emm-msgtx-attach-auth-failed
- emm-msgtx-attach-diff-attach-recv
- emm-msgtx-attach-no-rej-send-total

The following bulk statistics are provided to track Inter-MME TAUs where no reject or accept is sent:

- emm-msgtx-tau-inter-auth-failed
- emm-msgtx-tau-inter-ue-initiated-detach
- emm-msgtx-tau-inter-diff-tau-recv
- emm-msgtx-tau-inter-no-rej-send-total

The following bulk statistics are provided to track Intra-MME TAUs where no reject or accept is sent:

- emm-msgtx-tau-intra-auth-failed
- emm-msgtx-tau-intra-ue-initiated-detach
- emm-msgtx-tau-intra-diff-tau-recv
- emm-msgtx-tau-intra-detach-in-progress
- emm-msgtx-tau-intra-attach-awaits-mb-resp
- emm-msgtx-tau-intra-no-rej-send-total
The following bulk statistics provide a sum of both Intra-MME TAUs and Inter-MME TAUs where no reject or accept is sent:

- emm-msgtx-tau-auth-failed
- emm-msgtx-tau-ue-initiated-detach
- emm-msgtx-tau-diff-tau-recv
- emm-msgtx-tau-detach-in-progress
- emm-msgtx-tau-attach-awaits-mb-resp
- emm-msgtx-tau-no-rej-send-total

The following bulk statistics are provided to track attach procedure failures:

- attach-proc-fail-max-retx-auth-req
- attach-proc-fail-max-retx-sec-mode-cmd
- attach-proc-fail-max-retx-attach-accept
- attach-proc-fail-setup-timeout-exp
- attach-proc-fail-sctp-fail
- attach-proc-fail-guard-timeout-exp
- attach-proc-fail-ue-ctxt-release
- attach-proc-fail-max-retx-esm-info-req
- attach-proc-fail-other-reasons
- attach-proc-fail-total

The following bulk statistics are provided to track Intra-MME TAU procedure failures:

- intra-mme-tau-proc-fail-max-retx-auth-req
- intra-mme-tau-proc-fail-max-retx-sec-mode-cmd
- intra-mme-tau-proc-fail-max-retx-tau-accept
- intra-mme-tau-proc-fail-sctp-fail
- intra-mme-tau-proc-fail-guard-timeout-exp
- intra-mme-tau-proc-fail-ue-ctxt-release
- intra-mme-tau-proc-other-reasons
- intra-mme-tau-proc-total

The following bulk statistics are provided to track Inter-MME TAU procedure failures:

- inter-node-tau-proc-fail-max-retx-auth-req
- inter-node-tau-proc-fail-max-retx-sec-mode-cmd
- inter-node-tau-proc-fail-max-retx-tau-accept
- inter-node-tau-proc-fail-setup-timeout-exp
- inter-node-tau-proc-fail-sctp-fail
- inter-node-tau-proc-fail-guard-timeout-exp
- inter-node-tau-proc-fail-ue-ctxt-release
- inter-node-tau-proc-fail-relocation-failure
- inter-node-tau-proc-other-reasons
- inter-node-tau-proc-total

The following bulk statistics are provided to track Idle-mode (IM) exit procedure failures:

- im-exit-proc-fail-max-retx-tau-accept
- im-exit-proc-fail-sctp-fail
- im-exit-proc-fail-guard-timeout-exp
- im-exit-proc-fail-ue-ctxt-release
- im-exit-proc-fail-other-reasons
- im-exit-proc-fail-total

**TAI Schema**

The following bulk statistics are provided to track attaches where no reject or accept is sent:

- tai-emm-msgtx-attach-auth-failed
- tai-emm-msgtx-attach-ue-initiated-detach
- tai-emm-msgtx-attach-detach-in-progress
- tai-emm-msgtx-attach-diff-attach-recv
- tai-emm-msgtx-attach-no-rej-send-total

The following bulk statistics are provided to track Intra-MME TAUs where no reject or accept is sent:

- tai-emm-msgtx-tau-intra-auth-failed
- tai-emm-msgtx-tau-intra-ue-initiated-detach
- tai-emm-msgtx-tau-intra-diff-tau-recv
- tai-emm-msgtx-tau-intra-detach-in-progress
- tai-emm-msgtx-tau-intra-attach-awaits-mbr-resp
- tai-emm-msgtx-tau-intra-no-rej-send-total

The following bulk statistics are provided to track Inter-MME TAUs where no reject or accept is sent:

- tai-emm-msgtx-tau-inter-auth-failed
- tai-emm-msgtx-tau-inter-ue-initiated-detach
- tai-emm-msgtx-tau-inter-diff-tau-recv
- tai-emm-msgtx-tau-inter-no-rej-send-total

The following bulk statistics provide a sum of both Intra-MME TAUs and Inter-MME TAUs where no reject or accept is sent:

- tai-emm-msgtx-tau-auth-failed
- tai-emm-msgtx-tau-ue-initiated-detach
• tai-emm-msgtx-tau-diff-tau-recv
• tai-emm-msgtx-tau-detach-in-progress
• tai-emm-msgtx-tau-attach-awaits-mbr-resp
• tai-emm-msgtx-tau-no-rej-send-total

show mme-service statistics

CORRECTIONS: (1) In the paragraph below, ‘inter-Node’ has replaced ‘inter-MME’. (2) 'Authentication Failed' added under 'No InterNode TAU Rej/Act'

The following counters have been added to the output of the show mme-service statistics command to track procedure failures (attach, intra-MME TAU, and inter-Node TAU) where no Reject or Accept is sent:

EMM Control Messages:

...  
No Attach Reject/Accept:  0  
Authentication Fail:  0  UE initiated detach:  0  
Detach in progress:  0  Different Attach Recvd:  0  
...

No TAU Rej/Accept Total:  0  
Authentication Failed:  0  UE initiated detach:  0  
Different TAU received:  0  Detach in progress:  0  
Attach awaits MBResp:  0  
No IntraMME TAU Rej/Act:  0  
Authentication Failed:  0  UE initiated detach:  0  
Different TAU received:  0  Detach in progress:  0  
Attach awaits MBResp:  0  
No InterNode TAU Rej/Act:  0  
Authentication Failed:  0  UE initiated detach:  0  
Different TAU received:  0

show mme-service statistics verbose

The following Procedure Failure Reason counters have been added to the output of the show mme-service statistics verbose command:

Attach failure:  0
<table>
<thead>
<tr>
<th>Event</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max retx auth req:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx attach accept:</td>
<td>0</td>
</tr>
<tr>
<td>SCTP/S1-failure:</td>
<td>0</td>
</tr>
<tr>
<td>UE context release:</td>
<td>0</td>
</tr>
<tr>
<td>Other reasons</td>
<td>0</td>
</tr>
<tr>
<td>Intra MME TAU failure:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx auth req:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx sec mode cmd:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx TAU accept:</td>
<td>0</td>
</tr>
<tr>
<td>Internal guard timeout:</td>
<td>0</td>
</tr>
<tr>
<td>UE context release:</td>
<td>0</td>
</tr>
<tr>
<td>Internal guard timeout:</td>
<td>0</td>
</tr>
<tr>
<td>Other reasons</td>
<td>0</td>
</tr>
<tr>
<td>Inter node TAU failure:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx auth req:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx sec mode cmd:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx TAU accept:</td>
<td>0</td>
</tr>
<tr>
<td>Setup timeout expiry:</td>
<td>0</td>
</tr>
<tr>
<td>SCTP/S1-failure:</td>
<td>0</td>
</tr>
<tr>
<td>UE context release:</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>IM exit failure:</td>
<td>0</td>
</tr>
<tr>
<td>Max retx TAU accept:</td>
<td>0</td>
</tr>
<tr>
<td>SCTP/S1-failure:</td>
<td>0</td>
</tr>
<tr>
<td>Internal guard timeout:</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>Relocation failure:</td>
<td>0</td>
</tr>
</tbody>
</table>

**CSCul17198 - [SGW] GTP echo and GTP message retry shall be configured separately**

**Feature Changes**

**Separate Configuration for GTPC Echo and GTPC Non-Echo Messages**

Previously, the GTP echo and GTP message retry timer could be configured separately, but the number of GTPC echo requests could not. The maximum retry number now can be configured separately along similar lines as the timer configuration.

In egtp-service, the `echo-max-retransmissions` keyword is added to allow the separate configuration of GTPC echo retransmissions.
MME Changes in Release 17

MME Enhancements for 17.0

Previous Behavior: The maximum number of retransmissions for Echo Requests was configured by `max-retransmissions` configuration option.

New Behavior: `echo-max-retransmissions` is introduced explicitly for the configuration of echo max retransmissions in both GTPC Service Configuration Mode.

Command Changes

gtpc echo-max-retransmissions

The `echo-max-retransmissions` keyword is now available in EGTP Service Configuration Mode. This keyword is available to allow for the separate configuration of GTP echo retransmissions.

configure

c context context_name

egtp-service egtp_service_name

gtpc echo-max-retransmissions number

default gtpc echo-max-retransmissions

d end

Notes:

- `Important: service_name` must be unique across all contexts.

- `echo-max-retransmissions`: Configures the maximum retries for GTP Echo requests. This option must be an integer from 0 to 15. The default is 4. If `echo-max-retransmissions` configuration option is not configured, then the `max-retransmissions` configuration will be used for maximum number of echo retries.

Performance Indicator Changes

show egtp-service [ all | name service_name ]

The output of this command has been enhanced to show the configured number of GTPC echo max retransmissions.

- GTPC Echo Max Retransmission

CSCum35622 - Ability to define same TAI in multiple TAI Lists

Feature Changes

Ability to define same TAI in multiple TAI Lists

Prior to 17.0, the MME could have a tracking area in only one tracking area list (TAI List). Consequently, the tracking area list assigned to subscribers attaching from different TAI will be same, even if the adjacency of these tracking areas is not same. This results in MME getting TAU even as subscribers moved to the adjacent area.
With this enhancement, the MME will allow operators to configure adjacency lists as TAI Lists, thus reducing the Tracking Area Updates (TAU) received by MME. This feature enables the MME to send configured customized TAI List in ATTACH_ACCEPT/TAU_ACCEPT when a request is received from the custom or border TAI.

The reduced TAU results in less signaling load on the MME and better operational efficiency.

**Command Changes**

tai-custom-list

This new command creates a custom TAI list, and enters the tai-cstm-list configuration mode.

```plaintext
configure
lte-policy
tai-mgmt-db db_name
    [ no ] tai-custom-list tac cstm_tac_value [ -noconfirm ]
end
```

Notes:
- `cstm_tac_value`: Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535.
- A maximum of 1000 Custom TAI Lists can be configured per TAI Management Database.

tai

This command configures the Tracking Area Identifiers (TAIs) within this custom TAI list.

```plaintext
configure
lte-policy
tai-mgmt-db db_name
tai-custom-list tac cstm_tac_value
    [ no ] tai mcc number mnc number { tac value } +
end
```

Notes:
- `mcc number`: Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.
- `mnc number`: Specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.
- `tac value` : Specifies the Tracking Area Code (TAC) portion of the TAI as an integer from 1 through 65535. Up to 16 TAC values can be entered on a single line.
- A maximum of 15 TAIs can be configured per Custom TAI List.
A TAC can be added in this custom TAI list only if it has already configured in any of the TAI management objects within this TAI Management Database.

All the TAIs configured within a Custom TAI List are assumed to use same S-GW, time-zone, zone-code, and other configurations within the TAI Management Object. If a Custom TAI List includes TAIs from different objects then those objects should be configured with same S-GW address, time-zone, zone-code, etc.

```
show lte-policy tai-mgmt-db
```

This command includes two new keywords to display information about a specific TAI Management Object (tai-mgmt-obj object_name) or Custom TAI List (tai-custom-list tac cstm_tac_value).

```
show lte-policy tai-mgmt-db { name db_name [ tai-mgmt-obj obj_name | tai-custom-list tac cstm_tac_value ] | summary }  
```

Performance Indicator Changes

```
show lte-policy tai-mgmt-db
```

The output of the `show lte-policy tai-mgmt-db summary` command now lists all TAI Management Objects and Custom TAI List TACs configured within each TAI Management Database. For example:

- TAI Management DB taidb1
- TAI Management Object obj1
- TAI Management Object obj2
- Custom TAI List Tac 3024

The output of the `show lte-policy tai-mgmt-db name db_name` command has been enhanced to display all TAI Management Objects and Custom TAI List TACs configured within the specified TAI Management Database.

```
show lte-policy tai-mgmt-db name <name>
```

The following command has been enhanced with the new `tai-mgmt-obj obj_name` keyword. Using this keyword displays the configuration of the specified TAI Management Object within specified TAI Management Database.

```
show lte-policy tai-mgmt-db name db_name tai-mgmt-obj object_name
```

The following command has been enhanced with the new `custom-tai-list tac number` keyword. Using this keyword displays the configuration of the specified Custom TAI List within specified TAI Management Database.

```
show lte-policy tai-mgmt-db name db_name tai-custom-list tac number
```

CSCum35642 - Improve ENB support from 32K to 64K

Feature Changes

Increase eNodeB Supported From 32,000 to 64,000
With this feature the MME can now support a maximum of 64,000 eNodeB connections on the ASR 5500 platform with a fully loaded system (chassis). The maximum number of MME Managers has been increased to 16 in order to support this increase in eNodeB connections.

On the ASR 5000, the number of supported eNodeBs and MME Managers has not changed (32,000 and 8 respectively). Operators can potentially reduce operating expenditures as a greater number of eNodeBs can be connected to the same MME.

**CSCum35668 - Node Restoration: MME handling of PGW restart**

**Feature Changes**

**MME handling of PGW Restart**

This feature requires that a valid MME Resiliency license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

P-GW Restart Notification Procedure is a standards-based procedure supported on the S-GW to notify detection of P-GW failure to the MME/S4-SGSN. P-GW failure detection is performed by the S-GW when it detects that the P-GW has restarted (based on restart counter received from the restarted P-GW) or when it detects that P-GW has failed but not restarted (based on path failure detection). When an S-GW detects that a peer P-GW has restarted, it deletes all PDN connection table data and bearer contexts associated with the failed P-GW and notifies the MME via P-GW Restart Notification. The S-GW indicates in the echo request/response on S11/S4 interface that the P-GW Restart Notification procedure is supported.

P-GW Restart Notification Procedure is an optional procedure and is invoked only if both the peers, MME/S4-SGSN and S-GW, support it.

In the absence of this procedure, the S-GW will initiate the Delete procedure to clear all the PDNs anchored at that failed P-GW, which can lead to flooding of GTP messages on S11/S4 interface if there are multiple PDNs using that S-GW and P-GW.

In this release, the MME adds support for the P-GW restart handling procedures as specified in 3GPP TS 23.007 v11.6.0. An S-GW will send the “PGW Restart Notification” message only to the SGSNs / MMEs that indicated their support of this feature through the Echo Request -> Node Features IE -> PRN bit.

This feature reduces the S11 signaling load between the S-GW and MME in case of a P-GW restart.

**PDN Deactivation Behavior**

If a PDN is impacted and needs to be restored:

- If all PDNs of a UE are impacted, a UE in ECM-Connected state will be explicitly detached with cause “reattach required” and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be explicitly detached with cause “reattach required”. Otherwise, the UE will be implicitly detached.

- If some PDNs of a UE are impacted, a UE in ECM-Connected will be sent NAS Deactivate Bearer Request with cause “reactivation requested” and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be sent a NAS Deactivate Bearer Request with cause “reactivation requested”. Otherwise, the PDN will be locally deactivated.

If a PDN is impacted but does not need to be restored:

- If all PDNs of a UE are impacted, a UE in ECM-Connected state will be explicitly detached with cause “reattach required” and a UE in ECM-IDLE state will be paged. If Paging is successful, then the UE will be explicitly detached with cause “reattach required”. Otherwise, the UE will be implicitly detached.
- If some PDNs of a UE are impacted, a UE in ECM-Connected will be sent NAS Deactivate Bearer Request with cause “regular deactivation”, and a UE in ECM-IDLE will not be paged and will be locally deactivated in a paced manner.

**PDN Deactivation Rate**

By default, the MME will perform deactivations at the rate of 100 PDNs (50 Idle + 50 Connected) per session manager per second. This rate will be applied to MME specific pacing queues (Idle & Connected).

This default pacing rate can be altered using the **MME Messaging Rate Control** feature.

Refer to the *MME Administration Guide* and to the `network-overload-protection mme-tx-msg-rate` command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for more information about this feature.

**Note:** Configuration of this deactivation rate should be based on appropriate dimensioning exercise to arrive at the appropriate rate.

**PDN Reactivation Behavior**

After the affected subscribers have been deactivated, the MME will prioritize the re-activation of impacted PDN connections based on subscribed APN restoration priority, if received from the HSS. If an APN restoration priority is not received from the HSS, then this locally configured value is used. If there is no local configuration then by default such PDNs will be assigned the lowest restoration priority.

**Limitations**

In this release, the MME will not deactivate a PDN connection upon receiving P-GW Restart Notification when the P-GW serving the PDN is dual IP stack.

The PGW Restart Notification is received with cause PGW-NOT-RESPONDING, however the MME is not able to find the matching P-GW entry as the MME stores either IPv4 or IPv6 PGW address.

This occurs when the PGW Restart Notification does not contain the P-GW IP address stored by MME.

**Command Changes**

```plaintext
getc node-feature pgw-restart-notification
```

The MME now supports P-GW Restart Notification functionality through the existing `pgw-restart-notification` keyword per EGTP service.

```plaintext
configure

context context_name

egtp-service svc_name

[ no ] gtpc node-feature pgw-restart-notification

end
```

Notes:

- This command enables the MME to advertise the PGW restart notification in EGTPC echo request/response messages.

**apn-restoration priority**
This command configures the APN restoration priority for an APN profile. This determines the priority given for re- 
activation of subscribers after receiving a P-GW restart notification. The MME will only restore PDNs for which the 
APN restoration priority is configured and/or received from HSS. Otherwise PDNs will be released by regular 
deactivation.

```plaintext
configure

apn-profile profile_name

    apn-restoration priority priority_value

[ no ] apn-restoration priority

end

Notes:

- Use the `apn-restoration` command to define a restoration priority for this APN. By default, a restoration 
  priority of 16 (1 is highest, 16 is lowest) is applied.
- To apply a different restoration priority for this APN, include the `priority` keyword and provide a 
  `priority_value` as an integer from 1 through 16.

apn

This command includes a new keyword to define restoration priority for emergency sessions.

```plaintext
configure

lte-policy

    lte-emergency-profile profile_name

        apn apn_name pdn-type { ipv4 | ipv4v6 | ipv6 } [ restoration-priority priority_value ]

    end

Notes:

- Use the `restoration-priority priority_value` keyword to define the restoration priority (1 is highest, 16 is lowest) for the APN used for emergency PDN connections. By default, a restoration priority of 16 is applied.

precedence

This command includes a new `node-restoration` keyword. This keyword enables the operator to define a 
precedence value for node restoration paging traffic within an LTE Policy paging map.

```plaintext
configure

lte-policy

    paging-map map_name
precedence priority traffic-type { signaling [ detach | lcs | node-restoration ] } paging-profile paging_profile_name 

[ no ] precedence priority 

end

Notes:

- Use the node-restoration keyword to define a precedence and paging-map for node restoration (due to P-GW Restart Notification) paging traffic.
- By default, no precedence is assigned to node restoration traffic. The MME treats node restoration paging with the least priority.
- Refer to the LTE Paging Map Configuration Mode Commands chapter in the Command Line Interface Reference for more information about the precedence command.

Performance Indicator Changes

MME Schema

The following new bulk statistics have been introduced in this release to track paging in order to deactivate PDNs. Separate bulk statistics are used to track paging to detach UEs (for example, a signaling-detach is used for paging to detach a UE due to PRN).

- signaling-noderes-paging-init-events-attempted
- signaling-noderes-paging-init-events-success
- signaling-noderes-paging-init-events-failure
- signaling-noderes-paging-last-enb-success
- signaling-noderes-paging-last-tai-success
- signaling-noderes-paging-tai-list-success

show egtpc statistics

The output of the show egtpc statistics command now displays the following counters for P-GW Restart Notification requests and acknowledgements.

PGW Restart Notification Request:

| Total TX: | 0 | Total RX: | 0 |
| Initial TX: | 0 | Initial RX: | 0 |
| Retrans TX: | 0 | Retrans RX: | 0 |
| Discarded: | 0 |
| No Rsp RX: | 0 |
show mme-service statistics

The output of the show mme-service statistics command now displays the following counters for signaling node restoration events.

Paging Initiation for SIGNALING Node Restoration Events:

- Attempted: 0
- Success: 0
- Failures: 0
- Success at Last n eNB: 0
- Success at Last TAI: 0
- Success at TAI List: 0

show apn-profile full all

The output of this command now displays the restoration priority configured for each APN.

- APN Restoration Priority

show lte-policy lte-emergency-profile name

The output of show lte-policy lte-emergency-profile name name now displays the APN restoration priority configured for emergency sessions.

The following sample output shows the configuration of a LTE Emergency Profile named lte123 which defines APN abcd.com with node restoration priority of 1:

```
Lte Emergency Profile lte123
  ue-validation-level none
  apn abcd.com pdn-type ipv4 restoration-priority 1
```

show lte-policy paging-map name

The output of show lte-policy paging-map name name now displays the precedence value and paging profile configured for node restoration paging traffic.

The following sample output shows a paging map where node restoration paging traffic is assigned a precedence of 2, and paging is performed according to the paging profile named ltepp:

```
===================================================================
Paging Map : pm1
```

Total TX: 0 Total RX: 0
Initial TX: 0 Initial RX: 0
Accepted: 0 Accepted: 0
Denied: 0 Denied: 0
Retrans TX: 0 Discarded: 0
Precedence 2 : Signaling-NODE-RESTORATION ; Paging is performed as per paging-profile ltepp

show mme-service session full

The output of this command now displays the APN restoration priority for the session, as shown in the following sample output:

SessMgr Instance: 1
MSID: 123456789012346 Callid: 00004e21

PDN Information:
APN Name: cisco.com
APN Restriction: 0

Marked for Deletion: No

APN Restoration Priority: 4
Bearer Id: 5 QCI: 9

show mme-service db record imsi

The output of this command now displays the APN restoration priority for each MME db record, as shown in the following sample output:

APN Config Data

Service Selection : cisco.com
Max Req Bandwidth UL : 150000000

PDN-GW Name : test
PDN-GW Realm : test.com
PDN-GW Address : 4123::30:30:2

APN Restoration Priority : 4

show session disconnect-reasons

The following disconnect reason tracks disconnects due to a P-GW restart notification:

• mme-pgw-restarted(564)
CSCum37090, CSCuo78943, CSCuo78935, CSCuq60916 - MME needs to support MME Restoration Lite

Feature Changes

MME Restoration - Standards Extension

The feature implements the Network Triggered Service Restoration (NTSR) procedures defined in 3GPP TS 23.007 Release 11 (DDN with IMSI) on the MME.

By implementing the extensions to the standard MME restoration, the robustness of the network is greatly enhanced and potential issues due to the MME downtime are mitigated.

The solution to recover from MME node failures proposed in the 3GPP standards rely on the deployment of MME pools where each pool services a coverage area. Following a MME failure, the S-GW and MSC/VLR nodes may select the same MME that used to service a UE, if it has restarted, or an alternate MME in the same pool to process Network-initiated signaling that it received in accordance with the NTSR procedures defined in 3GPP TS 23.007 Release 11.

Upon receipt of a DDN without any TAI list or other previously sent information from the S-GW after a MME failure or restart, the MME shall proceed with regular IMSI-based paging.

The MME can be configured to throttle IMSI-based DDN requests as needed to maintain adequate service performance for normal procedure processing. Refer to the network-overload-protection mme-new-connections-per-second below for more information.

MME/VLR Restoration Procedure Via Alternate MME

The MME now supports the Mobile Terminated CS service delivery via an alternate MME in MME pool feature described in 3GPP TS 23.007 Section 14.1.3 & 26 and 29.118 Release 11.

Upon receipt of a SGs Paging request from a VLR with CS restoration bit set, the MME will perform a regular IMSI-based paging procedure, in the absence of any additional context information. If the CS Restoration Indicator is set, the MME shall page the UE regardless of the value of MME-Reset indicator. The location information shall be set in accordance with the existing procedures for unknown UE with the MME-Reset indicator set to TRUE.

No special configuration is needed to enable this functionality.

ULA for Periodic TAU when VLR Inaccessible

When processing a periodic TAU request from a UE, if the MME detects that the VLR serving the UE is inaccessible, the MME now selects an alternative VLR that is in service for the UE and performs a location update for non-EPS services procedure towards the selected VLR.

The MME previously supported this functionality in case of non-periodic TAU.

Command Changes

`gtpc node-feature network-triggered-service-restoration`

This command includes the new network-triggered-service-restoration keyword to enable NTSR functionality for this EGTP service.

`configure`
context context_name

egtp-service svc_name

[ no ] gtpc node-feature network-triggered-service-restoration

end

Notes:

- When this command is issued, the MME will indicate support for the Network Triggered Service Restoration procedure in the Node Features IE.
- Upon receipt of a Downlink Data Notification (DDN) message including an IMSI, the MME will accept the request and initiate paging including the IMSI in order to force the UE to re-attach.
- IMSI-based DDN requests contain a zero TEID.
- Since the UE is not attached, the UE will be paged over the whole MME coverage area.
- A different MME may be selected by the eNodeB to service the attach request. Since the MME that serviced the DDN will not be aware that the UE has responded with the attach request, it will stop paging upon a timeout.
- A new disconnect-reason counter has been added: ue-ctxt-normal-dei-ntsr-ddn. This is incremented when UE contexts created to handle NTSR DDN's are destroyed when the UE re-attaches.

network-overload-protection mme-new-connections-per-second

In the event of an MME failure, the surviving MME in the pool may receive a very large number of IMSI requests, which may overwhelm the IMSI Manager. To avoid congestion, the IMSI Manager can throttle the IMSI-based DDN requests it receives if the configurable rate is exceeded, as specified using this command.

This command includes the new ddn { drop | reject-with-cause { unable-to-page-ue | context-not-found } } keywords to drop or reject IMSI-based DDN requests as needed to maintain adequate service performance for normal procedure processing.

Also included is the ability to configure the default cause code to be sent in the DDN Ack in case the IMSI Manager cannot send the DDN to a Session Manager.

configure

    network-overload-protection mme-new-connections-per-second #_new_connections action
    attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } tau { drop | reject-with-emm-cause { congestion | network-failure | no-sec-ctxt-in-nw | no-suitable-cell-in-tracking-area } fwd-reloc { drop | reject } ddn { drop | reject-with-cause { unable-to-page-ue | context-not-found } } } } [ queue-size ] [ wait-time wait_time ]

    default network-overload-protection mme-new-connections-per-second

end

Performance Indicator Changes

System Schema
A new disconnect-reason bulk statistic has been added to the System schema. The following counter is incremented when UE contexts created to handle NTSR DDNs are destroyed when the UE re-attaches.

- disc-reason-587

**show session disconnect-reasons verbose**

A new session disconnect-reason counter has been added to track the number of times UE contexts created to handle NTSR DDN's are destroyed when the UE re-attaches.

- ue-ctxt-normal-del-ntsr-ddn(587)

### CSCum37443, CSCum67205 - MTC Support : Subscribed periodic TAU times

#### Feature Changes

### Subcribed Periodic TAU Timer

**Important:** Correction in 17.2 for this content. The extended-t3412 timer was incorrectly documented as the extended-3412 timer - this error has been corrected in the text below in the 17.2 publication cycle.

This feature helps the MME to reduce network load from periodic TAU signaling and to increase the time until the UE detects a potential need for changing the RAT or PLMN.

The feature enables the Operator to configure longer values for the periodic TAU timer and Mobile Reachable timer using new commands on the MME.

A new configuration is supported under the MME Service to define an EMM extended-t3412 timer value in seconds. Refer to the Command Changes section below for more information.

The MME must include the “MS network feature support” IE in the Attach Request/TAU Request. This IE indicates to the MME that the UE supports the extended periodic timer T3412, in which case the MME sends the extended-t3412 IE (T3412_E) in the attach/TAU response. The MME will not forward the extended-t3412 timer value to any UE which has not indicated that it supports this extended-t3412 timer.

The MME supports storing the Subscribed-Periodic-RAU-TAU-Timer value if received as part of subscription data, and deleting this stored value if the corresponding withdrawal flag is received in the DSR command.

For homers, the MME will send the extended-t3412 IE value as received in Subscribed-Periodic-RAU-TAU-Timer IE in subscription data.

For roamers, the MME takes the presence of Subscribed-Periodic-RAU-TAU-Timer IE in subscription data as an indication and shall send the extended-t3412 IE with the value from the local configuration.

The MME adjusts the configured mobile reachability timer value if the subscribed extended-t3412 timer value received from HSS is greater than the sum of the mobile reachability timer + implicit detach timer such that the extended-t3412 timer value becomes 10% less than the mobile reachability timer + implicit detach timer.

Refer to 3GPP TS 23.401 Section 4.3.17.3 (Version 10.4.0) & 29.272 for more details.

**Command Changes**

emm
This command now includes new keywords to configure the t3412-extended timeout values.

```
configure
  context  context_name
    mme-service  mme_svc_name
      [ default ]  emm  
        [ t3412-extended-timeout  t3412_ext_dur ]
  end
```

Notes:
- **t3412-extended-timeout**: Extended periodic TAU timer sends to UE. Range: 0-1116000 seconds (0-18600 minutes). Default: 3600 seconds (60 minutes).

### Performance Indicator Changes

**show mme-service all**

The following highlighted field has been added to show the configuration of the extended t3412 timer for the MME service.

- T3412 Extended Timeout

**show mme-service db record imsi**

The following highlighted field has been added to show the configuration of the extended t3412 timer.

- Subscribed Periodic RAU TAU Timer Value

### CSCum37475 - MTC Support : Reject causes with MM & SM back-off time

### Feature Changes

**Support for Reject Causes with MM and SM Back Off Timers**

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Under congestion, the MME can now assign EMM or ESM back-off timer to the UEs and request the UEs not to access the network for a given period of time.

Refer to 3GPP TS 23.401 Section 4.3.7.4.2.4 (Version 10.4.0) for more details.

**EMM T3346 Timer**

The MME now allows configuration of the T3346 back-off timer value. EMM timer value. The default value of this timer will be set to 25 minutes.

With this feature, when any EMM request rejected by MME because of congestion, the reject will have EMM cause of “congestion” (#22) and will include the back-off timer (T3346) IE. This back-off timer is chosen randomly and will be 10% below or above the configured T3346 timer value.
While storing the back-off timer expiry time, MME shall adjust the mobile reachability timer and/or implicit detach timer. This is to make sure that the sum of the mobile reachability timer + implicit detach timer is greater than the back-off timer duration.

The MME will store the DB for at least the EMM back-off timer duration even if the attach is rejected because of congestion. The MME will not start any timer for EMM back-off. Instead, back-off timer expiry time will be stored in the DB as the DB is stored for at least back-off timer duration.

If an EMM call is rejected due to congestion control for EMM, the DB created during ULA will not be cleared and the purge timer will be started for a time period 10% greater than the back-off timer duration. This is done to make sure that DB is available during back-off timer duration to reject any requests during this period and also to avoid the HSS signaling again if the UE comes back immediately after the back-off timer duration.

The MME will not reject any TAU received in EMM-CONNECTED state.

The MME will not reject any requests related to handovers as part of this feature even if EMM back-off timer is running.

The MME will drop attach requests received during congestion while EMM back-off timer is running based on configuration in congestion-action-profile. For example, if configuration is enabled to reject new call only when low priority indication is set and the UE comes without low priority indication while back off timer is running, the MME will accept the new call attempt from the UE.

The MME will not reject/drop attach requests received even if EMM back-off timer is running if the congestion gets cleared.

The MME will forward SGS paging requests received from MSC for a UE attached in MME even if back-off timer is running.

**ESM T3396 Timer**

The MME now allows configuration of the T3396 back-off timer value.

With this feature, when any ESM request is rejected because of congestion, the reject will have ESM cause “Insufficient resources” and will include a back-off timer IE (T3396). This back-off timer is chosen randomly and will be 10% below or above the configured T3396 timer value.

The MME will not start any timer for SM back-off, nor store the SM back-off timer expiry time. If an SM request is received and if congestion exists, the request would be rejected based and a new random value will be sent as the ESM back-off timer value.

The MME will reject any subsequent requests from the UE targeting to the same APN based on the presence of congestion at that time and not based on the SM back-off time previously sent to the UE.

If the ESM cause value is #26 “insufficient resources” or #27 “missing or unknown APN”, the MME will include a value for timer T3396 in the reject message. If the ESM cause value is #26 “insufficient resources” and the request message was sent by a UE accessing the network with access class 11 - 15 or if the request type in the PDN CONNECTIVITY REQUEST message was set to “emergency”, the MME will not include a value for timer T3396.

**Command Changes**

**emm**

This command now includes a new keyword to configure the t3346 timeout value.

**configure**

  **context context_name**
mme-service mme_svc_name

[ default ] emm { t3346-timeout t3346_dur } end

Notes:

- **t3346-timeout**: EMM backoff timer in seconds. Range: 0-11160 seconds (0-186 minutes). Default: 1500 seconds (25 minutes).
- If an EMM request is rejected by MME because of congestion, it shall have EMM cause as congestion (#22) and shall include back-off timer (T3346) IE. The back-off timer shall be chosen randomly and shall be 10% below or above the configured T3346 timer value.

esm

This command now includes a new keyword to configure the t3396 timeout value.

configure

context context_name

mme-service mme_svc_name

[ default ] esm { t3396-timeout t3396_dur } end

Notes:

- **t3396-timeout**: ESM backoff timer in seconds. Range: 0-1116000 seconds (0-18600 minutes). Default: 1500 seconds (25 minutes).
- If an ESM request is rejected because of congestion, the rejects shall have ESM cause #26: “Insufficient resources” and the MME will include the back-off timer IE (T3396). The back-off timer shall be chosen randomly and shall be 10% below or above the configured T3396 timer value.

Performance Indicator Changes

**show mme-service all**

The following fields have been added to show the configured values for the T3346 and T3396 timers.

- T3346 Timeout
- T3396 Timeout
CSCum68847, CSCum82648 - MME to support Network Provided Location Info (NPLI) for IMS

Feature Changes

Network Provided Location Info for IMS

Network provided Location Info (NPLI) enables the MME to send user location information (ULI) to the P-GW/S-GW (and consequently PCRF) in a number of Session Management messages. This information is required for Lawful Intercept (LI), VoLTE, aids in charging in the IMS domain.

In this release, the MME supports the PCC-EPC based framework, defined in 3GPP TR 23.842 section 6.4, which allows the P-CSCF to request the user location through PCRF when it needs it (for example, at voice call establishment).

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

No special configuration is required to enable this functionality.

The MME can now report the Location of a UE through the GTPv2 messages using the NPLI IEs (ULI Info, ULI-Timestamp and the UE-Timezone). The ULI Info is now included in the following GTPv2 messages:

- Create Session Request
- Create Bearer Response
- Delete Session Request
- Delete Bearer Response
- Update Bearer Response
- Delete Bearer Command

This feature also includes:

- Support for Retrieve Location Indication in the Update Bearer Request message. For this feature, the MME does not retrieve specific location information of UE but instead uses the last stored location information.
- Support for ULI timestamp in Delete Bearer Response, Delete Session Request and Delete Bearer Command messages. (Added newly in 3GPP TS 29.274 V11.8.0)
- Support for UE Time Zone in Delete Bearer Command messages.

Note: NPLI related IEs in CSReq and DSReq messages will be sent only in case of PDN establishment, but not in case of SGW relocation.

CSCuo88872 - TAU procedure counters incremented in wrong bucket

Feature Changes

Updated Counters

Old Behavior: The counter for TAU triggered after a S10 handover were incorrectly counted under Intra MME TAU failure counters.
New Behavior: This procedure is now counted under Inter node TAU failures.

CSCup02441 - IM exit procedure's failure counter not getting populated for sctp down

Feature Changes

Updated Counters

Previous Behavior: IM exit failure counter did not get incremented when a TAU with AF fails when the SCTP connection goes down and the sctp-down policy is configured to detach-ue.

New Behavior: Now this case will be accounted for correctly.

CSCup49398 - IM_Exit_Failure counter not pegged properly

Feature Changes

Updated Counters

Previous Behavior: IM exit failure counter was not accounting for the case where Inter node TAU fails due to maximum retransmission of TAU accept.

New Behavior: If an Inter node TAU enters an IM exit procedure and fails due to maximum retransmission of TAU accept, then it will be counted as failure and will be accounted for correctly in the statistics.

CSCup54025 - S1 and SGs associations not equally distributed across mmemgr tasks

Feature Changes

Delay in Processing Traffic After Restart

Previous Behavior: After an MME reboot or an SGs service configuration change, the S1 and SGs associations were not equally distributed across available MME Manager processes. On startup, the MME was starting to allocate traffic to individual MME Manager processes before all MME Manager processes were activated.

New Behavior: The MME now waits for all MME Manager processes to become available before processing traffic.

Performance Indicator Changes

show session subsystem facility mmedemux verbose

The following counter has been added to the output of the show session subsystem facility mmedemux verbose command.
This counter tracks the number of incoming packets dropped by the MME Demux subsystem (at S1 interface, coming from eNodeB) while waiting for all MME Managers to be activated (status = UP). The MME waits to start processing traffic only after the expected number of MME Managers are UP after an MME restart.

- Total number of packets dropped (Total MME Unavail)

**CSCup82616 - Handling display of Cell Trace logs and the Cell Trace config**

**Performance Indicator Changes**

*show session trace statistics*

The highlighted field below has been added to the output of the `show session trace statistics` command. This indicates if Cell Traffic Tracing is enabled or disabled.

- Network element status:
  - MME: Enabled, **Cell-Trace Disabled**

**CSCup98586 - "show session trace statistics" not updated in SSD**

**Performance Indicator Changes**

*show support details*

The information provided by the `show session trace statistics` command is now included in the output of the `show support details` command.
Chapter 13
MVG Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from MVG in StarOS 17 software releases.
MVG Enhancements for 17.0

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *MVG 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.

---

**CSCtr17295 - [MVG-0500] - Policy-Link monitoring congestion trigger**

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

**Feature Changes**

**Congestion Management**

Congestion can happen more frequently in a cellular network than in a wired network due to various factors such as airlink interface, high RTT for wireless connections. In this release, MVG supports TCP link state monitoring and estimation of congestion level at subscriber side airlink interface. The congestion level thus estimated can be sent to CAE during the start of a video flow. Based on this information, CAE can decide to stream video appropriately optimized for the subscriber side network. If the first flow from the subscriber itself is video, that flow cannot have congestion level value. The Congestion Management feature makes use of the existing Link Monitoring feature. So to enable congestion management, link monitoring has to be enabled.

Congestion detection is based on all types of data traffic - video and non-video, and works only for TCP traffic. CLI support is provided to configure the parameters to interpret the congestion indications per TCP flow and correlate them for a subscriber to allow experimentation. Congestion sampling time and reporting frequency can also be configured. Congestion monitoring is done in the downlink direction only.

CLI support is provided to enable or disable the Congestion Management feature at either APN or subscriber.

**Command Changes**

```bash
radio-congestion

In this release, `radio-congestion` is a new keyword in the APN Configuration mode to create/configure/delete Radio Congestion policy.

configure

context context_name

apn apn_name

active-charging radio-congestion policy policy_name
```
In this release, radio-congestion is a new keyword in the Subscriber Configuration mode to create/configure/delete Radio Congestion policy.

```plaintext
configure

correlation_method
```

In this release, radio-congestion is a new command in the ACS Configuration mode to create/configure/delete Radio Congestion policy.

```plaintext
configure

correlation_method
```
This is a new command in the Radio Congestion Policy Configuration mode to configure the correlation method used to correlate multiple flows of a subscriber to calculate the congestion level of a subscriber.

```
configure

active-charging service service_name

radio-congestion policy policy_name

correlation-method { mean | optimistic | pessimistic }

default correlation-method

end

data-loss threshold

This is a new command in the Radio Congestion Policy Configuration mode to configure the acceptable data loss percentage in the network.

```
configure

active-charging service service_name

radio-congestion policy policy_name

data-loss threshold threshold_value weightage weightage_value

default data-loss

end

reporting-interval

This is a new command in the Radio Congestion Policy Configuration mode to configure the reporting interval in terms of the number of sampling intervals.

```
configure

active-charging service service_name

radio-congestion policy policy_name

reporting-interval interval_value min-samples-required num_samples

default reporting-interval

end

rtt-samples

This is a new command in the Radio Congestion Policy Configuration mode to configure the RTT (Round Trip Time) samples for base RTT.

```
configure


active-charging service service_name
radio-congestion policy policy_name
rtt-samples min_samples
default rtt-samples
end

rtt-variance
This is a new command in the Radio Congestion Policy Configuration mode to configure the RTT (Round Trip Time) variance.

configure
active-charging service service_name
radio-congestion policy policy_name
rtt-variance threshold variance_percent weightage rtt_weightage
default rtt-variance
end

sampling-interval
This is a new command in the Radio Congestion Policy Configuration mode to configure the sampling interval.

configure
active-charging service service_name
radio-congestion policy policy_name
sampling-interval sampling_interval
default sampling-interval
end

Performance Indicator Changes

show active-charging radio-congestion policy all
This is a new command in this release, and the following new counters are added to the output of this command:

- Service Name
- Radio Congestion Policy
- Sampling Interval
- Reporting Interval
- Num Of Samples Required
- Min Samples Required Per Flow
- Rtt Samples
- Data Loss
  - Threshold
  - Weightage
- Rtt Variance
  - Threshold
  - Weightage
- Congestion-level
  - Low
  - Medium
  - High
  - Extreme
- Correlation-method

**show active-charging radio-congestion policy statistics**

This is a new command in this release, and the following new counters are added to the output of this command:

- Total Bytes Analyzed
- Total Bytes Retransmitted
- Total RTT Samples Analyzed
- Link Monitoring Average RTT
- Total Reports Generated
- Total Reports Generated with Congestion Level no
- Total Reports Generated with Congestion Level low
- Total Reports Generated with Congestion Level medium
- Total Reports Generated with Congestion Level high
- Total Reports Generated with Congestion Level extreme
- Total Reports Send with Congestion Level no
- Total Reports Send with Congestion Level low
- Total Reports Send with Congestion Level medium
- Total Reports Send with Congestion Level high
- Total Reports Send with Congestion Level extreme
- Total Flows Analyzed
- Total Flows Eligible for Correlation
- Total Flows with Congestion Level No
- Total Flows with Congestion Level Low
- Total Flows with Congestion Level Medium
- Total Flows with Congestion Level High
- Total Flows with Congestion Level Extreme

**show active-charging subscribers full all**

This is a new command in this release, and the following new counters are added to the output of this command:

- Radio-Congestion Subscriber Full Stats:
  - Last Reported Congestion Level
  - Total Flows Analyzed
  - Total Flows Eligible for Correlation
- Radio-Congestion Session Last Reported Stats:
  - Total Flows Analyzed
  - Total Flows Eligible for Correlation
  - Total Flows with Congestion Level
    - No Congestion
    - Low Congestion
    - Medium Congestion
    - High Congestion
    - Extreme Congestion

**show active-charging sessions full all**

This is a new command in this release, and the following new counters are added to the output of this command:

- Radio-Congestion Session Full Stats:
  - Last Reported Congestion Level
  - Total Flows Analyzed
  - Total Flows Eligible for Correlation
- Radio-Congestion Session Last Reported Stats:
  - Total Flows Analyzed
  - Total Flows Eligible for Correlation
  - Total Flows with Congestion Level
    - No Congestion
    - Low Congestion
    - Medium Congestion
MVG Changes in Release 17

MVG Enhancements for 17.0

CSCua96416 - Video : URL stripping

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

Feature Changes

URL Stripping Feature Support

The URL Stripping feature allows the ASR5000 to strip a specific URL argument from the URL, based on ECS configuration. The `stripurl token name value` command can be configured in the ACS Charging Action Configuration mode to specify the URL token to be stripped. For example, for the following URL:

```
http://www.videoserver.com?Name1=val1&Name2=val2&Name3=val3
```

if the above CLI is used, this will strip parameter `name2` and its optional value `val2` from the above URL and give the following new URL:

```
http://www.videoserver.com?Name1=val1&Name3=val3
```

The `stripurl token` command is case-sensitive. Hence if the token name does not match, then charging action will not be applied.

Limitations of URL Stripping:

- URL stripping has a limitation in case of partial packets. In cases where the HTTP Request header is split into multiple packets, the token will not be stripped from URL while forwarding the request to the origin server. This is because ECS does not buffer the HTTP packets for rule matching and added buffering will have performance impact.
- URL stripping must have higher priority than Request-Readdressing in the rulebase. Otherwise even if the URL contains the token, Request-Readdressing will happen before token is stripped.
- URL Stripping cannot be used with Response-Readdressing feature. Once the URL is stripped and sent to the new destination, the response may contain Video. Hence if Response-Readdressing is enabled, it will be readdressed back to the CAE Server, causing loop condition.

Command Changes

`stripurl`

This is a new command to configure the token and value to be stripped from the HTTP URL.

```
configure

active-charging service service_name

charging-action charging_action_name

   stripurl token token_name [ value token_value ]

no stripurl
```
Performance Indicator Changes

ECS Schema
The following new bulk statistic is added in this release:
- strip-url-token-success

show active-charging charging-action statistics name
The following new counters are added to the output of this command:
- Strip URL:
  - Successful Token stripped
  - Total strip URL failure
  - Failure - Missing config
  - Failure - Existing flow bid
  - Failure - Token matching failed
  - Failure - Empty packet
  - Failure - Req end not found
  - Failure - Subset of big token

CSCum88267 - MVG: URL Based Readdressing

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

Feature Changes

URL Based Re-addressing Feature
In this release, URL-based Re-addressing can be enabled based on L7 matching, particularly for HTTP URLs. Re-addressing charging action can also be applied based on L3/L4 matching. CLI and Statistics support are provided for this feature. The url-readdress keyword is added to the flow action command in the ACS Charging Action Configuration Mode.

Command Changes

flow action
The url-readdress keyword is added to the flow action command in the ACS Charging Action Configuration Mode to configure the URL server to re-address for the specified charging action.

configure
active-charging service service_name

charging-action charging_action_name

flow action url-readdress server ipv4_address [ port port_number ]

no flow action
end

Performance Indicator Changes

ECS Schema

The following new bulk statistics are added in this release:
- url-flow-readdress-success
- url-flow-readdress-failure

show active-charging charging-action statistics name

The following new counters are added to the output of this command:
- URL-Readdressing:
  - Requests URL-Readdressed
  - Total Charging action hit - Req. Readdr
  - Proxy Disable Success
  - Flows connected to URL Server
- URL Readdressing Error Conditions:
  - Total connect failed to URL Server
  - URL Readdress - pipelined case
  - URL Readdress - Socket Mig. failed
  - Proxy Disable Failed

show active-charging rulebase statistics name

The following new counters are added to the output of this command:
- URL-Readdressing:
  - Requests URL-Readdressed
  - Total Charging action hit - Req. Readdr
  - Proxy Disable Success
  - Flows connected to URL Server
- URL Readdressing Error Conditions:
  - Total connect failed to URL Server
- URL Readdress - pipelined case
- URL Readdress - Socket Mig. failed
- Proxy Disable Failed
Chapter 14
NAT Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from NAT in StarOS 17 software releases.
NAT Enhancements for 17.0

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.

CSCuf30336 - fw-and-nat policy ID checkpointing to peer chassis

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

Feature Changes

Firewall-and-NAT Policy ID Checkpointing

In this release, the Firewall-and-NAT Policy ID can be used for checkpointing. In earlier releases, the “Policy-name” is checkpointed to peer-chassis. Backward compatibility must be provided to support checkpointing to peer-chassis.

CSCuh60799 - Remove memory fair usage feature

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

Feature Changes

Memory Fair Usage Feature

The Memory Fair Usage feature has been deprecated in this release and is no longer supported.

CSCum39918 - KPI for NAT Port Chunk Blocking per Sub

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

Feature Changes

NAT Port Chunk Blocking per Subscriber

Previous Behavior: In earlier releases, there was no method to find out how many packets have been dropped for a subscriber due to unavailability of NAT IP and port chunks. The current NAT Realm related KPIs only indicate the number of subscribers using maximum port chunks.
New Behavior: The new KPI will contain data to indicate how many packets have been dropped for a subscriber due to unavailability of port chunks. EDRs will be generated to track the event with IMSI and a time stamp of the event. Since there is a potential for many packets to be dropped, the number of EDRs generated will be limited to one per occurrence. Only one EDR will be generated where start of the event will be packets drop due to unavailability of port chunks and end of the event will be a configured timer value. An Alarm will also be generated if the packets drop due to port unavailability by configuring a threshold for dropped packets. If exceeded, the system will suspend creating EDRs and send out an SNMP trap to notify administrators.

The **nat pkts-drop** CLI keyword has been added in the Firewall-and-NAT Policy Configuration mode to configure the format of the EDR in which records for packets drop will be saved, and the time interval for EDR generation. Statistics, SNMP Traps and Thresholds support have also been provided in support of this feature.

Command Changes

**nat pkts-drop**

In this release, **nat pkts-drop** is a new command. This command is used to configure the EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

```
configure
  active-charging service service_name
  fw-and-nat policy policy_name
    nat pkts-drop { edr-format edr_format_name | timeout timeout_value }
    { default | no } nat pkts-drop { edr-format | timeout }
  end
attribute
In this release, the **sn-nat-no-port-packet-dropped** attribute is added to report the number of packets dropped because of no NAT IP/port.

configure
  active-charging service service_name
  edr-format format_name
    [ no ] attribute sn-nat-no-port-packet-dropped priority <priority>
  end
ip pool
In this release, **pkts-drop** is a new keyword added to this command, and displays information about packets dropped because of unavailability of NAT resources.

configure
  context context_name
NAT Changes in Release 17

ip pool pool_name [ napt-users-per-ip-address | nat-one-to-one ] nat-pkt-drop
threshold high_thresh [ clear low_thresh ]
end

show active-charging subscribers nat

In this release, pkts-drop is a new keyword added to this command, and displays information about packets dropped because of unavailability of NAT resources.

show active-charging subscribers nat { required [ nat-pkts-drop [ < | = | > | equal-to | greater-than | less-than ] pkts_drop ] | not-required }

snmp trap

In this release, two new SNMP traps are added — ThreshNATPktDrop and ThreshclearNATPktDrop.

configure

snmp trap { enable | suppress } [ ThreshNATPktDrop | ThreshclearNATPktDrop ]
end

threshold nat-pkt-drop

This is a new command in this release to configure alarm or alert thresholds for the percentage of Network Address Translation (NAT) packet drops.

configure

threshold nat-pkt-drop high_thresh [ clear low_thresh ]

default threshold nat-pkt-drop

close

threshold poll nat-pkt-drop

This is a new command in this release to configure the polling interval over which to measure the percentage of Network Address Translation (NAT) packet drops.

configure

threshold poll nat-pkt-drop interval duration

default threshold poll nat-pkt-drop interval

close

Performance Indicator Changes

show active-charging subscribers full

The output of this command is modified to include the following packet drop statistics:
Packets dropped due no NAT IP/Port:
- Total Packets Dropped
- Total Packets Since Last EDR trigger

CSCum39930 - Pilot Packet to Multiple Destinations

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

Feature Changes

Pilot Packet to Multiple Destinations

Pilot Packet is a feature which provides subscriber session information to an external element. When there is a trigger for any event in which a subscriber's IP address assignment is allocated, changed, or de-allocated, a “Pilot” packet is generated. Pilot packets are generated when:

- Non-NAT IPv4 address is allocated to a session
- Non-NAT IPv4 address is de-allocated
- NAT chunk is allocated to a session
- NAT chunk is de-allocated
- IPv6 address is allocated to a session
- IPv6 address is de-allocated

This feature is enhanced to allow Gateways to send the same Pilot Packet to up to four IP destinations/nodes. These IP destinations are IPv4 nodes. IPv6 is not required or supported. Pilot packets have to be configured in the destination context of a session.

Previous Behavior: Currently the ASR5x00 sends Pilot Packet to only a single IP destination.

New Behavior: The Pilot Packet feature will send Pilot packets to multiple applications, up to four destinations.

Command Changes

pilot-packet

This CLI command is extended to support up to four Pilot Packet destinations in the destination context. The name keyword that is new in this release, specifies the pilot packet server name.

configure
  context context_name

    pilot-packet name server_name source-ip-address src-ip destination-ip-address dst-ip1 destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

    pilot-packet name server_name source-ip-address src-ip destination-ip-address dst-ip2 destination-udp-port dst-udp-port [ dscp-marking dscp_value ]
pilot-packet name server_name source-ip-address src-ip destination-ip-address dst-ip destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

pilot-packet name server_name source-ip-address src-ip destination-ip-address dst-ip destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

end

CSCum39932 - Pilot Packet Statistics Enhancement

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

Feature Changes

Pilot Packet Statistics

Pilot Packet is a feature which provides subscriber session information to an external element. When there is a trigger for any event in which a subscriber’s IP address assignment is allocated, changed, or de-allocated, a “Pilot” packet is generated. In earlier releases, Pilot Packet statistics are tracked at the aggregate level and only through the `show session subsystem` CLI command. With this release, the statistics are available at the APN level, destination level and global level. CLI and Statistics support is provided in support of this enhancement.

Performance Indicator Changes

APN Schema

The following new bulk statistics have been added in this release:

- nat-alloc-pilot-packet-sent-per-apn
- nat-de-alloc-pilot-packet-sent-per-apn
- non-nat-alloc-pilot-packet-sent-per-apn
- non-nat-de-alloc-pilot-packet-sent-per-apn

System Schema

The following new bulk statistics have been added in this release:

- nat-alloc-pilot-packet-sent
- nat-de-alloc-pilot-packet-sent
- non-nat-alloc-pilot-packet-sent
- non-nat-de-alloc-pilot-packet-sent

show apn statistics name

The output of this command has been modified to include the following Pilot Packet statistics:

- APN Name
- NAT Alloc
• Nat De Alloc
• Non NAT Alloc
• Non NAT De Alloc
• Total Alloc
• Total De Alloc

**show pilot-packet statistics**

A new Exec mode, *show pilot-packet statistics* command is available to display the following Pilot Packet statistics:

• VPN Name
• Server name
• Total NAT Alloc Pilot-Packets Sent
• Total NAT De-alloc Pilot-Packets Sent
• Total Non NAT Alloc Pilot-Packets Sent
• Total Non NAT De-alloc Pilot-Packets Sent
• Total Alloc Pilot-Packets Sent
• Total De-alloc Pilot-Packets Sent

**show session subsystem facility sessmgr**

The output of this command has been modified to include the following Pilot Packet statistics:

• VPN Name
• Server name
• Total NAT Alloc Pilot-Packets Sent
• Total NAT De-alloc Pilot-Packets Sent
• Total Non NAT Alloc Pilot-Packets Sent
• Total Non NAT De-alloc Pilot-Packets Sent
• Total Alloc Pilot-Packets Sent
• Total De-alloc Pilot-Packets Sent

**CSCum67985 - L3/L4 NAT to interwork with Accelerated ECS**

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

**Feature Changes**

**Interworking of L3/L4 NAT with A-ECS**

In this release, NAT support for A-ECS is provided. Accelerated-ECS (A-ECS) feature speeds up the processing of certain types of flows such that packet-actions and charging applicable to packets from those flows is done in a fast...
manner. The throughput in terms of PPS (Packets Processed per Second) is improved by caching rule matching results for a flow for selected flows so as to not incur the lookup penalty for a large number of packets in that flow. The A-ECS path is capable of performing a full range of basic functions including handling charging, modification of packet headers and incrementing various counters. Accelerated ECS identifies packets that need only a small amount of processing, and performs only those necessary tasks on these packets. Only those packets that do not require DPI are allowed to enter the Accelerated path.

Layer-3/Layer-4 NAT interworks with A-ECS, so that A-ECS will capture a larger chunk of traffic at various operators that use L3/L4 NAT. This basically involves separating out the NAT and SFW functionalities, and within that, separate out L3/L4 NAT from ALG-NAT. Once that is done, the accelerated-path is modified to allow L3/L4 NAT flows, and not SFW or ALG flows. Refer to the ECS Enhancements chapter for more information.
Chapter 15
PDSN Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from PDSN in StarOS 17.0 software releases.
PDSN Enhancements for 17.1

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
- SNMP MIB Enhancements
- System and Platform Enhancements

---

CSCup93612 - PDSN support for enhanced PPP Redirection

**Feature Changes**

**New CLI to support enhanced redirection feature**

The new CLI, `enhanced-pcf-redirection` is introduced under `psdn-service` configuration to support the following enhanced PPP redirection by PDSN when:

1. Subscribers access the PDSN from a restricted PCF area, then PDSN will redirect them to a specific PDSN.
2. Subscribers handoff from restricted PCF area to unrestricted PCF area, then PDSN will terminate the session.
3. Subscribers handoff from unrestricted PCF area to restricted PCF area, then PDSN will terminate the session.
4. Subscribers handoff from restricted PCF area to another restricted PCF area, then PDSN will terminate the session.
5. If subscribers access PDSN from an unrestricted zone or if enhanced redirection feature is disabled, PDSN treats the mobile node in a normal way.

PDSN will be able to configure and recognize at least 100 PCF addresses.
Command Changes

enhanced-pcf-redirection

This command is added under pdn-service configuration to support enhanced redirection feature.

```
configure
  context context_name
  pdn-service
    [ no ] enhanced-pcf-redirection
  end
```

Notes:
- **enhanced-pcf-redirection**: This enables the enhanced PCF redirection feature.
- By default, the enhanced PCF redirection feature is disabled.

policy pcf-zone-match

This command is modified to include restricted as a new optional keyword to indicate the zone is restricted. Restricted zone is meaningful only if enhanced-pcf-redirection feature is enabled, otherwise the zone follows the default behavior.

```
configure
  context context_name
  pdn-service
    policy pcf-zone-match zone_number redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | restricted [ redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] ]
  end
```

Notes:
- **restricted**: This is an optional keyword which means the zone is restricted.

Performance Indicator Changes

show rp statistics pdn-service service_name

New statistics is added to indicate session release due to handoff restrictions.
- handoff-pcf-restriction
Chapter 16
P-GW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from P-GW in StarOS 17 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:

- P-GW Enhancements for 17.3
  - “CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure” - Added
- P-GW Enhancements for 17.0
  - “CSCum88464, CSCup56698 - Intelligent graceful PDN disconnection during maintenance-mode” - Corrected and enhanced description
P-GW Enhancements for 17.5

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 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

---

CSCuv73563 - Support for SN1-QOS-Traffic-Policy AVP received from Radius server on PGW

**Feature Changes**

**RADIUS SN1-QOS-Traffic-Policy Attribute Support on P-GW**

In order to configure rate limiting parameters for subscriber traffic on P-GW from RADIUS/AAA server, SN1-QOS-Traffic-Policy attribute will now be supported for P-GW calls in Initial Authentication and Change Of Authentication (CoA) messages in custom33 RADIUS dictionary. This existing compound RADIUS attribute was previously used by GGSN only.

The following scope of behavior is supported for P-GW:

1. SN1-QOS-Traffic-Policy attribute is supported for P-GW call.
2. Support added for this attribute in Initial Auth and CoA.
3. Only Class and Peak-Data-Rate values in SN1-QOS-Traffic-Policy attribute will be used to derive APN-AMBR data rate and QCI; the rest of the values are ignored and APN-AMBR local configuration in APN configuration will be used to determine Violate action.
4. No Gx may be enabled while this feature is being used.
5. Only Default bearer will be supported with this feature.
6. Multi-PDN support to the same APN is not supported.
7. ICSR and Session Recovery are supported.

Possible scenarios where SN1-QOS-Traffic-Policy attribute would be sent by AAA server:

1. SN1-QOS-Traffic-Policy attribute would be sent by AAA server in Initial Authentication Message for P-GW call:
   - Create Session request received.
   - Access-request sent to AAA server for authentication.
   - Received Access-response with SN1-QOS-Traffic-Policy (Class, Direction, Peak-Data-Rate) from AAA server.
   - Peak-Data-Rate would be applied to common_apn_ambr data structure and rate limiting applies on apn_ambr.
   - Create Session Response would be sent to access side with the radius-returned values.

   **Important:** Violate action should be configured under APN for both uplink and downlink traffic.

2. SN1-QOS-Traffic-Policy attribute would be sent by AAA server in Change of Authentication Message for P-GW call:
   - CoA sent with SN1-QOS-Traffic-Policy (Direction, Peak-Data-Rate).
   - Peak-Data-Rate values would be applied to clp->apn_ambr data structure with the radius-returned values.
   - The radius-returned values would not be communicated to access side.

   **Important:** Violate action should be configured under APN for both uplink and downlink traffic.

Only Class and Peak-Data-Rate values in SN1-QOS-Traffic-Policy attribute will be used to derive APN-AMBR data rate and QCI; the rest of the values are ignored and APN-AMBR local configuration in APN configuration will be used to determine Violate action. QCI is used to only apply peak data rate for the bearer; Radius-return QCI would not be applied to change QCI of the bearer.

The grouped attribute SN1-QOS-Traffic-Policy (in custom33 RADIUS dictionary) is used to send the QOS parameters in Authentication response. Contents of this attribute are:

SN1-QOS-Traffic-Policy
{
  Direction
  Class
  Peak-Data-Rate
}
Command Changes

apn-ambr

Use this existing command to configure rate limiting actions under APN for both uplink and downlink traffic.

```
configure

    context context_name

    apn apn_name

    apn-ambr rate-limit direction { downlink | uplink } [ burst-size { auto-readjust
duration seconds } | violate-action { drop | lower-ip-precedence | transmit } ]

    { default | no } apn-ambr rate-limit direction { downlink | uplink }

end
```

Notes:
- See the Command Line Interface Reference for a detailed description of the apn-ambr command.

aaa group

Use this existing command to enable applying the AVP values received in CoA.

```
configure

    context context_name

    aaa group group_name

end
```

Notes:
- See the Command Line Interface Reference for a detailed description of the aaa group command.

radius change-authorize-nas-ip

Use this existing command to enable listening for CoA messages from the RADIUS server.

```
configure

    context context_name

    radius change-authorize-nas-ip ip_address key value no-nas-identification-check

end
```

Notes:
- This command configures the NAS IP address on which the context will listen for COA messages. If the NAS IP address is not defined with this command, any COA messages from the RADIUS server are returned with a Destination Unreachable error.
See the Command Line Interface Reference for a detailed description of the `radius change-authorize-nas-ip` command.

CSCzn47162 - Routing Behind the Mobile Station on an APN

Feature Changes

Routing Behind the Mobile Station on an APN

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDP context which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the “mobile router.” If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDP context.

Command Changes

network-behind-mobile

The following `network-behind-mobile` has been added to enable or disable a Network behind Mobile Station for APN.

```
config

context context_name

apn apn_name

network-behind-mobile { max-addresses-behind-mobile max_addrs | max-subnets max_subnets }

{ default | no } network-behind-mobile

end
```

Notes:

- **default**
  
  Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

- **no**
  
  Disables the network behind mobile station functionality on the APN.

- **max-addresses-behind-mobile max_addrs**
  
  Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

- **max-subnets max_subnets**
Specifies the maximum number of subnets that can be enabled for a call in the APN. 

`max_subnets` must be an integer from 1 through 16.

Default: 10

**Performance Indicator Changes**

**show apn name <apn_name>**

The following fields have been added to this command.

- Network Behind Mobile Station: Enabled
- Maximum subnets behind Mobile station: 10
- Maximum Addresses Behind Mobile Station: 16777214
P-GW Enhancements for 17.4

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 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**

---

**CSCus82761 - Charging Id in GTPv2 S2b/S2a**

**Feature Changes**

**Charging ID sent in Create-Session-Response and Create-Bearer-Request**

Introduced charging ID IE in S2b/S2a-GTPv2 as part of CDR support for 3GPP compliance for Wifi.

**Previous Behavior:** The P-GW did not send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.

**New Behavior:** The P-GW will send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.
CSCut53373, CSCuu63751, CSCuu64308 - PGW initiates UBR while no QoS change

Feature Changes

UBR Suppression Feature

**Important:** The Update Bearer Request (UBR) Suppression feature is a license controlled feature. Please contact your Cisco sales representative for more information.

As the bit rate is expressed in bps on Gx and kbps on GTP, P-GW does a round-off to convert a Gx request into a GTP request. When P-GW receives RAR from PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in Kbps) is already set for the bearer. The UBR suppression feature enables P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

A new CLI has been added to the P-GW service configuration to enable UBR suppression. Once the CLI is configured, P-GW suppresses the UBR if the bit rate is the same after the round-off.

When UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

**Previous Behavior:** UBR was not suppressed, even if bit rates were the same.

**New Behavior:** If license is enabled and CLI is configured for UBR suppression, then UBR is suppressed if bit rates in kbps are the same after round-off and all other parameters, such as QCI, ARP, and TFT, that might trigger UBR are also unchanged.

Command Changes

**suppress-ubr no-bitrate-change**

A new CLI command has been introduced to control UBR suppression. This CLI is disabled by default; UBR is triggered, even if the Gx and GTP bit rates in kbps are the same after round-off.

```
configure

context context_name

pgw-service <pgw-service-name>

    egtp suppress-ubr no-bitrate-change

    no egtp suppress-ubr no-bitrate-change

end
```

Notes:

- **suppress-ubr:** Enables or disables suppression of UBR when there is no change in PCRF authorized bit rates. By default, the UBR suppression feature is disabled.
• **no-bitrate-change**: Configures UBR suppression when there is no change in bit rates after bps to kbps round-off. By default, this keyword is disabled.

• **no**: Disables UBR suppression. UBR is triggered, even if the Gx and GTP bit rates in kbps are the same after round-off.

**Performance Indicator Changes**

**show configuration**

The following field has been added to the output of this command under the P-GW service:

- `egtp suppress-ubr no-bitrate-change`

**show configuration verbose**

The following field has been added to the output of this command under the P-GW service:

- `no egtp suppress-ubr no-bitrate-change`

**show pgw-service name <pgw-service-name >**

The following field has been added to the output of this command under the P-GW service:

- `EGTP Suppress Update Bearer Request (no bitrate change): Enabled / Disabled`

**CSCus03709 - Command <b>clear subs</b> with grep does not prompt for confirm**

**Feature Changes**

**Grep Option Removed from clear subscriber Command**

**Previous Behavior:** Earlier, the command `clear subscriber` asked for a confirmation before clearing the subscribers when `no autoconfirm` was set. Also, when `clear subscriber` command was given in conjunction with a `, the command cleared the subscribers without asking for confirmation, even when `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 `clear subscriber` now always ask for a confirmation message when `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 `no autoconfirm` is set.
P-GW Enhancements for 17.3

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

**CSCus12585 - Bulkstat counter sessstat-bearrel-ded often zero when rel-dedbear is not**

**Feature Changes**

**Bulkstat Counter sessstat-bearrel Incremented for All Disconnect Reasons.**

Added code to count all the disconnects on a dedicated bearer.

**Previous Behavior:** `sessstat-bearrel` was only used to increment for the following disconnect reasons: `admin_disconnect`, `gtpu_err_ind`, `remote_disconnect`, `srvcc_ps_to_cs_handover`, `inactivity_timeout`, `session_timeout`, `session_setup_timeout`, and `emergency_inactivity_timeout`.

**New Behavior:** Now, `sessstat-bearrel` will be incremented for all dedicated bearer release for all disconnect reasons. A few of the disconnect reasons are: `gx-policy-disconnect`, `path failure`, and so on.
CSCus80195 - T3/N3 timer with 100 ms granularity

Feature Changes

Granularity Added to T3/N3 Timer

This enhancement introduces the ability to configure T3/N3 timer in millisecond (ms) granularity. This helps reduce the possibility of “packet collision” between P-GW/S-GW/MME and so on by being able to configure a nearly identical second value separated by a few 100 ms.

The new T3 value is configured in 100 ms granularity, starting at 1000 ms (1 second). The previous range for T3 value was between 1 to 20 seconds, with a default of 5 seconds. The range for the new T3 value is 1000-20000 ms, with numbers going up by 100 ms.

Previous Behavior: The CLI command `retransmission-timeout` was operational. Timer granularity for T3/N3 timer was in seconds.

New Behavior: The CLI command `retransmission-timeout` is now obsolete; this CLI has been replaced by the CLI command `retransmission-timeout-ms`. Timer granularity for T3/N3 has been changed from seconds granularity to 100 milliseconds.

Command Changes

```
retransmission-timeout-ms
```

This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer.

The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure
  context context_name
    ggsn-service service_name
      retransmission-timeout-ms retransmit_time
      default retransmission-timeout-ms
    end
```

Notes:

- `default`: Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.
- `retransmit_time`: Specifies the amount of time, in milliseconds, that must pass without an SGSN response before the GGSN service retransmits GTP control packets. Must be an integer from 1000 to 20000, with increments of 100.
  Default: 5000

```
retransmission-timeout-ms
```
This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer. The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure

context context_name
    egtp-service service_name
        gtpc retransmission-timeout-ms retransmit_time
    default gtpc retransmission-timeout-ms
end
```

**Notes:**
- **default:** Configures the default control packet retransmission timeout in GTP.
- **retransmit_time:** Specifies the GTP control packet retransmission timeout in milliseconds. Must be an integer from 1000 to 20000, with increments of 100.
  Default: 5000

**retransmission-timeout-ms**

This new CLI command introduces 100 millisecond (ms) timer granularity for the T3 timer. The range for the T3 value was 1 to 20 seconds, with a default value of 5 seconds. The new range is 1000 to 20000 ms, with increments of 100 ms.

```
configure

peer-profile service-type [ ggsn-access | pgw-access | sgw-access | sgw-network ] name peer_profile_name
    gtpc-service service_name
        gtpc retransmission-timeout-ms retransmit_time
    default gtpc retransmission-timeout-ms
end
```

**Notes:**
- **default:** Configures the default control packet retransmission timeout in GTP.
- **retransmit_time:** Specifies the GTP control packet retransmission timeout in milliseconds. Must be an integer from 1000 to 20000, with increments of 100.
  Default: 5000
CSCus82761 - Charging Id in GTPv2 S2b/S2a

Feature Changes

Charging ID Sent in Create-Session-Response and Create-Bearer-Request

Introduced charging ID IE in S2b/S2a-GTPv2 as part of CDR support for 3GPP compliance for WiFi.

**Previous Behavior:** The P-GW did not send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.

**New Behavior:** The P-GW will send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.

CSCut22844 - SegFault: libc.so.6/__strlen_sse2_bsf()

Feature Changes

Behavior Change in APN Removal

**Previous Behavior:** Earlier, while removing APN using the `no apn <apn_name>` command, all active and inactive subscribers would get deleted with warning.

**New Behavior:** Now, active or inactive subscribers are not deleted when you try to remove an APN using the command `no apn <apn_name>`. APN removal is not allowed if active or inactive subscribers are present and an error message is displayed.

**Customer Impact:** APN removal is not allowed if already some active or inactive subscribers are present for the APN.

Command Changes

```
no apn
```

Modification has been made to the command `no apn`, earlier all active/inactive subscribers were deleted with a warning message. With the new modification, the APN removal is not allowed and the following error message is displayed:

“Error: Clear all subscribers connected to the APN <apn_name> before removing it from configuration”.

```
cfg
    context context_name
    no apn apn_name
end
```

**Notes:**
If `-noconfirm` keyword was used with `no apn <apn_name>`, earlier active or inactive subscribers were deleted without prompting any warning or confirmation. With new modification, the APN removal is not allowed and the following error message is displayed:

“Error: Clear all subscribers connected to the APN <apn_name> before removing it from configuration”.

CSCut38800 - PGW sends CCR-U with RESOURCES_LIMITATION for VoLTE calls in 17.1 build.

Feature Changes

Handling of Collision of GnGp (LTE to GnGP GGSN) Handoff with Ongoing CBReq or UBReq Transaction

**Previous Behavior:** When P-GW initiates CBReq for bearer creation due to RAR from PCRF, and handoff to GGSN happens before CBRsp has come from S-GW, the transaction will not be cleaned from PGW. The call relocates back to PGW & now if RAR is received for the same bearer creation (same Qos/ARP) then P-GW ignores RAR and do not initiate CBReq for the bearer creation.

**New Behavior:** P-GW aborts all pending transactions while performing handoff to GGSN. All further RAR for the same Qos/ARP RAR requests are handled when call move back to PGW.

**Customer Impact:** VoLTE calls will not be impacted if the GnGp handover happens when CBReq or UBReq was in process in the LTE access.

CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure

Feature Changes

Control of GTP Cause Being Sent in Create Session Response

**Previous Behavior:** If during initial call setup at P-GW (Create Session Request) PCRF rejects the call with 5xxx cause code, P-GW sends GTP cause “User Authentication Failure” in Create Session Response message.

In 16.x and earlier StarOS releases, P-GW rejected the call with GTP cause “No Resources Available”. The behavior above was implemented as an enhancement.

**New Behavior:** When Create Session Request message arrives at P-GW, CCR-I is sent to PCRF and PCRF rejects calls with 5xxx cause code in CCA-I. In this case, Create Session Response is sent with failure indicated by GTP cause code. A new CLI command has been introduced to control which GTP cause code is sent, “No Resources Available” or “User Authentication Failed”, in Create Session Response message for this scenario. By default, “No Resources Available” is sent for this case; however, enabling the new command sends “User Authentication Failed” cause code in Create Session Response.

Command Changes

```
map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail
```

This is a new command that maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message.

```
configure

context context_name
```
pgw-service  pgw_service_name

[ default | no ] map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail

end

Notes:

- **default | no**: Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.
P-GW Enhancements for 17.2

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.

---

**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

---

**CSCur22641 - QoS enforcement issue using GxR10 during IRAT on R15.0 PGW**

**Feature Changes**

**QoS Enforcement Issue using GxR10 During IRAT**

Previously, during GnGp handoff the SGSN was incapable of communicating the last authorized ARP (PV and PC) values to the MME. In this case, the MME tried to query the P-GW to get the last authorized ARP. Neither the PCRF nor the P-GW replied with the last authorized value to the MME. Therefore, the MME applied the subscribed ARP values from the HSS which was different from the last authorized value. This cause the P-GW and the MME to go out of sync on ARP.

**Previous Behavior:** Previously, the UB request for MBC contained the last negotiated APN AMBR after GnGp handoff if the PCRF was not reachable. The UB request for MBC contained the last authorized APN AMBR if the PCRF provided an APN AMBR after GnGp. The default EPS bearer QoS was not addressed as part of the `egtp modify-bearer-cmd-negotiate-qos` CLI command.
New Behavior: The UB request for MBC contains the last negotiated APN AMBR after GnGp if the PCRF is not reachable and the UB request for MBC contains the last authorized APN AMBR if the PCRF provides an APN AMBR after GnGp. This change sends the last authorized DEBQ in UB request if:

- the UB request is triggered by MBC
- the MBC requested a DEBQ
- the requested DEBQ is different than the current authorized value
- the PCRF is configured and if does not provide DEBQ
- `egtp modify-bearer-cmd-negotiate-qos` is configured under P-GW service
P-GW Enhancements for 17.1

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.

---

**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

---

**CSCug80236 - Cause code mapping difference in LTE/UMTS authorization-reject 5003**

**Feature Changes**

**Cause Code Mapping Difference in LTE/UMTS authorization-reject 5003**

For UMTS, Gx 5003 is mapped to GTP-USER-AUTHENTICATION-FAILED. For LTE, Gx 5003 is mapped to NO-RESOURCES.

**Previous Behavior:** For UMTS, Gx 5003 is mapped to GTP-USER-AUTHENTICATION-FAILED; however, for LTE Gx 5003 is mapped to NO-RESOURCES. When a call is rejected with the reason IMS-AUTH-FAILED, the reject reason from the session manager to the P-GW is actually set to SNX_REJECT_REASON_NONE. Since the reason is incorrectly set in the SMGR-APP, the driver sets the EGTP cause to NO-RESOURCES. The reason from SMGR-APP should have been set to SNX_REJECT_AUTH_FAILED for IMS-AUTH-FAILED case.
**New Behavior:** Added case for handling the disconnect reason IMS.AUTHORISATION_FAILED case in SM-APP. As a result, EGTP_CREATE_SESSION_RESPONSE is received with EGTP_CAUSE_USER_AUTHENTICATION_FAILED in such a case.

### CSCug96117 - Alternate Care-of Address Mobility Option support on PGW/LMA

#### Feature Changes

**Alternate Care-of Address Mobility Option Support**

Proxy Mobile IPv6 is a network-based mobility management protocol. The mobility entities involved in the Proxy Mobile IPv6 protocol, the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA), setup tunnels dynamically to manage mobility for a mobile node within the Proxy Mobile IPv6 domain. This document describes an extension to the Proxy Mobile IPv6 protocol to register an IPv4 or IPv6 data plane address that is different from the Proxy Care-of Address with the LMA. This allows separation of control and data plane.

Some of the deployments of Proxy Mobile IPv6 separated the control and data plane end points for Mobile Access Gateway. There will be a separate IP address for the entity that sends and received the Proxy Mobile IPv6 signaling messages. Similarly, there will be a separate IP address for the entity that encapsulates and decapsulates the data traffic to and from the mobile node.

In order to allow the separation of the control and data plane, the address of the data plane traffic endpoint needs to be sent in a separate extension to register two IP addresses with the LMA. The IP address used for the signaling messages will continue to be called the Proxy Care-of-Address. A separate IP address for the data plane is carried in the Proxy Binding Update to indicate the tunnel end point for the data traffic.

The extension Alternate Care-of-Address Mobility Option defined in RFC 6275 should be used. When using IPv6 transport and IPv4 transport, Alternate IPv4 Care of Address Mobility Option defined in RFC 6463 should be used.

Normally, a binding update specifies the desired care-of-address in the source address field of the IPv6 header. However, in some cases such as when the mobile node wishes to indicate a Care-of-Address that it cannot use as a topologically correct source address or when the used security mechanism does not protect the IPv6 header it is not possible.

The Alternate Care-of-Address option is for this type of situation. This option is valid only in binding update. The Alternate Care-of Address field contains an address to use as the care-of-address for binding rather than using the source address of the packet as the care-of-address.

A MAG may include the Alternate IPv4 Care-of-Address option in a PBU. An LMA that receives and implements the Alternate IPv4 Care-of-Address option must echo the option back to the MAG in a reply PBA.

With this feature, P-GW/LMA will support data-plane address endpoint separation with alternate care-of-address mobility option defined in RFC 6275 and RFC 6463 for IPv6 and IPv4 transport respectively.

#### Command Changes

**alt-coa-allowed**

This new command allows Alternate Care-of-address support to be added at LMA to separate signaling and control plane traffic.

configure

    context context_name
lma-service service_name

[ default | no ] alt-coa-allowed
end

Notes:

- By default, alternate Care-of-Address is not supported.
- The support of the extensions and functionality is defined in RFC 6275 and RFC 6463 for IPv6 and IPv4 transport respectively.

Performance Indicator Changes

show configuration

The following field has been added to display the Alternate Care-of Address support in configuration:

- alt-coa-allowed

test command

show lma-service name service_name

The following field has been added to display the Alternate Care-of Address support at LMA service:

- Alt-Coa

show subscribers lma-only full

The following field has been added to display the Alternate Care-of Address support for subscribers at LMA service:

- Alt-Care of Address

show subscribers pgw-only full

The following field has been added to display the Alternate Care-of Address support for subscribers on P-GW:

- Alt-Care of Address

CSCuh06473, CSCuq23971 - Cause IE enhancement for Delete Bearer Request

Feature Changes

Cause IE enhancement for Delete Bearer Request

Cause value in the Delete Bearer Request has been limited. The behavior impacted by this feature is:

- Delete Bearer Request/Delete PDP Context due to idle-timer/session-timer expiration
- Delete Bearer Request due to bearer inactivity of default bearer
- Delete PDP Context due to bearer inactivity of the last PDP context of PDN connection
- Delete Bearer Request/Delete PDP Context triggered by clear subscriber CLI command
Configuration has been added to set cause values and cause inclusion in the following scenarios:

- CLI-based trigger to disconnect
- per APN when P-GW initiated disconnection for above mentioned timer expiry

**Important:** Cause IE Enhancement for Delete Bearer Request is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Previous Behavior:**
1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, its cause-IE is not configurable.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, its cause-IE is not configurable.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, its cause-IE is not configurable.

**New Behavior:**
1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, the cause-IE to be used may optionally be specified by the operator in CLI. The CLI also allows the operator not to include cause-IE.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, the cause-IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, the cause IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.

**Customer Impact:** Cause-Code during PDN connection teardown may be modified.

**Important:** This feature allows operator to override existing behavior. Such overridden behavior may not be compliant with standards.

**Command Changes**

`clear subscribers`

When subscribers are deleted, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword `del-cause` is optional and can be combined with existing options to modify “Cause-IE” behavior.

```
clear subscribers all [ del-cause { none | reactiv-req } ] [ verbose ] [ -noconfirm ]
clear subscribers apn apn_name [ del-cause { none | reactiv-req } ] [ verbose ] [ -noconfirm ]
```

**Notes:**
- `del-cause`: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests generated for default bearer.
- **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- The new behavior for “Cause-IE” will be effective only if the `clear subscribers` CLI results in the sending of a Delete Bearer Request for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for “Cause-IE” given in this CLI shall override the cause-code set by existing features.

### timeout

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword `del-cause` is optional and can be combined with existing options to modify “Cause-IE” behavior.

```plaintext
configure
  context context_name
    apn apn_name
      timeout absolute time [ del-cause { none | reactiv-req } ]
      { default | no } timeout absolute del-cause
    end

Notes:
- `del-cause`: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- `none`: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- `reactiv-req`: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- By default, the `del-cause` option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

### timeout bearer-inactivity

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword `del-cause` is optional and can be combined with existing options to modify “Cause-IE” behavior.

```plaintext
configure
  context context_name
    apn apn_name
      timeout bearer-inactivity del-cause { none | reactiv-req }
      { default | no } timeout bearer-inactivity del-cause
    end
```
Notes:

- **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- By default, the **del-cause** option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**timeout idle**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword **del-cause** is optional and can be combined with existing options to modify “Cause-IE” behavior.

**configure**

```
context context_name

apn apn_name

  timeout idle idle_dur [ del-cause { none | reactiv-req } ]

  { default | no } timeout idle del-cause

end
```

Notes:

- **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.
- **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.
- **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- By default, the **del-cause** option is not defined and existing behavior is retained.
- The new behavior is applicable only if Delete Bearer Request is sent for Default Bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.
- The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**CSCuI30091 - PGW fails to resolve P-CSCF address**

**Feature Changes**

**P-GW Support for P-CSCF Discovery During Handoff**

**Previous Behavior**: A specific customer relied on the P-GW to resolve the P-CSCF address over DNS and include the PCO Options if the UE requests the P-CSCF address. During certain external or internal DNS failures, the P-GW may
not have resolved the P-CSCF address. In this case, the P-GW did not include the P-CSCF in the PCO Options and the request was still successful. This caused issues to VoLTE devices and a rescue attempt occurred with some other technology like eHRPD or LTE. In such cases, the P-GW would not re-trying the P-CSCF resolution and rather continue with the empty P-CSCF request.

**New Behavior:** If the P-CSCF address information is not available at the time of handoff, then the P-GW will attempt to re-discover the P-CSCF address and include it as part of the handoff message exchange.

### CSCum51840 - eHRPD support: PGW fails to resolve P-CSCF address

**Feature Changes**

**P-GW Failed to Resolved P-CSCF Address**

During certain external or internal DNS failures the P-GW may not have been able to resolve the P-CSCF address during new call setup. In this scenario, the P-GW did not include the P-CSCF in the PCO Options and the request was still successful.

During LTE2eHRPD Handoff if local P-CSCF addresses were not present, then the P-GW would not reattempt the P-CSCF resolution and continue with the empty P-CSCF request.

**Previous Behavior:** During LTE2eHRPD Handoff if local P-CSCF addresses were not present, then the P-GW would not reattempt the P-CSCF resolution and continue with the empty P-CSCF request.

**New Behavior:** During LTE2eHRPD handoff if local P-CSCF addresses were not present, then the PGW will attempt to resolve the P-CSCF address and include it in PBA.

### CSCum51844 - eHRPD Additional support for PCSCF Discovery

**Feature Changes**

**eHRPD Additional Support for P-CSCF Discovery**

**Previous Behavior:** Previously, the order of resolution of P-CSCF address was:

1. DNS resolution: (FQDN fetched from S6b)
2. P-CSCF Addresses via APN configuration
3. P-CSCF Addresses that were received from the IMSA configured locally under imsa-service

**New Behavior:** Modified P-CSCF discovery logic. The order of resolution of P-CSCF address is:

1. DNS resolution: (FQDN fetched from S6b or APN config)
2. PCSCF Addresses that are received from the IMSA (IMSA based P-CSCF end to end support for V4 and V6)
3. P-CSCF Addresses via APN configuration
CSCuo51256 - Filter-ID Invalid name should not overwrite default ACL configuration

Feature Changes

Modification in ACL's Selection During Call Setup

**Previous Behavior:** In GGSN/P-GW Context, an APN was configured with certain ACLs via the `ip access-group` command. During the User Context activation, in the Access-Accept from RADIUS the Attribute “Filter-Id” was returned, but the Filter-Id Attribute-Value was not pre-configured on the ASR 5000. Therefore, it was considered an “invalid” value for the Filter-Id. Then, the ACL configuration was not configured, which meant that the locally configured ACL name from the APN Template was also not being applied.

**New Behavior:** In the case of an “invalid Filter-Id” attribute value in a RADIUS Access-Accept message, the behavior should be the same as in the case of a “missing Filter-ID” AVP. Therefore, during Context Activation in the RADIUS Access-Accept, a Filter-Id Attribute is returned. However, the Value of the Filter-Id attribute is considered as invalid. Then, if any ACL value is locally configured in the APN, it should be taken and applied in the context.

**Customer Impact:** There will be no loss of CDR and missing charging information when incorrect ACL is sent via RADIUS.

Command Changes

```
ip access-group
```

The new keyword `fallback-enabled` helps to prevent loss of CDR and missing charging information when incorrect ACL is sent via RADIUS.

```
configure
  context context_name
    apn apn_name
      ip access-group acl_group_name [ in | out ] [ fallback-enabled ]
  end
```

Notes:
- `fallback-enabled`: When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.
- By default, ACL fallback is disabled.
- Run command without `fallback-enabled` option to disable ACL fallback for a previously configured ACL applied to a particular APN.

```
ipv6 access-group
```

The new keyword `fallback-enabled` helps to prevent loss of CDR and missing charging information when incorrect ACL is sent via RADIUS.
configure

context context_name

apn apn_name

ipv6 access-group group_name [ in | out ] [ fallback-enabled ]

end

Notes:

- **fallback-enabled**: When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.
- By default, ACL fallback is disabled.
- Run command without `fallback-enabled` option to disable ACL fallback for a previously configured ACL applied to a particular APN.

**Performance Indicator Changes**

show apn name apn_name

The following fields have been added to show whether the ACL fallback option is enabled or disabled:

- Ipv4 Input ACL Fallback
- Ipv4 Output ACL Fallback
- Ipv6 Input ACL Fallback
- Ipv6 Output ACL Fallback

**CSCuo92945 - 110 cause when temp fail not configured is treating as success**

**Feature Changes**

**Call Flow and Bearer Creation**

**Previous Behavior:** In pgw-service, if `egtp cause-code temp-fail timeout` was not enabled and a 110 cause code `EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS` was received in the create bearer response message, then the P-GW created a new dedicated bearer.

**New Behavior:** In pgw-service, if `egtp cause-code temp-fail timeout` is not enabled and a 110 cause code `EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS` is received in the create bearer response message, then the P-GW does not create a new bearer. Instead, it sends a `RESOURCE_ALLOCATION_FAILURE` message to the PCRF.
CSCup44058 - Acct msg shows both v4 and v6 addr even if v4 is denied for static alloc

Feature Changes

Correct IP Address and PDN Type sent in RADIUS Accounting.

Previous Behavior: If there was a UE request for dual PDP type and either IPv4 or IPv6 PDP type failed, then the RADIUS account would have a failed IP address/PDP type.

New Behavior: If there is a UE request for dual PDP type and either IPv4/IPv6 address allocation fails, a new PDP type and correct IP address is sent in RADIUS accounting.”

CSCup44635 - SM support for CSCul22770, SFR - PSP algorithm modification

Feature Changes

Modification in Bandwidth Policy Selection During Call Setup

Previous Behavior: A single bandwidth policy was being sent from the session manager to ECS for validation. When an invalid bandwidth policy was received from RADIUS, the call was being terminated.

New Behavior: Primary and fallback policies are sent from SM to ECS. When an invalid bandwidth policy is received from RADIUS, bandwidth policy from APN can be applied if it is valid and the call will remain active.

Customer Impact: This will help prevent termination of calls when an incorrect bandwidth policy is sent through RADIUS.

CSCup59406 - sesstrc task in over state during longevity/aggravator run

Feature Changes

Configuring Session Trace File Type

To address the issues caused when the sesstrc task allocates memory over the allotted limit, under a random subscriber session trace load tests on P-GW/S-GW, support for B-type XML files is introduced in addition to the A-type files already supported.

Previous Behavior: The file type was A-type XML file and the type could not be changed.

New Behavior: The CLI has been modified (see Command Changes section) to allow the operator to select the file type generated by session trace. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.
Command Changes

`session trace network-element`

The new optional `file-type` keyword enables the operator to determine which type of XML file is generated by the session trace:

```plaintext
configure

  session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw } [ file-type { a-type | b-type } ] [ collection-timer | tce-mode ]

  no session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw }

end
```

Notes:
- Default file-type is `a-type`.
- To keep the syntax simple, the optional `file-type` keyword must be entered before entering either of the other optional keywords.
- To modify the session trace network-element configuration, you must first enter the `no session trace network-element` form of the command to remove the session trace configuration.

CSCuq19244 - PGW does not initiate DNS query to resolve P-CSCF addr after ehrpd-epdg ho

Feature Changes

P-GW Did Not Initiate DNS Query to Resolved P-CSCF Address after Inter-tech Handoffs

P-GW did not initiate P-CSCF Discovery to resolved P-CSCF Address after following inter-tech handoff scenarios if P-CSCF Address information is already missing.

**Previous Behavior:** If P-CSCF address information was already missing, then the P-GW did not initiate P-CSCF Discovery to resolve the P-CSCF address after the following inter-tech handoff scenario.

- eHRPD to S2B
- LTE to S2B
- S2B to LTE
- S2A to LTE

**Important:** LTE to S2A Handoff is intentionally NOT mentioned here as P-CSCF IE is not supported for this Handoff.

**New Behavior:** If P-CSCF address information is already missing, then the P-GW initiates P-CSCF Discovery to resolve the P-CSCF address after the following inter-tech handoff scenarios.
- eHRPD to S2B
- LTE to S2B
- S2B to LTE
- S2A to LTE

**Important:** LTE to S2A Handoff is intentionally NOT mentioned here as P-CSCF IE is not supported for this Handoff.

**Important:** P-CSCF Discovery for GnGp Handoff is not supported as part of ID CSCuq19244.

**CSCuq63677 - Assertion failure at Function:**
```
sessmgr_sesstrc_allocate_clp_data()
```

**Feature Changes**

**Improper Removal for Session Tracer**

**Previous Behavior:** SAEGW removal for session trace was not handled properly. Random session trace was selecting collapsed calls (S-GW/P-GW or SAEGW) which lead to a failure.

**New Behavior:** Removed all types of session trace (management, random, signaling) from the code for S-GW of SAEGW. Now, SAEGW collapsed/collocated calls will only get traced at the P-GW for all types of session trace.

**CSCuq89887 - pgw sends ICMP MTU too big when user pkt size is greater than 1500**

**Feature Changes**

**Uplink MTU Size Restriction Removed**

**Previous Behavior:** The uplink MTU was restricted to a maximum of 1,500 Bytes.

**New Behavior:** Removed the 1,500 Bytes restriction for MTU size for P-GW, S-GW, SAEGW and GGSN services.

**CSCur08331 - [17.1] P-CSCF discovery over GTP S2a via the APCO parameter in the CSR**

**Feature Changes**

**Behavior Enhanced to support P-CSCF address in APCO IE for S2a interface**
Enhanced P-GW behavior to support P-CSCF address in APCO IE for S2a interface.

**Previous Behavior:** Support for P-CSCF in APCO IE on S2a interface was not there at the P-GW.

**New Behavior:** The P-GW can now send P-CSCF address in CSResp for P-CSCF address request in APCO IE by the HSGW.

**CSCur15224 - [ePDG] PGW Support for IPv4 and IPv6 P-CSCF address in private extn IE**

**Feature Changes**

**Private Extension IE of the Create Session Message on S2b interface**

**Previous Behavior:** The previous behavior is if:

- IPv6 P-CSCF address was requested in the message, then the IPv6 P-CSCF address was sent in the Create session response message.
- IPv4 P-CSCF address was requested in the message, then the IPv4 P-CSCF address was sent in the Create session response message.
- both IPv4 and IPv6 P-CSCF address were requested in the message, then either the IPv4 or IPv6 P-CSCF address was sent in the Create session response message (not both).

**New Behavior:** The new behavior is if:

- IPv6 P-CSCF address is requested in the message, then send the IPv6 P-CSCF address in the Create session response message.
- IPv4 P-CSCF address is requested in the message, then send the IPv4 P-CSCF address in the Create session response message.
- both IPv4 and IPv6 P-CSCF address are requested in this message, then send both the IPv4 and IPv6 P-CSCF address in the Create session response message.

**CSCur33479 - DCCA-GTP cause code APN access denied not working for PGW and GGSN**

**Feature Changes**

**DCCA-GTP Cause Code APN Access Denied Not Working for P-GW**

**Previous Behavior:**

When the following CLI was configured in StarOS:

```bash
configure

active-charging service service_name
credit-control
```
diameter result-code authorization-rejected use-gtp-cause-code apn-access-denied-no-subscription
end

- Diameter (Gy) Server had configuration as: --result-code 5003
- P-GW GTP cause in Create Session Response was GTP_NO_RESOURCESAVAILABLE.

When the following CLI was configured in StarOS:

configure

  active-charging service service_name
  credit-control

  diameter result-code user-unknown use-gtp-cause-code authentication-failure
end

- Diameter (Gy) Server had configuration as: --result-code 5030
- P-GW GTP cause in Create Session Response was GTP_NO_RESOURCESAVAILABLE.

New Behavior:

When the following CLI is configured in StarOS:

configure

  active-charging service service_name
  credit-control

  diameter result-code authorization-rejected use-gtp-cause-code apn-access-denied-no-subscription
end

- Diameter (Gy) Server has configuration as: --result-code 5003
- P-GW GTP cause in Create Session Response is APN_ACCESS_DENIED-NO_SUBSCRIPTION.

When the following CLI is configured in StarOS:

configure

  active-charging service service_name
  credit-control

  diameter result-code user-unknown use-gtp-cause-code authentication-failure
end
• Diameter (Gy) Server has configuration as: --result-code 5030
• P-GW GTP cause in Create Session Response is USER_AUTHENTICATION_FAILED.

CSCur51701 - Disconnect Reason Not Updated correctly For Saegw-collapsed call

Feature Changes

P-GW and SAEGW Session Disconnect Reason Not Updated Correctly for Multi Bearer Call

Previous Behavior: When the first dedicated bearer was released for P-GW and SAEGW calls for a multi bearer call, the disconnect reason was set for all bearers. Other bearers went down with different disconnect reasons and the new disconnect reason was not updated in the bearers. Therefore, the show session disconnect reason displayed the wrong output.

New Behavior: When the first dedicated bearer is released for P-GW and SAEGW calls for a multi bearer call, the disconnect reason is only set to specific bearers. After other bearers go down with a different disconnect reason, the new disconnect reasons is updated correctly in the bearers. Therefore, the show session disconnect reason will display the correct output.

CSCur52706 - PGW/GGSN: Disc-reason Bulkstats verifiction reqd for CSCur33479

Performance Indicator Changes

show pgw-service statistics

The following counter has been added under PDNs Rejected By Reason section:

• Apn-Denied No Subscription

CSCur47338 - [SysTest] audit-gtpumgr-failure CRR recovery failures observed

Feature Changes

SM and GTPUMGR Behavior for Same Remote TEID

Initially, there was inconsistency between sm and gtpumgr if dedicated bearer had the same remote TEID for the same peer. In gtpumgr, the old bearer was replaced by a new bearer; in sm, P-GW kept both bearers.

Previous Behavior: If both bearers have same remote TEID, then gtpumgr removed old bearer and replaced with a new bearer; however, sm kept both bearers.

New Behavior: Now, both sm and gtpumgr keep only the new bearer and old bearer is deleted/removed from the sm and gtpumgr.
CSCur74924 - DCCA-GTP cause code mapping not working for system-failure

Performance Indicator Changes

show pgw-service statistics name pgw_service

New counter added in PDNs Rejected By Reason section to ease debugging:

- System Failure

CSCur84831 - P-CSCF Discovery TO-BE Initiated S4-SGSN to LTE (and vice versa) Handoff

Feature Changes

P-CSCF Discovery Upon S4-SGSN to LTE (and Vice Versa) Handoff

**Previous Behavior:** When the P-CSCF Address information is missing, P-CSCF Discovery does not get initiated upon S4-SGSN to LTE (and vice versa) handoff.

**New Behavior:** When the P-CSCF Address information is missing, P-CSCF Discovery is now initiated upon S4-SGSN to LTE (and vice versa) handoff. If the P-CSCF Address information is already available, there is no need to explicitly trigger another P-CSCF Discovery upon S4-SGSN to LTE (and vice versa) handoff.
P-GW Enhancements for 17.0

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

---

**CSCug47563 - ASR5K LMA fails to assign client IP address using external DHCP Server**

**Feature Changes**

**ASR 5000 LMA Failed to Assign Client IP Address Using External DHCP Server**

DHCPv4 proxy functionality has been enhanced to provide the information the DHCP server will need to assign the correct DHCP address and properly manage the UE device.

**Relay Address**

P-GW/LMA has been enhanced to support DHCPv4 proxy functionality to have the ability to define a Relay Agent IP Address (giaddr) in the DHCP Discover and Request messages to the external DHCPv4 server, per RFC 2131. This is configurable on a per-APN basis.
This information is used by the DHCPv4 server to determine the appropriate IP Pool to assign an IP address, subnet mask, IPv4 default router, and DNSv4 IP addresses. This is taken from the bind address of the DHCP service or the bind address of the service that the DHCP service is associated with. Use of this address is configurable on a per-APN basis.

**DHCP Client MAC Address and Client Identifier**

P-GW/LMA has also been enhanced to support DHCPv4 proxy functionality to map the LLID received in the PBU from the MAG to the Client MAC Address (chaddr), per RFC 2131 (Dynamic Host Configuration Protocol), and Option(61) Client Identifier, per RFC 2132 (DHCP Options and BOOTP Vendor Extensions), AVPs within the DHCPv4 Discover and Request messages to the external DHCPv4 server. This is encoded in the MAC48 format. This functionality is enabled by a configuration command in the DHCP service configuration.

**Command Changes**

dhcp client-identifier

`link-layer-identifier` is a new keyword in this command that enables giaddr in the DHCP proxy client messages. The APN configuration has the ability to include which DHCP service it will be associated with.

```plaintext
configure

context context_name

dhcp-service service-name

   dhcp client-identifier link-layer-identifier

   default dhcp client-identifier

end
```

Notes:

- By associating a different APN with a different DHCP service, and configuring a different bind address with each DHCP service, each APN can configure its own relay agent address. The DHCP service is associated with an APN with the existing `dhcp-service-name` command in the APN Configuration Mode and the DHCP service will specify the bind address to be used as the giaddr.

- Once the DHCP service has been associated with an APN, Client Mac Address and Client Identifier behavior can be configured in the DHCP service configuration. When `client-identifier` is configured with `link-layer-identifier`, the link-layer-identifier from PBU is used to populate the client-identifier value. This configuration only applies to DHCP service associated with an LMA service. When associated with a non-LMA service, choosing this option will cause client-identifier to be empty.

**CSCuh35078 - PGW responds to Create Session Request with Mandatory IE incorrect**

**Feature Changes**

**P-GW responds to Create Session Request with Mandator IE incorrect**

**Previous Behavior:** Protocol layer was rejecting CS Requests with MEI IE having value as all
New Behavior: Protocol layer will not reject CS Requests with MEI IE having value as all 0.

Customer Impact: Customers having MEI value as all 0 will be allowed to latch onto the network.

**CSCuh48881 - TCP support for DNS upon P-CSCF discovery**

Feature Changes

**TCP Support for DNS upon P-CSCF Discovery**

Confirmed that the DNS falls back from UDP to TCP when the DNS answer is more than 40965 bytes and it is received with the 'truncated flag' set.

**CSCui87830 - Incorrect cause code set for EGTP_BEARER_RESOURCE_FAILURE_IND msg**

Feature Changes

**Incorrect Cause Code Set for eGTP_Bearer_Resource_Failure_Indication Message**

Previous Behavior: In “Bearer Resource Failure Indication” message, “No Resource Available” cause code was used for failure scenarios like BRC for default bearer, some PCC failures, etc.

New Behavior: From 3GPPRelease 10, the cause code “No Resource Available” is removed for “Bearer Resource Failure Indication” message; therefore, in “Bearer Resource Failure Indication”, “Service Denied” cause code is used instead of “No Resource Available” message.

**CSCul72349, CSCug75135 - PGW LORC mechanism for subscriber billing**

Feature Changes

**Overcharging Protection**

Confirmed that the Overcharging Protection feature is supported at APN and P-GW service. When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

**CSCum17169 - Per APN, and QCI, GTP-C v2 responses**

Feature Changes

**Per APN and QCI GTP-C v2 Responses**

This feature collects the eGTP-C cause codes as bulkstats and categorizes them per APN and per QCI. Operator can derive KPI based on the bulkstat counters per QCI for a particular APN (for example: IMS APN and VoLTE APN).
Supporting more granular statistics/bulkstats on APN (up to 2,000 APNs are supported) has an impact on system performance and this occurs for bulkstats. Statistics need to be obtained at regular intervals for a few minutes. Each of these retrievals can lead to gigabytes of information to be gathered and consolidated. Due to this issue, a restricted/controlled usage of granular bulkstats is introduced. The operator can enable which APN to collect granular statistics using the configuration. In those granular statistics, it is possible to decide which particular statistics to collect.

**Previous Behavior:** In general, the current bulkstats APN configuration gathers the bulkstat data for all of the APNs; there is no option to restrict gathering of bulkstats for selective APN(s).

**New Behavior:** A new CLI is introduced to selectively enable an APN candidate list for the new bulkstat schema “apn-expansion”. The eGTP-C cause code bulkstats will be collected for those APN(s) which are configured through this CLI only.

**Customer Impact:** This feature allows operators to collect more granular GTP-C statistics on a per-APN and per-QCI level to monitor certain KPIs based on these statistics.

### Command Changes

**egtpc-qci-stats**

This new command enables/disables an APN candidate list for the apn-expansion bulkstat schema.

```
configure

context context_name

apn apn_name

[ no ] egtpc-qci-stats { all | qci1 | qci2 | qci3 | qci4 | qci5 | qci6 | qci7 | qci8 | qci9 } +

default egtpc-qci-stats

end
```

**Notes:**
- Refer to the *APN Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information about this command.

### Performance Indicator Changes

**APN-expansion schema**

A new schema has been added to categorize bulkstats per APN QCI.

- cresessrespaccept
- cresessrespdienCtxtNotFound
- cresessrespdienInvalidMsgFormat
- cresessrespdienInvalidLength
- cresessrespdienMandIEIncorrect
- cresessrespdienMandIEMissing
- cresessrespdeniedNoResourcesAvl
- cresessrespdeniedPrefPdnTypeUnsupported
- cresessrespdeniedAllDynamicAddrOccupied
- cresessrespdeniedServiceDenied
- cresessrespdeniedUserAuthFailed
- cresessrespdeniedApnAccessDenied
- cresessrespdeniedRequestRejected
- cresessrespdeniedCondIEMissing
- cresessrespdeniedApnRstTypeIncompatible
- cresessrespdeniedImsiNotKnown
- cresessrespdeniedOtherCause
- crebearNorsp
- crebearrespaccept
- crebearrespdeniedCtxtNotFound
- crebearrespdeniedSvcNotSupported
- crebearrespdeniedInvalidMsgFormat
- crebearrespdeniedMandIEIncorrect
- crebearrespdeniedMandIEMissing
- crebearrespdeniedCondIEMissing
- crebearrespdeniedNoResourcesAvl
- crebearrespdeniedSemanticErrinTFT
- crebearrespdeniedSyntacticErrinTFT
- crebearrespdeniedSemanticErrinPktFltr
- crebearrespdeniedSyntacticErrinPktFltr
- crebearrespdeniedUnableToPageUE
- crebearrespdeniedUENotResponding
- crebearrespdeniedUnableToPageUeSuspend
- crebearrespdeniedUERefuses
- crebearrespdeniedRequestRejected
- crebearrespdeniedInvalidLenPiggybkMsg
- crebearrespdeniedInvalidRemotePeerReply
- crebearrespdeniedPeerNotResponding
- crebearrespdeniedTempRejDueToHOProgress
- crebearrespdeniedDeniedInRat
- crebearerrespdeniedOtherCause
- modbearerrespaccept
- modbearerrespdeniedCtxNotFound
- modbearerrespdeniedInvalidMsgFormat
- modbearerrespdeniedInvalidLength
- modbearerrespdeniedMandIEIncorrect
- modbearerrespdeniedMandIEMissing
- modbearerrespdeniedNoResourcesAvl
- modbearerrespdeniedServiceDenied
- modbearerrespdeniedRequestRejected
- modbearerrespdeniedCondIEMissing
- modbearerrespdeniedOtherCause
delsessrespaccept
delsessrespdeniedInvalidMsgFormat
delsessrespdeniedMandIEIncorrect
delsessrespdeniedMandIEMissing
delsessrespdeniedNoResourcesAvl
delsessrespdeniedOtherCause
delbearerNorsp
delbearerrespaccept
delbearerrespdeniedCtxNotFound
delbearerrespdeniedInvalidMsgFormat
delbearerrespdeniedMandIEIncorrect
delbearerrespdeniedMandIEMissing
delbearerrespdeniedCondIEMissing
delbearerrespdeniedNoResourcesAvl
delbearerrespdeniedRequestRejected
delbearerrespdeniedUnableToPageUeSuspend
delbearerrespdeniedInvalidRemotePeerReply
delbearerrespdeniedPeerNotResponding
delbearerrespdeniedTempRejDueToHOProgress
delbearerrespdeniedOtherCause
updbearNorsp
updbearerrespaccept
• updbearspdeniedCtxtNotFound
• updbearspdeniedInvalidMsgFormat
• updbearspdeniedMandIEIncorrect
• updbearspdeniedMandIEMissing
• updbearspdeniedNoResourcesAvl
• updbearspdeniedSemanticErrinTFT
• updbearspdeniedSyntacticErrinTFT
• updbearspdeniedSemanticErrinPktFltr
• updbearspdeniedSyntacticErrinPktFltr
• updbearspdeniedUENotResponding
• updbearspdeniedUERefuses
• updbearspdeniedUnableToPageUE
• updbearspdeniedRequestRejected
• updbearspdeniedUnableToPageUeSuspend
• updbearspdeniedCondIEMissing
• updbearspdeniedInvalidRemotePeerReply
• updbearspdeniedPeerNotResponding
• updbearspdeniedTempRejDueToHOProgress
• updbearspdeniedOtherCause

show apn name

The following new field has been added:
• APN QCI Stats

CSCum17282 - VoLTE Retainability KPI

Feature Changes

Statistics Enhancements

**Previous Behavior:** P-GW dedicated bearer release statistics per APN per QCI were not present.

**New Behavior:** P-GW dedicated bearer release due to ‘Admin Clear' statistics per APN per QCI are now present.

**Customer Impact:** P-GW dedicated bearer release statistics are available per APN per QCI.

Performance Indicator Changes

APN Schema
Added the following new statistics in the APN schema to track how many dedicated bearers (QCI per APN) are released due to admin clear from P-GW:

- `sessstat-bearrel-ded-admin-clear`
- `sessstat-bearrel-ded-admin-clear-qci1`
- `sessstat-bearrel-ded-admin-clear-qci2`
- `sessstat-bearrel-ded-admin-clear-qci3`
- `sessstat-bearrel-ded-admin-clear-qci4`
- `sessstat-bearrel-ded-admin-clear-qci5`
- `sessstat-bearrel-ded-admin-clear-qci6`
- `sessstat-bearrel-ded-admin-clear-qci7`
- `sessstat-bearrel-ded-admin-clear-qci8`
- `sessstat-bearrel-ded-admin-clear-qci9`

**show apn statistics**

The following field has been added to the `show apn statistics` output.

- 4G Bearers Released by Reasons
  - QCI1
  - QCI2
  - QCI3
  - QCI4
  - QCI5
  - QCI6
  - QCI7
  - QCI8
  - QCI9

**CSCum17389 - [17.0] EGTPC Dependency to support Per APN, and QCI, GTP-C v2 responses**

**Feature Changes**

**eGTP-C Statistics Enhancements**

New counters and bulk statistics have been introduced to collect more granular GTP-C statistics on per-APN QCI level to monitor certain KPIs.

**Important:** See **CSCum17169** for additional information.
**Customer Impact:** This feature allows operator to collect more granular GTP-C statistics on per-APN per-QCI level to monitor certain KPIs based on these statistics.

**CSCum17434 - [17.0] AAA provide Restoration Priority Indicator to PGW**

**Feature Changes**

**Support for Restoration Priority Indicator**

To distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections, the gateway will now support receiving a new AVP “Restoration-Priority-Indicator” from AAA server over the S6b interface. The gateway will be able to provide KPIs based on the AVP value.

**Previous Behavior:** Previously, Restoration Priority Indicator was not available from AAA and the output of show subscribers saegw-only full all did not display the restoration priority value.

**New Behavior:** Added a “Restoration priority level” field to display the value of restoration priority. Restoration Priority Indicator is now received from AAA across S6b interface.

**Customer Impact:** The customer will see the value of restoration priority associated with a co-located call. The customer will also be able differentiate a VoLTE subscriber from non-VoLTE subscriber based on the value of “Restoration Priority Indicator” AVP.

**Command Changes**

**show pdn-connection-count**

This new command displays the current number of PDN connections for each of the Restoration-Priority-Level values (1 to 8).

```
show pdn-connection-count restoration-priority-level { priority_level | all }
```

**Notes:**

- **restoration-priority-level:** Restoration priority associated with PDN connection.
- **priority_level:** Restoration priority value. Must be an integer from 1 through 8.
- **all:** Displays number of PDN connections associated with all restoration priorities.

**Performance Indicator Changes**

**show saegw-only full all**

The following new field has been added.

- Restoration priority level

**show subscribers pgw-only full all**

The following new fields display the value of restoration priority associated with a P-GW subscriber.

- Restoration priority level
show bulkstats variables gtpc

The following new gauges display the current number of PDN connections for each of the Restoration-Priority-Level values (1 to 8):

- current-pdn-restore-priority-1
- current-pdn-restore-priority-2
- current-pdn-restore-priority-3
- current-pdn-restore-priority-4
- current-pdn-restore-priority-5
- current-pdn-restore-priority-6
- current-pdn-restore-priority-7
- current-pdn-restore-priority-8

show bulkstats variables pgw

The following new gauges display the current number of PDN connections for each of the Restoration-Priority-Level values (1 to 8):

- sessstat-pdn-restore-priority-1
- sessstat-pdn-restore-priority-2
- sessstat-pdn-restore-priority-3
- sessstat-pdn-restore-priority-4
- sessstat-pdn-restore-priority-5
- sessstat-pdn-restore-priority-6
- sessstat-pdn-restore-priority-7
- sessstat-pdn-restore-priority-8

CSCum17462 - PGW Support for PCSCF Recovery

Feature Changes

P-GW Support for P-CSCF Recovery

Previously, 3GPP was evaluating options to address P-CSCF failure and recovery scenarios. Most proposals at 3GPP included the UE being disconnected from the IMS PDN when the P-CSCF the UE was registered with failed. The other possible scenario was when the P-GW monitored the P-CSCFs and provided an update to the UE when one of the P-CSCFs provided to the UE had failed.

Previously, the user was disconnected and all P-GWs monitored all P-CSCFs. There was a customer request to avoid this scenario by using the S-CSCF that identifies the P-CSCF that the UE is currently registered with has failed. Then, it triggers a PCO update for the P-CSCF IP addresses provided to the UE. If there is an indication from the HSS that P-CSCF Recovery is required, then the PCO update is requested by the MME.
**Previous Behavior:**  Previously, P-CSCF Recovery was not supported. Discovery support was only available during the Initial Attach.

**New Behavior:**  P-CSCF Recovery is now supported while a session is on-going.

**Customer Impact:**  The customer will be able to see the number of P-CSCF restoration indications received at the P-GW Service Level.

### Performance Indicator Changes

**P-GW Schema**

The following statistic has been added for tracking the number of occurrences of P-CSCF Restoration Required Indications received from the MME/S-GW through a modify bearer request:

```plaintext
sesstat-pcsf-recovery-count
```

**show pgw-service statistics all**

The following field has been added for displaying the number of occurrences of P-CSCF Restoration Required Indications received from the MME/S-GW through a modify bearer request:

- P-CSCF Restoration Indications received: <Count at Service Level>

### CSCum17490 - EGTPC Support - PGW Support for PCSCF Recovery

#### Feature Changes

**P-GW Support for P-CSCF Recovery**

The P-GW can store the P-CSCF FQDN received during the initial registration with the AAA. Upon receiving the P-CSCF restoration flag from the MME/S-GW, the P-GW performs a new DNS query using the existing P-CSCF FQDN to provide the updated list of three P-CSCF IP addresses using PCO.

**Customer Impact:**  Supports spec-based mechanism to support P-CSCF discovery for GTP-based S2b interface for WiFi integration. This is needed for Voice over WiFi service.

### CSCum17693 - Rejecting non-emergency 9th network initiated DRB per UE

#### Feature Changes

**P-GW Cause Code Mapping**

Confirmed that the MME rejects the creation of more than 8 DRBs without initiating any UE procedures and the P-GW maps the MME provided GTP cause code to the Gx cause code.

**Important:**  This functionality is only applied to non-emergency calls.
CSCum41945, CSCum17370 - EGTPC - PDN session handling for Invalid IMEI & IMSI-less devices

Feature Changes

PDN Session Handling for Invalid IMEI and IMSI-less Devices

Due to legacy devices in the network which are configured with invalid IMEI or provide invalid IMEI to the network, it is possible that different UEs may report the same IMEI, resulting in duplicate IMEI in the network. In other scenarios, it is possible that IMEI is completely missing. In most scenarios, when IMSI is available and valid, the network can handle the subscriber session. For UEs that do not have valid IMSI and attach to the network for emergency PDN, a duplicate IMEI could be an issue because a unique index is not available for MME, S-GW, and P-GW to identify the user.

Customer Impact: To avoid unforeseen or un-deterministic behavior, P-GW supports a common behavior in these scenarios.

Performance Indicator Changes

show egtpc statistics verbose

The following fields have been added to track PDN session handling for invalid IMEI and IMSI-less devices:

- IMSI/IMEI Statistics:
  - IMSI Invalid Length
  - IMSI All Zero
  - IMSI Not BCD
  - IMEI Invalid Length
  - IMEI All Zero
  - IMEI Not BCD
  - IMEI All Zero (unauthenticated imsi)
  - IMEI Not BCD (unauthenticated imsi)
  - IMEI All Zero (unauthenticated imsi and context replacement)
  - IMEI Not BCD (unauthenticated imsi and context replacement)

CSCum42664, CSCum41968, CSCum76157 - Bit Rate mapping across Gx and GTP based interfaces

Feature Changes

Bit Rate Mapping Across Gx and GTP-based Interfaces
Bit rate granularity provided by different interfaces was not aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

With this feature, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up.

**Previous Behavior:** Previously, rounded-down kbps bitrate (AMBR, MBR, BGR) values were being sent towards the Access side.

**New Behavior:** Bitrate granularity is still maintained per the current interface specifications but 3GPP provides explicit guidance that whenever the conversion from bps to kbps results in decimal values, the node converting should round the value up.

Introduced a new CLI command under P-GW service `[ no ] egtp bit-rates-rounded-down-kbps` to control the behavior of rounding-up. The CLI command will enable/disable the old behavior of rounding down. By default, this CLI command is configured to use rounded-up bitrate values. Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value will be sent on GTP interface towards the Access side. If the CLI command is enabled, then it will result in the old behavior. This feature (rounding up the bitrate in kbps) will be enabled by default. Also, `show subscribers pgw-only full all` will show the APN-AMBR in terms of bps. Previously, `show subscribers pgw-only full all` used to show in terms of kbps.

CR - C4-132189 - is defined for TS 29.274 for GTP conversion by P-GW.

**Customer Impact:** This feature provides for more consistent behavior and ensures correct bandwidth is allocated for bearers.

**Command Changes**

`egtp bitrates-rounded-down-kbps`

This new command enables/disables the previous behavior of rounding down.

```
configure

    context context_name

    pgw-service service name

        [ no ] egtp bitrates-rounded-down-kbps

end
```

**Notes:**

- The default behavior is to use rounded-up bitrate values.
- Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value is sent on the GTP interface towards the Access side.
- If the CLI command is enabled, then it will result in the previous behavior.

**Performance Indicator Changes**

`show configuration context ingress`
The following field has been added:
- egtp bitrates-rounded-down-kbps

**show pgw-service all**

The following field has been added:
- EGTP Bit Rate in Rounded Down kbps

**show pgw-service name pgw-service**

The following field has been added:
- EGTP Bit Rate in Rounded Down kbps

**CSCum56817 - Use of well-known APN for customer-specific 4G subs**

**Feature Changes**

**Use of Well-known APN for 4G Subscribers**

Confirmed that well-known APN is supported for a specific customer’s enterprise P-GW.

**CSCum66168 - DHCPv6: IPv6 default prefix AAA and Delegated Prefix Correlation**

**Feature Changes**

**AAA and Prefix Delegation DHCP Correlation**

Currently at the DHCP server, DHCPv6 does not provide any mechanism to correlate allocated IPv6 (/64) prefix to a particular subscriber. This feature correlates the default prefix allocated from AAA server with the delegated prefix allocated from external DHCPv6 server during the PDN connection setup.

New options have been added to an existing CLI in DHCP Client Profile Configuration Mode to enable P-GW to send USER_CLASS_OPTION in DHCPv6 messages to external DHCPv6 server during delegated prefix setup.

**Important:** This feature 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**

```enable```
New keyword **user-class-option** has been added, along with some other options within it, to determine whether IMSI or MSISDN should be sent in the User_Class_Option in DHCPv6 Request during Prefix Delegation Setup. By default, this functionality is disabled.

```configure

context context_name

  dhcp-client-profile profile_name

    enable user-class-option { imsi | msisdn }

  end

end
```

**Notes:**
- **enable user-class-option imsi**: Triggers sending the “User_Class_Option” with UE’s IMSI in the DHCPv6 Request message from P-GW to the external DHCPv6 server during DHCPv6 Prefix Setup (for network behind UE).
- **enable user-class-option msisdn**: Triggers sending the “User_Class_Option” with UE’s MSISDN in the DHCPv6 Request message from P-GW to the external DHCPv6 server during DHCPv6 Prefix Setup (for network behind UE).

```disable

context context_name

  dhcp-client-profile profile_name

  disable user-class-option

  end

end
```

**Notes:**
- “User_Class_Option” is not sent with UE’s IMSI or MSISDN in the DHCPv6 Request message from P-GW to the external DHCPv6 server during DHCPv6 Prefix Setup (for network behind UE).

### Performance Indicator Changes

**show dhcpv6-client-profile all**

The following new field has been added to show whether sending the User_Class_Option in DHCPv6 Request during Prefix Delegation Setup has been enabled or disabled, and whether IMSI or MSISDN should be sent if enabled:

- **User_Class_Option**
CSCum85473, CSCui11396 - GTP-U DSCP marking needs enhancement

Feature Changes

DSCP Marking for GTP-U Echo

This feature adds CLI in GTP-U service to allow provisioning of DSCP value for GTP-U echo. This is similar to the DSCP value for GTP-C echo configuration that already exists in the eGTP service.

Command Changes

ip qos-dscp

This is a new command that configures the quality of service (QoS) differentiated service code point (DSCP) per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component.

configure

context context_name

gtpu-service service_name

    ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41
    | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

    [ default | no ] ip qos-dscp

end

Notes:

- This is a standards-based feature (RFC 2597 and RFC 2474).
- DSCP marking will be implemented only for GTP-U ECHO Request and Response messages.

CSCum88464, CSCup56698 - Intelligent graceful PDN disconnection during maintenance-mode

Feature Changes

Intelligent Graceful PDN Disconnection During Maintenance Mode

When a gateway is in maintenance mode and new-call policy is enabled at a service or APN level, it only rejects new calls as the rejection is at the demux. For PDNs that have dedicated bearers, even though the APN is in maintenance mode, since the default bearer is already up, network-initiated dedicated bearers will still be accepted by the gateway and thus block clearing of all PDNs. CLI has been added to clear the entire PDN when the last VoLTE dedicated bearer goes down.
Command Changes

clear subscribers

auto-delete is a new keyword that enables auto deletion when PDN connections that do not have an active voice call are disconnected.

clear subscribers apn apn_name non-volte-call auto-delete [ max-subscribers max_count ] [ uniform ]
clear subscribers all non-volte-call auto-delete [ max-subscribers max_count ] [ uniform ]

Notes:

• auto-delete: Clears the PDN/call when the last VoLTE dedicated bearer goes down for P-GW, S-GW, SAEGW, GGSN, and ePDG. Calls will not be cleared when one of the calls in a multiple PDN scenario is a VoLTE PDN. When the VoLTE PDN goes down, all of the other PDNs found for the same IMSI are brought down, which will bring down the call automatically.

• max-subscribers: (existing keyword) The maximum number of subscribers to be cleared.

max_count must be an integer from 0 through 20000000.

• uniform: (existing keyword) Subscribers will be cleared uniformly.

• This assumes that new call policy has been configured on the node to reject any new calls so that these new calls get directed to an alternate PDN before clear subscribers command is executed.

Performance Indicator Changes

show subscribers pgw-only full

A new field has been added to the output of this command to indicate if session Auto Delete is enabled.

• Auto Delete

show session disconnect-reasons verbose

The following disconnect reason is used to indicate the percentage of the total number of sessions that have been auto deleted.

• session-auto-delete(588)

CSCun46475 - PGW is sending wrong S6b STR Termination Cause

Feature Changes

P-GW Sending Incorrect S6b STR Termination Cause
**Previous Behavior:** When the UE moved up to LTE from eHRPD, the P-GW was sending S6b STR (Termination Cause=DIAMETER_LOGOUT).

**New Behavior:** When the UE moves up to LTE from the eHRPD, the P-GW is now sending the DIAMETER_USER_MOVED as the Termination cause.

**CSCun65038 - PGW/SAEGW - Network Provided Location Info (NPLI) for IMS [SM Support]**

**Feature Changes**

**Network Provided Location Information for IMS**

This feature enables the P-GW to provide the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP as requested by the PCRF. The P-GW will also provide the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

During bearer deactivation or UE detach procedure, the P-GW will provide the access network information to the PCRF within the 3GPP-User-Location-Info AVP and information on when the UE was last known to be in that location within User-Location-Info-Time AVP. If the PCRF requested User location info as part of the Required-Access-Info AVP and it is not available in the P-GW, then the P-GW will provide the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP.

This is required for VoLTE and aids in charging and LI functionality in IMS domain.

**Important:** Use of NPLI requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

**Previous Behavior:** Previously, the P-GW used to notify ULI/MS-TimeZone/PLMN-ID to ECS/IMSA/PCRF only when their value used to change.

**New Behavior:** This feature change the P-GW will now receive NetLoc indication in the rules sent by ECS regardless of whether the values changed and it will send this to the ECS/IMSA/PCRF. If the P-GW receives NetLoc as ‘0’, then it will inform MS-Timezone. If the P-GW receives NetLoc as ‘1’, then it will inform ULI and ULI Timestamp. If ULI is not available in that case, then the PLMN-ID is sent. If NetLoc indication is received for an update, then the P-GW will indicate this information to the access side in the UBReq using the RetLoc Indication flag.

**Customer Impact:** This feature allows EPC core to support an efficient way of reporting ULI and Time-Zone information of the subscriber to the IMS core network.

**CSCuo06912 - PGW call fails if Framed-Pool enforced from radius**

**Feature Changes**

**P-GW Call Fails if Frame-Pool Enforced from Radius**

In P-GW, if radius returned ip pool in access accept, then this scenario was not handled correctly.
**Previous Behavior:** For P-GW, if radius returned ip pool for ip address alloc method as no-dynamic, then ip address allocation was not successful.

**New Behavior:** For P-GW, if radius returns ip pool for ip address alloc method as no-dynamic, then ip address allocation will be successful.

**Customer Impact:** The customer will be able to use no-dynamic ip alloc method for radius returned ip pool.

---

**CSCuo11336 - Update bearer Request not triggered on FUA action from Gy**

**Feature Changes**

**Update Bearer Request Triggered on FUA Action from Gy**

The UBR should go when FUA triggered from Gy.

**Previous Behavior:** If Gy sent the same PCO value twice, UBR was initiated again for the same PCO.

**New Behavior:** Now, UBR will not be initiated in above scenario because previous PCO action value is stored before modifying the CLP PCO action value.

---

**CSCuo38762 - congestion-control threshold related CLI not visible in show config**

**Feature Changes**

**Congestion-control Threshold related CLI Not Visible in Show Config**

Updated the congestion-control command in the *Command Line Interface Reference*.

---

**CSCuo90006 - Formulation of P-CSCF Address Output as part of show sub full all**

**Feature Changes**

**Formulation of P-CSCF Address Output as Part of show subscribers full all**

Simplified the P-CSCF Address Output as part of `show subscribers full all` command output. The P-CSCF discovery mode specific information is SR/GR recovered.

**Previous Behavior:** Previously, the P-CSCF Address output displayed the P-CSCF Address information separately for S6b based FQDN and for Radius or configured scenarios. It also restricted the S6b mode to only display the IPv6 Address Information. IPv4 information was not being displayed. In addition, the earlier output did not support persistence across ICSR/Session Recovery for all the discovery modes.

**New Behavior:** In the new output, a “Discovery Mode” field specifies the method of discovery followed by the actual P-CSCF Address information. Also, the new output displays both IPv4 and IPv6 address information as per applicability. The new output remains persistent across ICSR/Session Recovery for all P-CSCF discovery modes.
CSCup27196 - License for 17.0.

Feature Changes

Support of Simultaneous Create Bearer Request and Update Bearer Request

Simultaneous Create Bearer Request and Update Bearer Request is supported by P-GW.

See CDETS ID CSCum62403 in the ECS Enhancements for 17.0 chapter for additional information.

**Important:** This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

CSCup54622 - CLI equivalent for these bulkstats variables of egtpc schema

Feature Changes

**CLI Equivalent for Bulk statistics Variables of eGTP-C schema**

Some CLI output for `show egtpc statistics` command was not displayed. Some of these bulk statistics were marked obsolete because there was not a requirement for them to be incremented.

**Previous Behavior:** Some CLI output for `show egtpc statistics` command was not displayed.

**New Behavior:** Added CLI output for `show egtpc statistics` command.

**Customer Impact:** The customer will now see additional counters in the `show egtpc statistics` output.

Performance Indicator Changes

**eGTP-C Service Schema**

The following counters have been added:

- csfb-recv-retranssuspendnotif
- csfb-sent-suspendackaccept
- csfb-sent-suspendackdenied
- csfb-recv-suspendackaccept
- csfb-recv-suspendeddenied
- csfb-recv-retransresumenotif
- csfb-sent-resumeackaccept
- csfb-sent-resumeackdenied
- csfb-recv-resumeackaccept
P-GW Changes in Release 17

P-GW Enhancements for 17.0

- csfb-recv-resumended
- mobility-recv-retransctxrsp
- mobility-sent-retransidtrsp
- mobility-sent-retransalertmmeack
- mobility-sent-retransueactivityack

The following counters have been removed:
- tun-recv-retransbearrescmd-fail
- tun-recv-retransmodbearfail
- tun-recv-retransdelbearfail
- tun-sent-noRspPgwrstnotfreq
- mobility-recv-retransctxack
- mobility-recv-retransidtrsp
- mobility-recv-retransfwdrlrsp
- mobility-recv-retransfwdaccack
- mobility-recv-retransfwdrelcmpack
- mobility-recv-retransrelcancelrsp
- mobility-recv-retransalertmmeack
- mobility-recv-retransueactivityack

CSCup60931 - [17.0] PGW should not send UBR after PCSCF recovery MBR on emergency APN

Feature Changes

P-GW Should Not Sent a UBR After P-CSCF Recovery MBR on an Emergency APN

Previous Behavior: When P-CSCF recovery gets initiated on an Active call, the P-CSCF Discovery gets re-initiated for that call. In addition, P-CSCF discovery gets initiated during Call Bring-up (PDN Establishment). P-CSCF Discovery upon PDN establishment was in place in StarOS Release 16.0.

New Behavior: For an Emergency Call, P-CSCF Discovery upon PDN establishment is applicable but P-CSCF recovery is not applicable. Even if a trigger is received for P-CSCF Recovery for Emergency PDN for the Access side (mostly for a multi-pdn scenario), then the P-GW will not perform P-CSCF Recovery processing for that trigger.

Important: See CSCum17462 for additional information.
CSCup89213 - Incorrect cause-code in DB Req for PCRF initiated session termination

Feature Changes

Incorrect cause-code in DB Requirement for PCRF Initiated Session Termination

**Previous Behavior:** For a APN with default/no pdn-behavior, a DB Request went out with the Cause Code “Reactivation Requested”. This occurred whenever a P-GW PDN deletion was triggered when a PCRF connection failure/result code based failure/ims service was removed from a configuration. However, according to a specific customer specification for an APN with default/no pdn-behavior, a Cause Code IE should not be included if a message is caused by PCRF initiated PDN disconnect procedure in a Delete Bearer Request.

**New Behavior:** For an APN with default/no pdn-behavior, a DB request will not include a Cause Code IE when a PCRF initiated P-GW PDN deletion is triggered. The trigger can be a PCRF connection failure/result code based failure/ims service that is removed from a configuration.

**Customer Impact:** For an APN with default/no pdn-behavior, a DB request will not include a Cause Code IE when a PCRF initiated P-GW PDN deletion is triggered. The trigger can be a PCRF connection failure/result code based failure/ims service that is removed from a configuration.

CSCuq19244 - PGW doesnt initiate dns query to resolve p-cscf addr after ehrpd-epdg ho

Feature Changes

**P-GW Did Not Initiate DNS Query to Resolved P-CSCF Address after Inter-tech Handoffs**

P-GW did not initiate P-CSCF Discovery to resolved P-CSCF Address after following inter-tech handoff scenarios if P-CSCF Address information is already missing.

**Previous Behavior:** If P-CSCF address information was already missing, then the P-GW did not initiate P-CSCF Discovery to resolve the P-CSCF address after the following inter-tech handoff scenario.

- eHRPD to S2B
- LTE to S2B
- S2B to LTE
- S2A to LTE

**Important:** LTE to S2A Handoff is intentionally NOT mentioned here as P-CSCF IE is not supported for this Handoff.

**New Behavior:** If P-CSCF address information is already missing, then the P-GW initiates P-CSCF Discovery to resolve the P-CSCF address after the following inter-tech handoff scenarios.

- eHRPD to S2B
- LTE to S2B
- S2B to LTE
- S2A to LTE

**Important**: LTE to S2A Handoff is intentionally NOT mentioned here as P-CSCF IE is not supported for this Handoff.

**Important**: P-CSCF Discovery for GnGp Handoff is not supported as part of ID CSCuq19244.

**CSCuq50437 - absolute timer truncated on MSB causing premature disconnects**

**Feature Changes**

**Absolute Timer Truncated on MSB Causing Premature Disconnects**

**Previous Behavior**: The maximum supported session timeout value was previously set to 49 days and 17 hours.

**New Behavior**: The maximum supported session timeout value has been extended to 12725 days and 19 hours.

**Customer Impact**: Customers may now set a greater session timeout value without the timeout value being truncated due to a counter overflow.
Chapter 17
PSF Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from PSF in StarOS 17 software releases.
PSF Enhancements for 17.1

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.

CSCup77524 - Pkts not reaching isp when junk policy configured for uplink protection

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

**Feature Changes**

**Uplink Protection Support**

**Previous Behavior:** When an unknown (junk) policy is defined for uplink protection, packets are not sent out.

**New Behavior:** When junk policy is configured for uplink protection, packets are sent out and the `show config errors` command displays the errors.
PSF Enhancements for 17.0

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.

CSCuc83562 - [SFW] Need a way to make PPTP work without PPTP Analyser

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

**Feature Changes**

**PPTP Traffic**

When NAT is disabled, there is no need for a PPTP analyzer to be configured. Since PPTP analyzer tagged GRE flows as 5-tuple, GRE flows were not passed through ASR5x00. As part of this enhancement, a rule is configured to allow all GRE traffic using ruledefs. Hence, while NAT is disabled and PPTP analyzer is not configured, GRE flows will be tagged as 3-tuple and flows will not be dropped.

PPTP analyzer is a must for PPTP to work with NAT.

Backward compatibility is provided in this release to tag GRE flows as 5-tuple when PPTP analyzer is present, and must be tagged as 3-tuple in the absence of PPTP analyzer.

**Customer Impact:** The user can allow PPTP traffic without performing DPI.

CSCue68175, CSCua99869 - Firewall changes for Radius policy support in Gx

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

**Feature Changes**

**Firewall Policy via Gx**

**Previous Behavior:** Firewall Policy via RADIUS and Gy is supported at call setup and also during mid-session.

**New Behavior:** Support for Firewall Policy via Gx is provided in this release. Recovery and ICSR is also supported for the new policy being received via Gx. Firewall-and-NAT Policy can be applied at the initial call setup and also during mid-session policy updates/changes.

The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the Firewall-and-NAT policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in...
Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the Firewall-and-NAT policy that is currently assigned to the PDP context.

**Customer Impact:** The user can now use PCRF for controlling Firewall Policies.

### CSCuf30336 - fw-and-nat policy ID checkpointing to peer chassis

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

**Feature Changes**

**Firewall-and-NAT Policy ID Checkpointing**

In this release, the Firewall-and-NAT Policy ID can be used for checkpointing. In earlier releases, the “Policy-name” is checkpointed to peer-chassis. Backward compatibility must be provided to support checkpointing to peer-chassis.

### CSCug91538, CSCug91568 - Move sfw/nat info to ‘show active-charging subscribers ....’

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

**Feature Changes**

**Firewall/NAT Statistics Support**

In this release, the statistics related to Firewall/NAT for multiple sub-sessions earlier displayed as part of the `show active-charging sessions full all` command will now be available as part of the `show active-charging subscribers full all` command. This can avoid displaying the same information for multiple sub-sessions in the `show active-charging sessions full all` command.

**Previous Behavior:** The `show active-charging sessions full all` displayed the Firewall/NAT specific attributes.

**New Behavior:** The `show active charging subscribers full all` CLI command is enhanced to display Firewall/NAT specific attributes at subscriber level. When data is sent, the packets that match specific ruledefs only are displayed.

**Performance Indicator Changes**

**show active-charging subscribers full all**

This is a new command in this release displaying the following statistics earlier displayed as part of the `show active-charging sessions full all` command.

- FW-and-NAT Policy
- FW-and-NAT Policy ID
- Firewall Policy IPv4
- Firewall Policy IPv6
- NAT Policy NAT44
- NAT Policy NAT64
- Bypass NAT Flow Present
- No Firewall ruledef(s) match the specified criteria
- No Default Firewall ruledef(s) match the specified criteria
- Predefined Firewall Rules Enabled List

**CSCuh60799 - Remove memory fair usage feature**

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

Feature Changes

Memory Fair Usage Feature

The Memory Fair Usage feature has been deprecated in this release and is no longer supported.

**CSCul71133 - Merge all the uplink firewall feature enabling to single CLI**

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

Feature Changes

Uplink Firewall Support

Enabling the uplink flooding, port-scan and IP-sweep features has been changed in this release.

**Previous Behavior:** The uplink flooding, port-scan and IP-sweep features were enabled through separate CLIs in the ACS Configuration mode.

**New Behavior:** Enabling the uplink flooding, port-scan and IP-sweep features must be made in a Firewall-and-NAT Policy that has to be configured in the ACS Configuration mode.

The following CLIs in the ACS Configuration mode that are duplicate Firewall-and-NAT Policy CLIs will be concealed. Backward compatibility is provided to support the previous behavior and configuration.

- firewall dos-protection flooding
- firewall dos-protection ip-sweep
- firewall dos-protection port-scan
CSCum02425 - Total DOS Attacks counter not to be updated for NAT only enabled

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

Feature Changes

DoS Attacks Counter

When FW-and-NAT policy had only NAT configured without Firewall enabled, NAT drops were seen and these drops were reported as DOS attacks in the show active-charging firewall statistics command meant for Firewall functionality. With this enhancement, the DoS Attacks counter will not be incremented for NAT-only calls.

Previous Behavior: The “Total DOS Attacks” counter in show active-charging firewall statistics command was displayed for NAT-only enabled calls.

New Behavior: The “Total DOS Attacks” counter will not be incremented for NAT-only enabled calls. Malformed packets and header error packets will still get dropped, but will not get incremented in DOS Attacks counter.

CSCum40056 - SFW/NAT changes for IPv6 IPSG

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

Feature Changes

Firewall/NAT Support for IPv6 IPSG

Previous Behavior: IPv6 was not supported by IPSG in earlier releases.

New Behavior: In this release, IPv6 IPSG supports Firewall and NAT.
Chapter 18
SAEGW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from SAEGW in StarOS 17 software releases.
SAEGW Enhancements for 17.5

There are no SAEGW enhancements for this release.
SAEGW Enhancements for 17.4

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

---

**CSCuu31324 - Idle subscribers not being cleared from SPGW**

**Applicable Products:** SAEGW

**Idle Subscribers Cleared Properly**

Some subscribers were not being cleared if a suspend notification was received on the call and before receiving the resume notification the 4G call receives an MBR or UPC (for a 4G-to-3G handoff).

**Previous Behavior:** If in 4G a UE went to the suspended state, the idle timer was not restarted if an MBR or UPC (for a Gn/Gp handoff) was received before the resume notification. This resulted in some idle subscribers not being cleared.

**New Behavior:** If in 4G a UE goes to the suspended state, the idle timer is restarted if an MBR or UPC (for Gn/Gp handoff) is received before the resume notification.

Idle subscribers are now cleared properly.
SAEGW Enhancements for 17.3

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

---

**CSCuu31324 - Idle subscribers not being cleared from SPGW**

**Applicable Products**: SAEGW

**Feature Changes**

**Idle Subscribers Cleared Properly**

Some subscribers were not being cleared if a suspend notification was received on the call and before receiving the resume notification the 4G call receives an MBR or UPC (for a 4G-to-3G handoff).

**Previous Behavior**: If in 4G a UE went to the suspended state, the idle timer was not restarted if an MBR or UPC (for a Gn/Gp handoff) was received before the resume notification. This resulted in some idle subscribers not being cleared.

**New Behavior**: If in 4G a UE goes to the suspended state, the idle timer is restarted if an MBR or UPC (for Gn/Gp handoff) is received before the resume notification.

Idle subscribers are now cleared properly.
SAEGW Enhancements for 17.3

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

CSCuu31324 - Idle subscribers not being cleared from SPGW

**Applicable Products:** SAEGW

**Feature Changes**

**Behavior Change Due to Implementation of Fix for CSCuu31324**

Some subscribers were not being cleared if a suspend notification was received on the call and before receiving the resume notification the 4G call receives an MBR or UPC (for a 4G-to-3G handoff).

**Previous Behavior:** If in 4G a UE went to the suspended state, the idle timer was not restarted if an MBR or UPC (for Gn/Gp handoff) was received before the resume notification. This resulted in some idle subscribers not being cleared.

**New Behavior:** If in 4G a UE goes to the suspended state, the idle timer is restarted if an MBR or UPC (for Gn/Gp handoff) is received before the resume notification.

Idle subscribers are now cleared properly.
CSCuu37427 - Assertion failure
egtpc_handle_create_sess_req_msg_at_sgw_ingress

Applicable Products: SAEGW

Feature Changes

Behavior Change Due to Implementation of Fix for CSCuu37427

The fix implemented for CSCuu37427 has resulted in a behavior change.

**Previous Behavior:** When two parallel CSReqs with different ebi and 0 TEID were received from the S4-SGSN, the second CSReq was rejected with cause "No Resource Available."

**New Behavior:** When two parallel CSReqs with different ebi and 0 TEID are received from S4-SGSN, both of the CSReqs are processed and the PDNs are created successfully.

**Customer Impact:**

1. Operators will see that both the PDNs are created successfully after the fix if the two CSReqs are received from S4-SGSN with 0 TEID and different ebi.
2. If both PDNs are received from the MME then the old behaviour of rejecting the CSReq with cause "No Resource Available" is applicable.
3. If one CSReq is received from the MME and the other from the S4-SGSN, or vice-versa, with the same or different ebi, then context replacement is triggered and the second CSReq replaces the existing PDN with a new PDN.
SAEGW Enhancements for 17.2

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.

---

**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

---

**CSCur22641 - QoS Enforcement Issue using GxR10 During IRAT**

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

**Feature Changes**

**QoS Enforcement Issue using GxR10 During IRAT**

Previously, during GnGp handoff the SGSN was incapable of communicating the last authorized ARP (PV and PC) values to the MME. In this case, the MME tried to query the P-GW to get the last authorized ARP. Neither the PCRF nor the P-GW replied with the last authorized value to the MME. Therefore, the MME applied the subscribed ARP values from the HSS which was different from the last authorized value. This cause the P-GW and the MME to go out of sync on ARP.

**Previous Behavior:** Previously, the UB request for MBC contained the last negotiated APN AMBR after GnGp handoff if the PCRF was not reachable. The UB request for MBC contained the last authorized APN AMBR if the
PCRF provided an APN AMBR after GnGp. The default EPS bearer QoS was not addressed as part of the `egtp modify-bearer-cmd-negotiate-qos` CLI command.

**New Behavior:** The UB request for MBC contains the last negotiated APN AMBR after GnGp if the PCRF is not reachable and the UB request for MBC contains the last authorized APN AMBR if the PCRF provides an APN AMBR after GnGp. This change sends the last authorized DEBQ in UB request if:

- the UB request is triggered by MBC
- the MBC requested a DEBQ
- the requested DEBQ is different than the current authorized value
- the PCRF is configured and if does not provide DEBQ
- `egtp modify-bearer-cmd-negotiate-qos` is configured under P-GW service

### CSCur61470 - S2B Support on SAE-GW

**Applicable Products:** SAEGW

**Feature Changes**

### GTP-based S2b Interface Support on the SAEGW

**Important:** GTP-based S2b Interface Support on the SAEGW is currently supported as lab quality only. Full support for this feature is planned for a future release.

GTP-based S2b interface support has been implemented on the SAEGW. The S2b interface connects the SAEGW with the ePDG. The access types supported are:

- 4G
- Wifi

GTP-based S2b interface support on the SAEGW supports the following features:

- Basic WIFI call over SAEGW service
- Collapsed LTE call to WiFi handover
- WiFi to collapsed LTE Call handover
- WiFi to LTE handover success
- LTE to WiFi handover success
- Context replacement from LTE (SAEGW S+P) for ongoing WiFi call
- Context replacement for WiFi call with SAEGW collapsed call
- Multi-PDN cases are supported, but not Multi-PDN cases for the same APN
- Support of all the above cases for IPv4, IPv6 and IPv4v6 addresses
Performance Indicator Changes

SAEGW Schema

The following bulk statistics have been added to the SAEGW schema to support the GTP-based S2B interface implementation on the SAEGW:

- pgw-handoverstat-s2bgtptoleatt
- pgw-handoverstat-s2bgtptoltesucc
- pgw-handoverstat-s2bgtptoltefail
- pgw-handoverstat-ltetosltpatt
- pgw-handoverstat-ltetosltpsucc
- pgw-handoverstat-ltetosltpfail

show saegw-service statistics all

The output of this command provides statistics related to successes, failures and attempts for various S2bGTP handovers for all P-GW SAEGW services.

- S2bGTP-to-LTE handover:
  - Attempted
  - Succeeded
  - Failed
- LTE-to-S2bGTP handover:
  - Attempted
  - Succeeded
  - Failed

show subscribers saegw-only full all

This command provides S2b call-related information for P-GW subscribers.

- Access Tech:
- Interface Type:
- Access Point MAC Address
- sgw-c-teid
- ePDG c-teid
- sgw c-addr
- ePDG c-addr
- sgw u-teid
- ePDG u-teid
- sgw u-addr
• ePDG u-addr
SAEGW Enhancements for 17.1

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

---

**CSCuh06473, CSCul42763, CSCuq23971 - Cause IE enhancement for Delete Bearer Request**

**Feature Changes**

**Cause IE enhancement for Delete Bearer Request**

Cause value in the Delete Bearer Request has been limited. The behavior impacted by this feature is:

- Delete Bearer Request/Delete PDP Context due to idle-timer/session-timer expiration
- Delete Bearer Request due to bearer inactivity of default bearer
- Delete PDP Context due to bearer inactivity of the last PDP context of PDN connection
- Delete Bearer Request/Delete PDP Context triggered by `clear subscriber` CLI command

Configuration has been added to set cause values and cause inclusion in the following scenarios:
• CLI-based trigger to disconnect
• per APN when P-GW initiated disconnection for above mentioned timer expiry

**Important:** Cause IE Enhancement for Delete Bearer Request is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

### Previous Behavior:

1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, its cause-IE is not configurable.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, its cause-IE is not configurable.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, its cause-IE is not configurable.

### New Behavior:

1. When GGSN/P-GW/SAEGW sends Delete Bearer Request/Delete PDP Context Request due to CLI `clear subscribers`, the cause-IE to be used may optionally be specified by the operator in CLI. The CLI also allows the operator not to include cause-IE.
2. When P-GW/SAEGW sends Delete Bearer Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” of default bearer, the cause-IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.
3. When GGSN sends Delete PDP Context Request due to “timeout-idle”, “timeout absolute”, or “timeout bearer-inactivity” to delete the PDN Connection, the cause IE to be used may optionally be specified by the operator during configuration. The configuration also allows the operator not to include cause-IE.

**Customer Impact:** Cause-Code during PDN connection teardown may be modified.

**Important:** This feature allows operator to override existing behavior. Such overridden behavior may not be compliant with standards.

### Command Changes

#### clear subscribers

When subscribers are deleted, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword `del-cause` is optional and can be combined with existing options to modify “Cause-IE” behavior.

```
clear subscribers all [ del-cause { reactiv-req | none } ] [ verbose ] [ -noconfirm ]
clear subscribers apn apn_name [ del-cause { reactiv-req | none } ] [ verbose ] [ -noconfirm ]
```

**Notes:**

- `del-cause`: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests generated for default bearer.
- `reactiv-req`: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.
- `none`: Omit GTP cause IE in DBR/DPC generated for default bearer.
• The new behavior for Cause-IE will be effective only if the clear subscribers CLI results in the sending of a Delete Bearer Request for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

• The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

timeout

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword del-cause is optional and can be combined with existing options to modify “Cause-IE” behavior.

configure

context context_name

  apn apn_name

    timeout absolute time [ del-cause { reactiv-req | none } ]

    { default | no } timeout absolute del-cause

end

Notes:
• del-cause: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.

• reactiv-req: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.

• none: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.

• By default, the del-cause option is not defined and existing behavior is retained.

• The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

• The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

timeout bearer-inactivity

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword del-cause is optional and can be combined with existing options to modify “Cause-IE” behavior.

configure

context context_name

  apn apn_name

    timeout bearer-inactivity del-cause { reactiv-req | none }

    { default | no } timeout bearer-inactivity del-cause

end

Notes:
• **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.

• **reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.

• **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.

• By default, the **del-cause** option is not defined and existing behavior is retained.

• The new behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

• The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**timeout idle**

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include “Cause-IE” in the resulting Delete Bearer Request/Delete PDP Context messages for default bearer. The new keyword **del-cause** is optional and can be combined with existing options to modify “Cause-IE” behavior.

```plaintext
command
context context_name

  apn apn_name

  timeout idle idle_dur [ del-cause { reactiv-req | none } ]

  { default | no } timeout idle del-cause

end
```

Notes:

• **del-cause**: Specifies the GTP cause code used in Delete Bearer/Delete PDP Context Requests when timeout occurs on default bearer.

• **del-cause reactiv-req**: The DBR/DPC will include “Cause-IE” with GTP cause code “Reactivation Requested”.

• **none**: Omit GTP cause IE in DBR/DPC when timeout occurs on default bearer.

• By default, the **del-cause** option is not defined and existing behavior is retained.

• The new behavior is applicable only if Delete Bearer Request is sent for Default Bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

• The new behavior for Cause-IE given in this CLI shall override the cause-code set by existing features.

**CSCup59406 - sesstrc task in over state during longevity/aggravator run**

**Feature Changes**

**Configuring Session Trace File Type**
To address the issues caused when the sesstrc task allocates memory over the allotted limit, under a random subscriber session trace load tests on P-GW/S-GW, support for B-type XML files is introduced in addition to the A-type files already supported.

**Previous Behavior:** The file type was A-type XML file and the type could not be changed.

**New Behavior:** The CLI has been modified (see Command Changes section) to allow the operator to select the file type generated by session trace. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. Each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

### Command Changes

```
session trace network-element
```

The new `file-type` keyword enables the operator to determine which type of XML file is generated by the session trace:

```
configure

    session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw } [ file-type { a-type | b-type } ] [ collection-timer | tce-mode ]

    no session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw }

end
```

**Notes:**

- Default file-type is `a-type`.
- To keep the syntax simple, we recommend that you enter the `file-type` keyword prior to adding either of the other optional keywords to the command.
- To modify the session trace network-element configuration, you must first enter the `no session trace network-element` form of the command to remove the session trace configuration.

### CSCur43509 - 17.1: MLF-3298: PCEF is not triggering 29 as APN-AMBR mod failure in CCR

#### Feature Changes

**APN AMBR Modification Failure Event Trigger Support for all Usage Report Trigger Values**

The fix implemented for CSCur43509 has resulted in a behavior change.

**Previous Behavior:** When diameter map usage-report is 26 then APN AMBR modification failure event trigger was not supported.

**New Behavior:** APN AMBR modification failure event trigger is supported for all usage report trigger values (26,33,29).

**Customer Impact:** This affects all Gx/Gxx products.
SAEGW Enhancements for 17.0

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

---

**CSCuh24813 - InTracer Support: Auto and more simultaneous traces - SAEGW**

**Feature Changes**

**InTracer Support for Auto-next-call and More Configurable Traces on the SAEGW**

The SAEGW has been enhanced to activate or De-activate a Signaling session trace. On activation, parameters pertaining to the specific trace are available to the InTracer application from the signaling messages. The following trace combinations are supported:

- Management
- Signaling
- Random
- Management and Random
• Management and Signaling

**CSCum17434 - AAA provide Restoration Priority Indicator to PGW**

**Feature Changes**

**AAA Restoration Priority Indicator**

As part of the implementation for CSCum17434, counters and bulk statistics have been added on the SAEGW. For a complete description of the AAA Restoration Priority Indicator feature, refer to the P-GW Enhancements chapter in this release note.

**Performance Indicator Changes**

**SAEGW Schema**

The following bulk statistics have been added to support the AAA Restoration Priority Indicator on the SAEGW.

- pgw-pdns-restore-priority-1
- pgw-pdns-restore-priority-2
- pgw-pdns-restore-priority-3
- pgw-pdns-restore-priority-4
- pgw-pdns-restore-priority-5
- pgw-pdns-restore-priority-6
- pgw-pdns-restore-priority-7
- pgw-pdns-restore-priority-8
- ggsn-pdns-restore-priority-1
- ggsn-pdns-restore-priority-2
- ggsn-pdns-restore-priority-3
- ggsn-pdns-restore-priority-4
- ggsn-pdns-restore-priority-5
- ggsn-pdns-restore-priority-6
- ggsn-pdns-restore-priority-7
- ggsn-pdns-restore-priority-8

**Important:** The **pgw-pdns** counts will be incremented for both pure P and co-located calls located at the SAEGW. The **ggsn-pdns** counts will be incremented for GGSN calls located at the SAEGW.

**show subscribers saegw-only full all**

The output of this command has been enhanced to show the restoration priority level
• Restoration Priority level: <1 to 8>

CSCum93697 - Per QCI data stats for collocated S&P calls

Feature Changes

Per QCI Data Statistics for Co-located Calls on the SAEGW

New counters and bulk statistics have been introduced for SAE-GW collapsed calls

Performance Indicator Changes

SAEGW Schema

The following bulk statistics have been added to support Per QCI Data Statistics for Co-located Calls on the SAEGW

• collapsed-subdatastat-ulpktfwd-qci1
• collapsed-subdatastat-ulpktfwd-qci2
• collapsed-subdatastat-ulpktfwd-qci3
• collapsed-subdatastat-ulpktfwd-qci4
• collapsed-subdatastat-ulpktfwd-qci5
• collapsed-subdatastat-ulpktfwd-qci6
• collapsed-subdatastat-ulpktfwd-qci7
• collapsed-subdatastat-ulpktfwd-qci8
• collapsed-subdatastat-ulpktfwd-qci9
• collapsed-subdatastat-ulbytefwd-qci1
• collapsed-subdatastat-ulbytefwd-qci2
• collapsed-subdatastat-ulbytefwd-qci3
• collapsed-subdatastat-ulbytefwd-qci4
• collapsed-subdatastat-ulbytefwd-qci5
• collapsed-subdatastat-ulbytefwd-qci6
• collapsed-subdatastat-ulbytefwd-qci7
• collapsed-subdatastat-ulbytefwd-qci8
• collapsed-subdatastat-ulbytefwd-qci9
• collapsed-subdatastat-dlpktfwd-qci1
• collapsed-subdatastat-dlpktfwd-qci2
• collapsed-subdatastat-dlpktfwd-qci3
• collapsed-subdatastat-dlpktfwd-qci4
- collapsed-subdatastat-dlpktfwd-qci5
- collapsed-subdatastat-dlpktfwd-qci6
- collapsed-subdatastat-dlpktfwd-qci7
- collapsed-subdatastat-dlpktfwd-qci8
- collapsed-subdatastat-dlpktfwd-qci9
- collapsed-subdatastat-dlbytefwd-qci1
- collapsed-subdatastat-dlbytefwd-qci2
- collapsed-subdatastat-dlbytefwd-qci3
- collapsed-subdatastat-dlbytefwd-qci4
- collapsed-subdatastat-dlbytefwd-qci5
- collapsed-subdatastat-dlbytefwd-qci6
- collapsed-subdatastat-dlbytefwd-qci7
- collapsed-subdatastat-dlbytefwd-qci8
- collapsed-subdatastat-dlbytefwd-qci9
- collapsed-subdatastat-ulpktdrop-qci1
- collapsed-subdatastat-ulpktdrop-qci2
- collapsed-subdatastat-ulpktdrop-qci3
- collapsed-subdatastat-ulpktdrop-qci4
- collapsed-subdatastat-ulpktdrop-qci5
- collapsed-subdatastat-ulpktdrop-qci6
- collapsed-subdatastat-ulpktdrop-qci7
- collapsed-subdatastat-ulpktdrop-qci8
- collapsed-subdatastat-ulpktdrop-qci9
- collapsed-subdatastat-ulbytedrop-qci1
- collapsed-subdatastat-ulbytedrop-qci2
- collapsed-subdatastat-ulbytedrop-qci3
- collapsed-subdatastat-ulbytedrop-qci4
- collapsed-subdatastat-ulbytedrop-qci5
- collapsed-subdatastat-ulbytedrop-qci6
- collapsed-subdatastat-ulbytedrop-qci7
- collapsed-subdatastat-ulbytedrop-qci8
- collapsed-subdatastat-ulbytedrop-qci9
- collapsed-subdatastat-dlpktdrop-qci1
- collapsed-subdatastat-dlpktdrop-qci2
• collapsed-subdatastat-dlpktdrop-qci3
• collapsed-subdatastat-dlpktdrop-qci4
• collapsed-subdatastat-dlpktdrop-qci5
• collapsed-subdatastat-dlpktdrop-qci6
• collapsed-subdatastat-dlpktdrop-qci7
• collapsed-subdatastat-dlpktdrop-qci8
• collapsed-subdatastat-dlpktdrop-qci9
• collapsed-subdatastat-dlbytedrop-qci1
• collapsed-subdatastat-dlbytedrop-qci2
• collapsed-subdatastat-dlbytedrop-qci3
• collapsed-subdatastat-dlbytedrop-qci4
• collapsed-subdatastat-dlbytedrop-qci5
• collapsed-subdatastat-dlbytedrop-qci6
• collapsed-subdatastat-dlbytedrop-qci7
• collapsed-subdatastat-dlbytedrop-qci8
• collapsed-subdatastat-dlbytedrop-qci9
• collapsed-subqosstat-bearact-qci1
• collapsed-subqosstat-bearact-qci2
• collapsed-subqosstat-bearact-qci3
• collapsed-subqosstat-bearact-qci4
• collapsed-subqosstat-bearact-qci5
• collapsed-subqosstat-bearact-qci6
• collapsed-subqosstat-bearact-qci7
• collapsed-subqosstat-bearact-qci8
• collapsed-subqosstat-bearact-qci9
• collapsed-subqosstat-bearset-qci1
• collapsed-subqosstat-bearset-qci2
• collapsed-subqosstat-bearset-qci3
• collapsed-subqosstat-bearset-qci4
• collapsed-subqosstat-bearset-qci5
• collapsed-subqosstat-bearset-qci6
• collapsed-subqosstat-bearset-qci7
• collapsed-subqosstat-bearset-qci8
• collapsed-subqosstat-bearset-qci9
- collapsed-subqosstat-bearrel-qci1
- collapsed-subqosstat-bearrel-qci2
- collapsed-subqosstat-bearrel-qci3
- collapsed-subqosstat-bearrel-qci4
- collapsed-subqosstat-bearrel-qci5
- collapsed-subqosstat-bearrel-qci6
- collapsed-subqosstat-bearrel-qci7
- collapsed-subqosstat-bearrel-qci8
- collapsed-subqosstat-bearrel-qci9

**show saegw-service statistics all**

The following new output fields have been added to this command to support Per QCI Data Statistics for Co-located Calls on the SAEGW.

- Colocated QCI Stats
- Bearers by QoS characteristics
  - Std QCI (Non-GBR)
    - Active
    - Setup
    - Released
  - Std QCI (GBR)
    - Active
    - Setup
    - Released
- Data Statistics by QoS Characteristics
- Uplink
  - Total Pkts
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Bytes
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Dropped Pkts
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Dropped Bytes
- Std QCI (Non-GBR)
- Std QCI (GBR)

- Downlink
  - Total Pkts
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Bytes
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Dropped Pkts
  - Std QCI (Non-GBR)
  - Std QCI (GBR)
  - Total Dropped Bytes
  - Std QCI (Non-GBR)
  - Std QCI (GBR)

**show saegw-service statistics all verbose**

The following new output fields have been added to this command to support Per QCI Data Statistics for Co-located Calls on the SAEGW.

- Uplink
- Packets
  - QCI 1
  - QCI 2
  - QCI 3
  - QCI 4
  - QCI 5
  - QCI6
  - QCI 7
  - QCI 8
  - QCI 9
  - Non-Std QCI

- Bytes
  - QCI 1
  - QCI 2
  - QCI 3
- QCI 4
- QCI 5
- QCI 6
- QCI 7
- QCI 8
- QCI 9
- Non-Std QCI

  - Dropped Packets
    - QCI 1
    - QCI 2
    - QCI 3
    - QCI 4
    - QCI 5
    - QCI 6
    - QCI 7
    - QCI 8
    - QCI 9
    - Non-Std QCI

  - Dropped Bytes
    - QCI 1
    - QCI 2
    - QCI 3
    - QCI 4
    - QCI 5
    - QCI 6
    - QCI 7
    - QCI 8
    - QCI 9
    - Non-Std QCI

- Downlink
- Packets
  - QCI 1
  - QCI 2
  - QCI 3
• QCI 4
• QCI 5
• QCI6
• QCI 7
• QCI 8
• QCI 9
• Non-Std QCI

• Bytes
  • QCI 1
  • QCI 2
  • QCI 3
  • QCI 4
  • QCI 5
  • QCI6
  • QCI 7
  • QCI 8
  • QCI 9
  • Non-Std QCI

• Dropped Packets
  • QCI 1
  • QCI 2
  • QCI 3
  • QCI 4
  • QCI 5
  • QCI6
  • QCI 7
  • QCI 8
  • QCI 9
  • Non-Std QCI

• Dropped Bytes
  • QCI 1
  • QCI 2
  • QCI 3
  • QCI 4
Feature Changes

Modification to MBR Collision Procedure

When the S5/S8 interface detected a collision between already initiated Create Bearer Request and newly incoming Modify Bearer Request, the Create Bearer Request was aborted at the P-GW. This resulted in any later Create Bearer Response received from the MME/SGW to be rejected. As an impact SAEGW/PGW had one bearer less than the peer. The software has been modified to resolve this problem, and has resulted in a behavior change:

**Previous Behavior:** Create Bearer Request aborted on Modify Bearer Request. Create Bearer Response ignored in Modify Bearer Pending state.

**New Behavior:** Create Bearer Request is not aborted on Modify Bearer Request. Create Bearer Response will abort the Modify Bearer Pending state, and re-transmit after Modify Bearer Response.

Feature Changes

Formulation of P-CSCF Address Output as Part of show sub full all

**Formulation of P-CSCF Address Output as Part of show sub full all**

Simplified the P-CSCF Address Output as part of show sub full all output. The P-CSCF discovery mode specific information is SR/GR recovered.

**Previous Behavior:** Previously, the P-CSCF Address Output displayed the P-CSCF Address information separately for S6b based FQDN and for Radius or configured scenarios. It also restricted the S6b mode to only display the IPv6 Address Information. IPv4 information was not being displayed. Also, the earlier output did not support persistence across ICSR/Session Recovery for all the discovery modes.

**New Behavior:** In the new output, a "Discovery Mode" field specifies the method of discovery followed by the actual P-CSCF Address Information. Also, the new Output displays both IPv4 and IPv6 address information as per applicability. The new Output remains persistent across ICSR/Session Recovery for all P-CSCF discovery modes.
CSCup89193 - SGW Access peer profile should be reflected in show output

Feature Changes

Enhancement to show subscribers CLI Output

The output of the `show subscriber saegw full all` command has been enhanced.

**Previous Behavior:** No `SGW Access` field was not available in the command output.

**New Behavior:** The `SGW Access` field is now added in the peer-profile section of the command output.

CSCup97222 - Wrong Termination-Cause sent in CCR over Gx for ims default bearer

Feature Changes

Enhancement to show subscriber saegw full

As part of the fix for CSCup97222, the output of the `show subscriber saegw full` command has been enhanced.

Performance Indicator Changes

**show subscriber saegw full**

Two fields have been added to the output of this command to indicate if session Auto Delete is enabled, and to indicate the percentage of the total number of sessions that have been auto-deleted.

- Auto Delete: Yes/No
- Disconnect Reason
  - session-auto-delete       Num | Disc Percentage

CSCuq46858 - NPLI: UBReq not triggered by PGW, when PCRF requests for ULI in RAR

Feature Changes

Enhancement to show subscriber saegw full

The fix for CSCuq46858 has resulted in a behavior change.

**Previous Behavior:** When there was no change in QoS and the P-GW received a RAR, a successful BBRsp was sent without generating a UBreq towards the S-GW.

**New Behavior:** If the PCRF request is for NPLI information only and there is no change in QoS, a UBReq is generated towards the S-GW.
Chapter 19
SaMOG Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from SaMOG in StarOS 17 software releases.
SaMOG Enhancements for 17.0

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 *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 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

---

**CSCug60305, CSCup63789 - Pseudonym/Fast reauth NAI support on SaMOG**

**Feature Changes**

**SaMOG Support for Pseudonym and Fast Re-authentication NAI**

In earlier releases, SaMOG provided support for the root Network Access Identifier (NAI), decorated NAI, and emergency NAI formats shared by the user equipment (UE) with SaMOG during initial network authentication. With this release, SaMOG extends support for pseudonym NAI and fast re-authentication NAI formats.

**Pseudonym NAI:** The pseudonym NAI is a temporary identity provided to a user by the AAA server that the subscriber uses while connecting to the network. This enables the subscriber to connect and authenticate without revealing its IMSI information on the network. The AAA server maintains a mapping between the real identity and the pseudonym NAI of the subscriber and uses the mapping to identify the subscriber.

**Fast Re-authentication NAI:** Where the AAA server supports fast re-authentication, the AAA server assigns an identity to the subscriber which is used by the subscriber's UE to initiate a re-attach or re-authentication. This
authentication method is faster than the full re-authentication method as the AAA server and UE use the authentication key from a previous full authentication. The UE sends the assigned fast re-authentication NAI for subsequent authentication attempts, and the AAA server looks up the mapping between the fast re-authentication NAI and the identity of the subscriber.

**Command Changes**

dictionary

In support of this feature, a new `dictionary` keyword has been introduced to enable the SaMOG service to forward the permanent identity of the subscriber to the AAA server.

```bash
configure
  context context_name
    twan-profile twan_profile_name
      radius client { ipv4/ipv6_address[/mask ] } [ encrypted ] key value [ disconnect-message [ dest-port destination_port_number ] ] [ dictionary { custom70 | custom71 } ]
    end
end
```

Notes:
- Default: custom70

The dictionary can also be configured at the TWAN profile level using the new `dictionary` CLI command. The configured dictionary at this level will be applied to all Radius clients belonging to that TWAN profile.

```bash
configure
  context context_name
    twan-profile twan_profile_name
      default dictionary
        dictionary { custom70 | custom71 }
    end
end
```

**Performance Indicator Changes**

`show twan-profile`

The following field has been introduced under the Radius Client List and Access-Type Client List sections of the `show twan-profile` command:

TWAN Profile Name
- Radius Client List
- Dictionary
• Access-Type Client List
  • Default Radius Dictionary

**show samog-service statistics**

The following field has been introduced to the output of the `show samog-service statistics` command to display the number of Access-Requests dropped due to non-availability of matching PLMN based local policy:

• No Policy Match

**CSCug95466, CSCum36863, CSCum36878, CSCum42124, CSCup84932 - Support Webauth on SaMOG GW**

**Feature Changes**

**SaMOG Web Authorization**

This feature enables SaMOG to authenticate user equipments (UE) over a web portal (based on a user ID and password), instead of an EAP-SIM, EAP-AKA, or EAP-AKA' authorization and connect the subscriber based on the IMSI profile. This authentication method can be performed on any non-SIM based devices or UEs that do not support EAP-SIM, EAP-AKA, or EAP-AKA' based authorization. SaMOG performs web authorization using the Enhanced Charging Services (ECS).

SaMOG performs web-based authorization in two phases:

**Pre-authentication Phase:** During this phase, SaMOG supports local IP address assignment and redirects the UE traffic to a web portal where the subscriber authenticates with a username and password. On successful authentication, the subscriber’s IMSI profile is associated with e MAC address of the UE and forwarded to the AAA server.

**Transparent Auto-logon Phase:** The subscriber profile is cached on the AAA server for a designated duration to enable subscribers to reconnect without further portal authentication, thus enabling a seamless user experience.

**License Requirements**

In support of the SaMOG Web Authorization feature, a separate SaMOG Web Authentication license has been introduced. This license comes bundled with the ECSv2 license.

**Important:** For more information on the SaMOG web authorization license, contact your Cisco account representative.

**Command Changes**

**apn**

In order to avoid overloading the `apn default-apn-profile` under the Operator Policy Configuration Mode with the web authorization configurations, a new `webauth-apn-profile` keyword has been introduced to enable operators to separately configure APN profiles dedicated to web authorization.
operator-policy { default | name policy_name }
apn webauth-apn-profile apn_profile_name
no apn webauth-apn-profile
end

active-charging rulebase
For web authorization, in order to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, the name of the rulebase that contains the charging action for the HTTP redirection and the URL for the portal can be configured under the APN Profile Configuration Mode using the following command:

configure
  apn-profile profile_name
    active-charging rulebase rulebase_name
    no active-charging rulebase
  end

dns
For web authorization, in order to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, the primary and secondary IP addresses of the DNS servers can be configured under the APN Profile Configuration Mode using the following command:

configure
  apn-profile profile_name
    [ no ] dns { primary | secondary } IPv4_address
  end

ip address pool name
For web authorization, in order to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, the IP pool name can be configured under the APN Profile Configuration Mode using the following command:

configure
  apn-profile profile_name
    [ no ] ip address pool name pool_name
  end

ip context-name
For web authorization, in order to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, the IP context name can be configured under the APN Profile Configuration Mode using the following command:

```
configure
apn-profile profile_name
   ip context-name context_name
   no ip context-name
   end
```

```
ip access-group
```

For web authorization, in order to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, the IP access group can be configured under the APN Profile Configuration Mode using the following command:

```
configure
apn-profile profile_name
   [ no ] ip access-group group_name [ in | out ]
   end
```

```
timeout
```

In support of the Web Authorization feature, the `timeout` command has been introduced under the Call Control Profile Configuration Mode to clear the cached MAC to IMSI mapping entry that was created during the pre-authentication phase if the entry is not cleared for more than the configured duration.

```
configure
call-control-profile profile_name
   timeout imsi cache timer_value
   { default | no } timeout imsi cache
   end
```

Notes:
- Default: 1440 minutes

```
subscriber
```

In support of the Web Authorization feature, the `subscriber` command has been introduced under the Call Control Profile Configuration Mode to specify if the Operator Policy permits multiple PDN connections for the same IMSI. This command can be used to permit or restrict the number of devices allowed for one subscriber.

```
configure
```
call-control-profile profile_name

    [ no ] subscriber multi-device

end

Notes:

- If the CLI is not configured, only one PDN connection is permitted per IMSI for a subscriber connecting through the Operator Policy.
- If enabled, a maximum of 11 PDN connections are allowed.

authenticate context

In support of the Web Authorization feature, the auth-method keyword has been introduced in the authenticate context command under the Call Control Profile Configuration Mode to specify the authentication method allowed.

call-control-profile profile_name

    authenticate context context_name auth-method [ eap ] [non-eap] 

end

configure

Notes:

- If the CLI is not configured, EAP-based authentication is selected for the Call Control Profile in the Operator Policy.

Performance Indicator Changes

SaMOG Schema

The following bulkstats have been introduced in support of the Web Authorization feature:

- cgw-sessstat-pdns-locally-terminated-active
- cgw-sessstat-pdns-locally-terminated-setup
- cgw-sessstat-pdns-locally-terminated-released
- cgw-sessstat-pdns-locally-terminated-rejected
- cgw-pre-auth-failure-ip-alloc
- mrme-non-eap-preauth-call-success
- mrme-non-eap-preauth-call-failure
- mrme-non-eap-aaa-call-success
- mrme-non-eap-aaa-call-failure
- mrme-non-eap-session-attempted
- mrme-non-eap-session-aaarejects
show samog-service statistics

The output of the `show samog-service statistics` command has been updated to display the following web authorization related counters:

Web Authorization Stats

- Pre-authentication Stats:
  - Success
  - Failure
  - AAA Disconnect with IMSI
  - AAA Disconnect without IMSI
  - AAA Disconnect timeout
- Transparent Auto-logon Stats:
  - Success
  - Failure
  - Abort
- PDNs Aborted By Reason:
  - IP Allocation Failure
  - Bearer Id allocation Failure

show subscribers samog-only full all

The output of the `show subscribers samog-only full all` command has been updated to display the following web authorization related counters:

- Network Access Mode: \{ EPC(GTPv2) | EPC(GTPv1) | Local-offload | HTTP redirect \}
- Web Authorization: \{ Yes | No \}
  - Web authorization phase: \{ pre-auth | TAL \}
  - IP pool name
  - IP context name
  - Rulebase Name
  - Access-list Name
  - Primary DNS Server Address
  - Secondary DNS Server Address

show apn-profile full

The output of the `show apn-profile full \{ all | name apn_profile_name \}` command has been updated to display the following web authorization related counters:

- SaMOG IP pool name
- SaMOG IP context name
- SaMOG Rulebase Name
- SaMOG Access-list Name
- SaMOG Primary DNS Server Address
- SaMOG Secondary DNS Server Address

**show call-control-profile full**

The output of the `show call-control-profile full { all | call_control_profile_name }` command has been updated to display the following web authorization related counters:

- MRME Authentication Method: {EAP | MAC | EAP, MAC}
- IMSI cache timeout(SaMOG)
- Multi device connection allowed

**show mrme-service active-session mac**

The `active-session mac mac_address` keyword has been introduced to the `show mrme-service` command to display the data stored in active session entry (if present) for the UE MAC address passed as input.

- Active Session Entry for UE MAC: <mac_address>
- Sessmgr Instance
- Allocated Call Id
- Username: <NAI or MAC>

**show mrme-service mac-sticky mac**

The `mac-sticky mac mac_address` keyword has been introduced to the `show mrme-service` command to display the UE MAC to IMSI mapping (if available) in the mapping table of the IPSGMGR.

- UE MAC: <mac_address>
- IMSI: <IMSI_value>

**show mrme-service imsi-sticky imsi**

The `imsi-sticky imsi imsi_value` keyword has been introduced to the `show mrme-service` command to display the IMSI to session manager mapping (if available) in the mapping table of the IPSGMGR.

- IMSI: <IMSI_number>
- SESSMGR Instance: <instance>

**CSCum35258 - AAA protocol agnostic GTP version support**

**Feature Changes**

**AAA Agnostic GTP Version Support**
In earlier releases, SaMOG made use of the Radius AAA interface to authenticate users in 3G networks, and the Diameter interface in 4G networks. With this release, SaMOG can be used to connect to P-GW or GGSN nodes independent of the AAA interface protocol. This enables operators upgrading from a 3G network to 4G network with a Radius based AAA infrastructure to authenticate 4G (EPC) subscribers and setup a 4G (GTPv2) session using SaMOG. Using the SaMOG general license, operators can now configure both A-AAAA and SNAPTR type DNS queries with a Radius based authentication, or a A-AAAA type DNS query with a Diameter based authentication.

CSCum35265 - Prepaid subscriber and Voucher support for LBO

Feature Changes

SaMOG Local Breakout Flow-based Support

With this release, SaMOG supports Flow-based Local Breakout (LBO) enabling time- and quota-based control to support prepaid subscribers. SaMOG interfaces with the Enhanced Charging Services (ECS) using the Gy interface for prepaid subscribers and AAA for voucher-based subscribers. Flow-based LBO is supported on both PMIPv6 and EoGRE access types.

When a GTP session with the local P-GW or GGSN is set up, the local P-GW or GGSN service communicates with ECS to obtain the time and quota limits of the subscriber by having the Gy interface forward the CCR-I message to the Diameter Credit Control Application (DCCA) server to establish connection. When the time or volume quota is reached, the local P-GW or GGSN forwards the CCR-U message to DCCA in order to refresh the permitted time or volume quota allowed.

SaMOG Local Breakout License Enhancement

The SaMOG LBO license has been enhanced by bundling the LBO license with the ECSv2 license to enable SaMOG to communicate with the ECS server in order to support prepaid subscribers.

Important: For more information on the SaMOG local breakout license, contact your Cisco account representative.

CSCum36839 - APN Local breakout support under SaMOG-3G license

Feature Changes

Support for Local Breakout on SaMOG 3G

The SaMOG Local Breakout feature was introduced in an earlier release to enable subscribers to access the Internet without having to connect to the EPC core. All subscribers of a particular APN are locally broken out with SaMOG performing IP allocation locally. This feature was limited to 4G (GTPv2) sessions only.

With this release, the SaMOG Local Breakout feature is extended to 3G (GTPv1) sessions where SaMOG associates GTPv1 calls with the internal GGSN service.

SaMOG Local Breakout License
The SaMOG Local Breakout license has been enhanced to support 3G subscribers. Operators with an SaMOG 3G license and a Local Breakout license can now configure the local breakout feature for 3G subscribers.

**Important:** For more information on the SaMOG local breakout license or SaMOG 3G licence, contact your Cisco account representative.

### Command Changes

**associate**

In support of the Local Breakout feature on SaMOG 3G sessions, the `ggsn-service` keyword has been introduced to the `associate` command under the CGW Service Configuration Mode to associate the configured GGSN service to the CGW service.

```
configure

  context context_name

    cgw-service cgw_service_name

    associate ggsn-service ggsn_service_name

    no associate ggsn-service

end
```

**Notes:**

- Use the `no associate ggsn-service` command to remove the association of the ggsn-service with the CGW service.

### Performance Indicator Changes

**show cgw-service all**

The output of the `show cgw-service all` command has been modified to display the name of the GGSN service associated with the CGW service.

- GGSN Service: `<ggsn_service_name>`

### CSCum42089 - Support for PGW fallback

### Feature Changes

**Fallback to Alternate PGW or GGSN**

This feature enables SaMOG to establish a session between the GTP interface and an alternate P-GW or GGSN when connection establishment fails towards the primary P-GW or GGSN (response timeout or localized issues). SaMOG
determines the alternate P-GW or GGSN IP address using the A/AAAA (Pre-release 8) or SNAPTR (Post-release 7) DNS procedure with the DNS server.

**CSCum79992 - Session disconnect reason needs to be changed for SSID change**

**Feature Changes**

**Change in SSID Change Session Disconnect Reason**

*Previous Behavior*: In earlier releases, during a reattach procedure by SaMOG due to an SSID change, the session disconnect reason for SaMOG call was “IPSG-session-replacement”.

*New Behavior*: With this release, the session disconnect reason has been changed to “samog-session-replacement”.

**CSCun58418 - [SAMOG] Flexibility to config to egress-egtp from diff context under CGW**

**Feature Changes**

**CGW Multi-Context Support**

With this release, multi-context support is available to enable operators to associate an egress EGTP service belonging to another context, with a CGW service. In combo services of SaMOG and P-GW/GGSN, the egress EGTP service can be made available in the same context as the P-GW/GGSN for routing traffic between the CGW and P-GW/GGSN.

**Command Changes**

```plaintext
dictionary

The `context` keyword has been introduced to associate the egress EGTP service belonging to another context with CGW.

configure

    context context_name

    cgw-service cgw_service_name

    associate egress-egtp-service egress_egtp_service [ context context_name ]

end
```
CSCup81813 - [SAMOG] ‘Unsupported NAI’ in EAP pkt should be changed to ‘Unknown NAI’

Feature Changes

Change to ‘Unsupported NAI’ Output Field

The SaMOG service recognizes the prefix IMSI, IMSI, IMEI, MAC, and Pseudonym NAI types in the EAP packets. SaMOG also forwards unknown NAI packets to the AAA server. In earlier releases, the “Unsupported NAI” counter in the output of the `show samog-service statistics` command gets incremented. With this release, the “Unsupported NAI” counter has been renamed to “Unknown NAI” as the label used in earlier releases was syntactically incorrect.
Chapter 20
SecGW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from SecGW StarOS 17 software releases.
SecGW Enhancements for 17.1

This section identifies all of the Security Gateway (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 bulkstat 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 SecGW.

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

**Important:** This is the FCS release of SecGW. For complete descriptions of SecGW functionality and features, see the *SecGW Administration Guide*.

**CSCui46785 - Need to target 40Gbps throughput performance for WSG on VSM SSI**

**Feature Changes**

**Four StarOS VMs per ASR 9000 VSM**

SecGW is enabled as a WSG service in a QvPC-VSM instance (StarOS VM). In previous releases, SecGW ran as a single StarOS VM across the four CPUs on the ASR 9000 VSM.

In this release, a single QvPC-VSM instance runs on each VSM CPU for a total of four QvPC-VSM instances per VSM. This new configuration provides substantially improved throughput.
The SecGW Administration Guide and QvPC-VSM System Administration Guide provide detailed information regarding the new four-VM configuration.
SecGW Enhancements for 17.0

This section identifies all of the Security Gateway (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 bulkstat 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 SecGW.

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

---

*Important:* This is the FCS release of SecGW. For complete descriptions of SecGW functionality and features, see the *SecGW Administration Guide*.

CSCtt22271 - RFC 4303 ESN

**Feature Changes**

**ESN for ikev2**

Every IKE message contains a Message ID (sequence number) as part of its fixed header. This sequence number is a monotonically increasing integer (incremented by 1 for every packet sent) used to match up requests and responses, and to identify retransmissions of messages. The sequence is a 32-bit integer which is zero for the first IKE request in each direction.
RFC 4304 outlines support for a 64-bit Extended Sequence Number (ESN) implemented for ikev2. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

StarOS supports ESN for ESP packets using ikev2 negotiation; ESN is not supported for ikev1. The configuration and processing sequence is as follows:

- Enable ESN in an IPSec transform set via a StarOS CLI command.
- Negotiate ESN (IPSec Domain of Interpretation (DOI) for Ikev2.
  - Send ESN in the proposal based on configuration.
  - Accept and process ESN in the proposal based on configuration.
- Configure data-path to use ESN.
- Read and checkpoint ESN.

**Command Changes**

`esn`

The IPSec Transform Set Configuration mode includes an `esn` command that enables ESN support.

```
configure
  context ipsec_ctx_name
     ipsec transform-set tset_name
       esn
     end
end
```

**Notes:**

- `ipsec_ctx_name` is the StarOS context associated with IPSec.
- `tset_name` is the name of the transform set in the current context that you want to configure for ESN.
- For more information on command parameters, see the *Extended Sequence Number* chapter in the *IPSec Reference*.
- By default ESN support is disabled.
- Enabling the `esn` command is the equivalent of sending ESN Transform = 0 and 1; support both 32-bit and 64-bit sequence numbers. If the `esn` command is not enabled, support only 32-bit sequence numbers (default behavior).

**Performance Indicator Changes**

`show crypto ipsec transform-set`

This command displays the IPSec transform set parameters as configured in a specific context and includes ESN status.

- ESN: Enabled/Disabled

`show crypto template`
This command displays ESN status under IPSec SA Payload.

- ESN: Enabled/Disabled

**CSCuh37234 - Layer 3 based High Availability**

**Feature Changes**

**ICSR Layer 3 Interchassis HA**

This feature supports L3 Interchassis High Availability for SecGW. This card-level redundancy uses Interchassis Session Recovery (ICSR) implemented for RRI to ensure that the routes are injected correctly on the appropriate VSM to route the traffic to the correct interface after an ICSR switchover.

An anchor route must be specified for ICSR L3 redundancy to map the physical interface IP addresses on both the active and standby VSMs to the virtual Anchor IP address.

Chassis-to-chassis redundancy employs HSRP to detect failure in the system and notify other elements of the need to change their HA State. Each VSM receives these notifications via oneP (Connected Apps) communication.

An external HSRP-aware entity switches traffic from the primary to the backup chassis. All application instances must failover to the backup chassis.

For additional information on L3 interchassis HA, see the *SecGW Administration Guide*.

**Command Changes – Reverse Route Injection**

There are several StarOS CLI commands associated with RRI configurations. They are briefly described below. For additional information, see the *Command Line Interface Reference* and *SecGW Administration Guide*.

**ip rri-remote-access**

This Context Configuration mode CLI command configures RRI remote access mode parameters. This command is only required for Remote Access Service configurations.

```plaintext
configure
  context context_name
    ip rri-remote-access { ip_address | next-hop nexthop_address } interface
    interface_name [ vrf vrf_name ]
```

Notes:

- `ip_address` and `nexthop_address` can be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.

**ip rri-route**

This Context Configuration mode CLI command configures RRI route parameters.
configure

context context_name

   ip rri-route network-mode { L2 | L3 } { clear_loopback_ip | rri-ip
   virtual_ip_address } { ip_address | next-hop nexthop_address } interface interface_name [ vrf vrf_name ]

end

Notes:

- `ip_address`, `virtual_ip_address` and `nexthop_address` can be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.

ip sri-route

This Context Configuration mode command configures L3 High Availability Service Route Injection parameters:

configure

context context_name

   ip sri-route sri-ip network_address next hop nexthop_address interface
   interface_name [ vrf vrf_name ]

end

Notes:

- `network_address` and `nexthop_address` are specified in IPv4 dotted-decimal notation.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.

rri-mode

This ConnectedApps Configuration mode CLI command configures the supported RRI mode.

configure

connectedapps

   rri-mode { both | none | ras | s2s }

end

Notes:

- `ras` = Remote Access Service
- `s2s` = site-to-site
Command Changes – Anchor Route Configuration

`ip anchor-route`

This command associates the anchor IP address and physical IP address for this route. The command syntax is as follows:

```
cfg context wsg_context

  ip anchor-route anchor-ip-addr/32 physical-ip-addr interface name
```

Notes:
- `anchor-ip-addr` is the virtual IP address used on the private network side of both the active and standby VSMs.
- `physical-ip-addr` is the unique IP address configured for the physical interface on each VSM.

Command Changes – HSRP

HSRP configuration parameters include:
- Interface name
- Address Family Identifier (AFI) type (IPv4 or IPv6)
- HSRP group number

---

**Important:** The above parameters must match those of the HSRP configuration in the ASR 9000 RSP.

The following limits also apply to the HSRP configuration:
- A maximum of one HSRP monitor is supported per QvPC-VSM instance.
- The `monitor hsrp` command is associated with the SRP context.

```
monitor hsrp
```

The syntax for the `monitor hsrp` command is as follows:

```
cfg context srp_context

  monitor hsrp interface ifname afi-type type group hsrp_group
```

CSCum19793 - WSG as IKEv2 Initiator

Feature Changes

WSG as IKEv2 Initiator
By default SecGW (WSG service) only responds to a setup request for an IKEv2 session. However, an SecGW can also be configured to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval.

**Previous Behavior:** By default SecGW only responds to an IKE setup request for an IKEv2 session.

**New Behavior:** An SecGW can now be configured to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval.

The following is the general event sequence for an SecGW acting as an initiator.

1. The SecGW waits for the peer to initiate a tunnel within a configurable time interval during which it is in responder mode. The default responder mode interval is 10 seconds.
2. Upon expiry of the responder mode timer, the SecGW switches to initiator mode for a configurable time interval. The default initiator mode interval is 10 seconds.
3. The SecGW retries the call if there is no response from the peer during the initiator mode interval.
4. When the SecGW is in initiator mode and the peer does not respond to the IKE messages or fails to establish the call, SecGW reverts to responder mode and waits for the peer to initiate the IKEv2 session.
5. If call creation is successful, the SecGW stops initiating any further calls to that peer.
6. If the SecGW and peer initiate a session call simultaneously (possible collision), the SecGW defers to the peer initiated call and drops any incoming packets.

When the SecGW as initiator feature is enabled, the SecGW only supports up to 1,000 peer addresses. This restriction is applied when configuring a crypto peer list.

The following is the general sequence for configuring this feature:

- Create a crypto peer-list
- Configure the Peer List in the WSG Service
- Configure Initiator Mode and Responder Mode Durations

See the Security Gateway as Initiator chapter of the IPSec Reference for additional information on this feature.

### Command Changes

**crypto peer-list**

Creating a crypto peer list enables WSG as IKEv2 Initiator. The CLI command sequence for creating a crypto peer list is shown below.

```
configure
  context context_name
    crypto peer-list { ipv4 | ipv6 } peer_list_name
      address peer_address
    exit
```

**Notes:**

- Repeat the `address peer_address` command to add up to 1,000 peer IP addresses.
- Use the `no address peer_address` command to remove a peer address from the peer list.
The following CLI command sequence configures the previously created peer list for use in the WSG service.

```
configure
  context wsg_ctxt_name
    wsg-service wsg_service_name
    peer-list peer_list_name
    exit
```

Notes:
- `peer_list_name` must have been previously configured via the Context Configuration mode `crypto peer-list` command.
- Use the `no peer-list` command to remove the peer-list and disable the SecGW as initiator feature.

**initiator-mode-duration, responder-mode-duration**

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the following CLI command sequence.

```
configure
  context wsg_ctxt_name
    wsg-service wsg_service_name
    initiator-mode-duration seconds
    responder-mode-duration seconds
    exit
```

Notes:
- `seconds` is an integer from 5 through 250.

**Performance Indicator Changes**

**show wsg-service all**

Run this CLI command to display the current crypto peer list configuration.

- peer list: `peer_list_name`
- Initiator mode duration: `nnn` seconds
- Responder mode duration: `nnn` seconds
CSCum81454 - CLI to support Allow one tunnel per remote IKE_ID feature

Applicable Products: SecGW (WSG Service)

Feature Changes

Duplicate Session Detection

RFC 5996 does not restrict the creation of multiple IKE SAs having the same remote IKE_ID (not necessarily from the same peer). The remote IKE_ID specifies the remote peer ID: IDi when the gateway is the responder, and IDr when the gateway is the initiator. In such implementations, a new IKE_SA is created for every IKE_SA_INIT/IKE_AUTH exchanges, unless INITIAL_CONTACT is indicated. If an IKE_AUTH is received with INITIAL_CONTACT, the node is expected to delete all IKE_SAs having the same authenticated identity.

When enabled via the StarOS `duplicate-session-detection` command in a WSG service, only one IKE_SA is allowed per remote IKE_ID. This feature is supported for WSG service, both RAS (Remote Access Service) and S2S (Site-to-Site) tunnel types.

Command Changes

duplicate-session-detection

This new CLI command enables duplicate session detection.

```
configure
    context wsg_ctx_name
    wsg-service wsg_srvc_name
        duplicate-session-detection
        [ no ] duplicate-session-detection variable
    end
```

Notes:
- `wsg_ctx_name` is the StarOS context associated with a WSG service.
- `wsg_srvc_name` is the name of the WSG service in the current context that you want to configure for duplicate session detection.
- For more information on parameters, refer to the WSG Service Configuration Mode Commands chapter in the Command Line Interface Reference.
- By default duplicate session detection is disabled.

Performance Indicator Changes

show wsg-service all

The output of this command will include the following parameter:
Duplicate-session-detection: Enabled/Disabled

CSCuo71292 - SecGW - Supporting TLS for Connectedapp

Feature Changes

OneP Support for TLS Connection between ASR 9000 RSP and VSM

Previous Behavior: OneP (ConnectedApps) only supported a TCP (Transmission Control Protocol) connection between the ASR 900 RSP and VSM.

New Behavior: For security reasons, the TCP connection between RSP and VSM is no longer be supported by OneP. TLS (Transport Layer Security) is the only connection type supported by OneP. This is an IOS-XR configuration change.

CSCup53154 - Upgrade oneP package to rel7 / dev7 which supports CSS

Feature Changes

Upgrade to OneP Package Release 7

The upgrade of the OneP SDK to Release 7 is necessary for the following reasons:

- Required when using IOS-XR 5.2.0. This oneP SDK is also backward compatible.
- Supports Certificate Service Set (CSS), required for “Certificate Sync between VSMs” feature.
- Bug fixes

CSCup72627 - snmp mib CLI enabling/disabling snmp tunnel stats retrieving

Feature Changes

Tunnel Statistics Available Via Cisco SNMP MIBs

SNMP tunnel statistics can be obtained by enabling the following SNMP MIBs:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-ENHANCED-IPSEC-FLOW-MIB

You enable these MIBs via the existing StarOS Global Configuration mode `snmp mib` CLI command.
CSCup81922 - Need different SysObjectID for SecGW/VSM and SI

Feature Changes

New MIB OID for ASR 9000 VSM

**Previous Behavior:** An SNMP GET of the SysObjectID (1.3.6.1.2.1.1.2) returned “QVPC-SI”.

**New Behavior:** An SNMP GET of the SysObjectID now returns “Cisco QvPC over VSM”.

Chapter 21
SGSN Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from the SGSN in StarOS 17 software releases.
SGSN Enhancements for 17.7

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 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

---

**CSCux33388, CSCur41900 - CLI Control for 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**

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 TAUs 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:** 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.

```
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 ]

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 ccprofl
...
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 ccprofl
  remove rau-inter ctxt-xfer-failure
  no subscriber-control-inactivity
...
  access-restriction-data target-access-restriction
...
...


SGSN Enhancements for 17.5

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

CSCus91182 - UPCQ Need Not be Sent With DT in Certain Scenarios to Modify MS INIT

**Feature Changes**

**Call Flow Change in Some DT Scenario**

If the MS initiates a PDP modification procedure in 3G when direct tunnel is enabled in the Call Control Profile configuration and 'release-and-establish' is the RAB modification procedure defined for the RNC configuration, then there is the possibility for error-indication from the GGSN during the RAB-release and re-establish procedure. This can cause the CN and RAN nodes to go out of sync with respect to the RAB-state.

**Previous Behavior:** Direct tunnel remains intact for the UE's session during the PDP modification procedure with the SGSN, using the following call flow:

1. 3G Attach and Activation.
2. MS-init Modify Request.
3. UPC Request to GGSN with DTI.
4. UPCR Response.
5. RAB Release and Response.
6. RAB Assignment and Response.
7. UPCQ with DTI and UPCR.
8. Modify Accept.

**New Behavior:** Direct tunnel is temporarily changed to two tunnels for the UE’s session during the PDP modification procedure with the SGSN and then after the PDP modification procedure completes the direct tunnel establishment is carried out. This new behavior adheres to the following flow:

1. 3G Attach and Activation.
2. MS-init Modify Request.
3. UPC Request to GGSN without DTI.
4. UPCR Response.
5. Modify Accept.
6. RAB Release and Response.
7. RAB Assignment and Response.
8. UPCQ with DTI and UPCR.

**Customer Impact:** With the noted configuration and the new call flow, the customer will not experience RAB-state sync issues between the SGSN and the RNC that previously would be due to MS-initiated modifications and GGSN error indication collision cases.

**CSCuv37204 - SGSN is sending incorrect cause code in Activate PDP Context Reject**

**Feature Changes**

**Cause Code in Activate PDP Context Reject**

**Previous Behavior:** With Direct Tunnel enabled, when there is a collision of the UPCQ and DPCQ (from GGSN) during the PDP activation procedures, then the SGSN triggers the Activation Reject with the SM cause "regular deactivation". For example,

- PDP Activation Request received from UE.
- CPCQ and CPCR with GGSN.
- RAB establishment procedure.
- UPCQ from SGSN with DTI info.
- DPCQ from GGSN.
- Activation reject from SGSN to UE with SM cause as "regular deactivation"

**New Behavior:** Now with Direct Tunnel enabled, when there is a collision of the UPCQ and DPCQ (from GGSN) during the PDP activation procedures, then the SGSN triggers the Activation Reject with the correct SM cause, "activation rejected by GGSN". For example:

- PDP Activation request from UE.
- CPCQ anc CPCR with GGSN.
SGSN Changes in Release 17

- RAB establishment procedure.
- UPCQ from SGSN with DTI info.
- DPCQ from GGSN.
- Activation Reject from SGSN to UE with SM cause as "activation rejected by GGSN"

**Customer Impact:** Use of this different cause code ensures that statistics and accounts will be properly updated for the correct SM cause.

**CSCuv92478 - Wrong CELL-ID/LAC information in S-CDR during relocation request**

**Feature Changes**

**UE Location**

**Previous Behavior:** The User Location Information (ULI) of the User Equipment (UE) consists of RAC, LAC and SAC values. However, during an intra-SRNS procedure (Relocation) only the RAC and LAC values were available in the ULI until a subsequent RAU was performed by the UE. This RAU provides the missing SAC value for the ULI.

During the transient period between Relocation and the initiation of a RAU, that is, before receiving the SAC value from the RAU by the UE, if a S-CDR is opened, this S-CDR would contain the new RAC and new LAC value, but the old SAC value.

**New Behavior:** The old known location of the UE is used in the ULI for a S-CDR opened during the transient period, that is, the period between SGSN receiving a Relocation Request and before it receives the follow up RAU. Also, the same location information is sent in the Update PDP Context Request message, which is sent to GGSN during the intra-SRNS procedure for some cases.

A new keyword `use-old-location-info` is added to the `inter-rnc-procedures` command to enable this behavior

**Command Changes**

`inter-rnc-procedures`

The `use-old-location-info` is a new keyword in this command which enables the SGSN to use the old known location of the UE during an intra-SRNS procedure. By default, this keyword is disabled.

```
configure
  context context_name
    iups-service service_name
      [ no ] inter-rnc-procedures use-old-location-info
  end
```

Notes:
- `no` disables the configuration.
- **use-old-location-info** selects and uses the old values of LAC, RAC and SAC for S-CDRs and ULI information sent to the GGSN during an intra-SRNS procedure.

**Performance Indicator Changes**

**show iups-service name service_name**

On executing this command the following new field is added to show if the old know UE location is enabled or disabled:

- Use old location in SCDR and ULI for ongoing intra-SRNS

**CSCuw40333 - Missing Mandatory AVP From HSS Causes Task Restart During Handoff**

**Feature Changes**

**Action Taken If QoS-Subscribed AVP Error**

This behavior change deals specifically with the action to be taken if QoS-Subscribed AVP is either missing or incorrect in the Update Location Answer (ULA) from the HSS. This AVP is under the PDP-context of the GPRS-Subscription.

**Previous Behavior:** The SGSN completes the Attach/RAU procedure even if the QoS-Subscribed AVP from the HSS in the ULA is missing or incorrect.

**New Behavior:** The SGSN rejects the Attach/RAU procedure if the QoS-Subscribed AVP from the HSS in the ULA is missing or incorrect.

**Customer Impact:** This change of behavior means the operator does not experience SessMgr restarts during old-ISRAU procedures as a result of errors in the QoS-Subscribed AVP that are received from the HSS in the ULA during new inter SGSN RAU.
SGSN Enhancements for 17.4

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

---

**CSCur41900 - TAU Reject with EMS Cause #15 mapping instead of #19**

**Feature Changes**

**Target Access Restricted for the Subscriber Cause Code**

This enhancement is a 3GPP TS (29.274 and 29.060) release compliance enhancement. As per 3GPP TS 29.274 and TS 29.060, the source-serving node (MME/SGSN) is allowed to reject SGSN Context Request (GTPv1) and Context Request (GTPv2) mobility management messages with “Target Access Restricted for the subscriber” cause if target access is restricted for the subscriber based on the Access-Restriction-Data in the subscription profile. The target node (MME/SGSN) is allowed to reject RAU/TAU with anyone one of the following NAS Causes:

- #15 “No suitable cells in tracking area”, or
- #13 “Roaming not allowed in this tracking area”, or
- #12 “Tracking area not allowed”
New statistics have been introduced under “show egtpc statistics verbose” and “show sgtpc statistics verbose” to reflect the context response sent and received with the new reject cause “Target Access Restricted for the subscriber”.

For more information refer to the 3GPP TS 29.274 (section 7.3.6), TS 29.060 (section 7.5.4), TS 29.060 Annex B (Table B.5: Mapping from Gn/Gp to NAS Cause values – Rejection indication from SGSN) and TS 29.274 Annex C (Table C.5: Mapping from S3/S16 to NAS Cause values – Rejection indication from MME/S4-SGSN)

**Previous Behavior:** In earlier releases:
- The target node (SGSN/MME) does not send the target RAT type in SGSN Context request to the source node.
- The target node (SGSN/MME) rejects RAU/TAU with cause “No suitable cells in Location/Tracking Area” only after ULA/ULR is received with target RAT restricted for the subscriber in Access-Restriction-Data.

**New Behavior:** From this release onwards:
- The target node (SGSN/MME) sends the target RAT Type in SGSN Context request to source node.
- The source node (SGSN/MME) rejects the SGSN Context Request/Context Request with the cause “Target Access Restricted for the subscriber” if target RAT is restricted for the subscriber as per Access-Restriction-Data received in ULA/ULR using RAT Type received in SGSN Context request/Context request.
- The target node (SGSN/MME) sends RAU/TAU reject after Context Response/SGSN Context Response received with EGTP/GTP cause “Target Access Restricted for the subscriber”.

**Customer Impact:** Rejecting RAU/TAU much early in call cycle results in reduced signaling.

**Performance Indicator Changes**

`show sgtpc statistics verbose`

New statistic is added to this show command to display Target Access Restricted statistics for GTPv1 mobility management messages.
- Target Access Restricted

`show egtpc statistics verbose`

New statistic is added to this show command to display Target Access Restricted statistics for GTPv2 mobility management messages.
- Target Access Restricted

**CSCus64306 - SGSN cannot reject RAU with MNC/MCC that arrive in HEX**

**Feature Changes**

**Validation of MCC/MNC Values in the Old RAI Field**

This feature is developed to comply with 3GPP TS 24.008. As per 3GPP TS 24.008, in some abnormal instances the MCC stored in the Mobile Station (MS) contains elements which do not belong to the set \{0, 1 ... 9\}. In such cases the Mobile Station should transmit the stored values using full hexadecimal encoding. When receiving such an MCC, the network should treat the RAI as deleted. In some instances it is possible that the MNC stored in the Mobile Station has the following:
- Digit 1 or 2 not in the set \{0, 1 ... 9\}
- Digit 3 not in the set \{0, 1 ... 9, F\} hex

In such cases the MS should transmit the stored values using full hexadecimal encoding. When receiving such an MNC, the network should treat the RAI as deleted. The same handling is applicable for a network where a 3-digit MNC is sent by the mobile station to a network using only a 2-digit MNC.

A validation check has been introduced to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU requests. When the MCC and MNC fields received in the RAU request (inter-SGSN) and are invalid, the RAU request is rejected by SGSN. When the MCC and MNC fields received in the Attach Request and are invalid, the identity of the MS is retrieved directly from the MS instead of sending identity request to the peer node where peer SGSN identity is derived from the old-RAI.

**Important:** This feature is applicable for both 2G and 3G networks.

A new CLI command `rai-skip-validation` has been introduced under both IuPS service and GPRS service configuration modes. This new command enables/disables rejection of RAU requests with invalid MCC/MNC values in the old RAI field. By default the old RAI MCC/MNC fields are validated. This command also impacts the PTMSI attaches where the old RAI field is invalid. If the OLD RAI field is invalid and if the validation is enabled through the new CLI command, the identity of the MS is requested directly from the MS instead of the peer SGSN.

**Previous Behavior:** Validation check is absent for the MCC/MNC fields in old RAI received from MS in RAU request or Attach request.

**New Behavior:** A validation check has been introduced to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU requests. A new CLI command `rai-skip-validation` has been introduced under the IuPS service and GPRS service configuration modes. If invalid MCC/MNC values are received from MS in old RAI field in a RAU request, the request is rejected by the SGSN. If invalid MCC/MNC values are received from MS in old RAI field in a Attach request, the identity of the MS is retrieved directly from the MS instead of sending identity request to the peer Node where the MS identity is derived from the valid old-RAI. By default the old RAI MCC/MNC fields are validated.

**Command Changes**

`rai-skip-validation`

This new command is introduced under both IuPS and GPRS service configuration modes. Validation check is done as per 3GPP TS 24.008 for MCC/MNC fields of old RAI IE in Attach/RAU requests. RAU requests with invalid MCC/MNC values in the old RAI field are rejected. For Attach requests with invalid MCC/MNC values in the old RAI field, identity of the MS is retrieved directly from the MS instead of sending identity request to the peer Node where the MS identity is derived from the valid old-RAI.
context context_name

gprs-service service_name

[no] rai-skip-validation

end

Notes:

- If invalid MCC/MNC values are received from MS in old RAI field in a RAU request, the request is rejected by the SGSN.
- If invalid MCC/MNC values are received from MS in old RAI field in an Attach request, the identity of the MS is retrieved directly from the MS instead of sending identity request to the peer Node where the MS identity is derived from the valid old-RAI.
- By default the old RAI MCC/MNC fields are validated.

CSCuu59020 - RAB Assignment Request sent with Alternate RAB param without RAB param

Feature Changes

Inclusion of Alternate RAB Parameters in RAB Assignment Request

Previous Behavior: Alternate RAB Parameters are always included in the RAB Assignment Request for RAB Establishment or Modification.

New Behavior: Alternate RAB Parameters are included only when the RAB Parameters are included in the RAB Assignment Request for RAB Establishment or Modification.

Customer Impact: RAB modification failures do not occur during direct-tunnel establishment after Inter-SGSN RAU.

CSCuu74352 - No rab release during upc/dpc collision

Feature Changes

Send Activate PDP Reject Instead of De-activate PDP Request

Scenario:

1. 3G Attach procedure begins.
2. The SGSN receives a PDP Context Activation Request from the UE.
3. The SGSN processes the activation until the RAB establishment procedure; as it is a direct tunnel-capable call, the SGSN initiates an UPC Request to the GGSN and waits for the UPC Response.
4. The GGSN initiates Delete PDP Context Request on the same context (Note: DPCR can occur for any reason, such as the GGSN clearing the PDP session).

Previous Behavior: The GGSN initiates a deletion before activation is completed at the SGSN. The SGSN sends a Deactivate PDP Request. Due to DPC/UPC collision, the SGSN does not release the old RAB at the RNC.
New Behavior: The SGSN now sends an Activate PDP Reject when the GGSN initiates a Delete PDP Context Request before activation is completed at the SGSN and then the SGSN releases the RAB at the RNC.

Customer Impact: DPC/UPC collision and presence of older RAB at the RNC do not affect further activations from the UE.

CSCuv02890 - Enforce license for MTC functionality

Feature Changes

License Control for MTC Functionality

Previous Behavior: The feature specific license was not enforced to use the commands and functionality related to the optional MTC feature on the SGSN.

New Behavior: With Release 17.4, the MTC Feature license is now enforced to use MTC functions and related commands. Please speak with your Cisco Customer Representative if you have questions about the MTC Feature license.

For an idea of the MTC functionality supported by the SGSN, refer to the sections covering CSCum47774, CSCum50056 in the SGSN Enhancements for 17.1 in this document. For detailed information about the SGSN’s MTC feature support, refer to the MTC Congestion Control chapter of the SGSN Administration Guide.
SGSN Enhancements for 17.2

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 *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 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**

---

**CSCus06673 - RAB Setup Fails with cause invalid-rab-parameters-combination**

**Feature Changes**

**GGSN initiated PDP-modification Call-flow Modified**

**Previous Behavior:** The RNC RAB-modification procedure is release-and-establish with Direct Tunnel enabled, the GGSN initiated PDP-modification call-flow for a successful case is as follows:

1. An UPCQ from GGSN is received for a PDP-context.
2. MS modify request and MS modify accept procedures occur.
3. RAB-release and RAB-assignment procedures occur.
4. An UPCR is sent to the GGSN with cause “Accepted” along with the DTI information.

**New Behavior:** The RAB-release and establishment is done after acknowledging the GGSN modification with UPCR without direct tunnel. This is followed by UPCQ with Direct tunnel information from SGSN post rab-assignment success. The modified call-flow during RNC RAB modification procedure is as follows:
1. An UPCQ from GGSN is received for a PDP-context
2. MS modify request and MS modify accept procedures occur.
3. Direct tunnel is disabled during this step and UPCR is sent to the GGSN with cause as “Accepted” (DTI information is not sent).
4. Direct tunnel procedure is initiated and the RAB is released and re-established.
5. UPCQ is sent to GGSN with DTI information, UPCR is received from the GGSN.

**Customer Impact:** When the GGSN tries to forward the downlink data to the RNC during PDP-modification procedure initiated by GGSN, error-indication will not be received during the RAB-release and RAB re-assignment procedures.

**CSCus50162 - QOS : Incorrect Reliability Class Mapping from QCI=5**

**Feature Changes**

**Improve Reliability Class Mapping**

During handovers involving Inter-RAT, some UEs experienced issues with existing behavior, which required the UEs to be powered off/on (reboot) to acquire service. Those issues should be resolved with the behavior changes identified below.

**Previous Behavior:** In situations where the SDU error ratio = 10^-6, the MME and SGSN each implemented QoS mapping of reliability class =2.

**New Behavior:** The MME and SGSN behavior has been modified such that in situations where the SDU error ratio = 10^-6, the MME and SGSN each implement QoS mapping of reliability class =3.
SGSN Enhancements for 17.1

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 *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 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

---

**CSCtq92045 - Need Linkmgr CPU added to bulkstats for SGSN cpcty monitoring**

**Feature Changes**

**Additional Card-level Bulk Statistics Added**

**Previous Behavior:** Some card-level bulk statistics were not supported.

**New Behavior:** Support for collection and display of card-level bulk statistics for LinkMgr, MMgr, GbMgr, and IMSIMgr have been added for the following:

- number of task instances
- average memory utilization
- average CPU utilization
• maximum CPU utilization
• maximum memory utilization

Performance Indicator Changes

Card Schema

The following statistical variables have been added to collect and display information for LinkMgr, MMgr, GbMgr, and IMSIMgr at the card level:

• task-linkmgr-num
• task-linkmgr-avgcpu
• task-linkmgr-avgmem
• task-linkmgr-maxcpu
• task-linkmgr-maxmem
• task-gbmgr-num
• task-gbmgr-avgcpu
• task-gbmgr-avgmem
• task-gbmgr-maxcpu
• task-gbmgr-maxmem
• task-imsimgr-num
• task-imsimgr-avgcpu
• task-imsimgr-avgmem
• task-imsimgr-maxcpu
• task-imsimgr-maxmem
• task-mmgr-num
• task-mmgr-avgcpu
• task-mmgr-avgmem
• task-mmgr-maxcpu
• task-mmgr-maxmem

CSCty74246 - SNMP trap when generated does not include the Restart count

Feature Changes

eGTPC Path Failure Clear Trap

Previous Behavior: The EGTPCPathFailClear trap did not include the correct ‘peer restart counter’ when a new user session was created after a path failure was detected for that peer.
New Behavior: The 'peer restart counter' is now updated correctly for the EGTPCPathFailClear trap when a new user session is created after a path failure is detected for that peer. The peer restart counter value is displayed in the output of the show snmp trap history command.

CSCup71665 - Routing-context cannot be set to 0

Feature Changes

Routing Context Value for M3UA Messages

Previous Behavior: The SGSN does not support configuration of value “0” for the M3UA routing-context parameter.

New Behavior: The SGSN now supports “0” as a valid configuration value for M3UA routing-context parameter.

Customer Impact: The customer now has an option to configure “0” as a value for the M3UA routing-context parameter, this is especially required when the HLR is serving SGSNs from other vendors in the network.

Command Changes

routing-context

The routing-context command in the SS7 Routing Domain Configuration Mode now allows configuration of routing context ID values starting from “0”.

configure

ss7-routing-domain routing_domain_id variant variant_type

    routing-context value

    end

routing-context

The routing-context command in the Peer-Server Configuration Mode now allows configuration of routing context ID values starting from “0”.

configure

ss7-routing-domain routing_domain_id variant variant_type

peer-server id server_id

    routing-context value

    end
CSCup99718 - SGSN should modify MR timer value based on backoff timer value.

Feature Changes

SGSN Modifications to MR Timer

**Previous Behavior:** If the configured MR timer value is less than the t3346 backoff timer by 4 minutes, then the SGSN does not modify the MR timer based on the sent value of the t3346 backoff timer.

**New Behavior:** When the configured MR timer value is less than the t3346 timer by 4 minutes, then the SGSN modifies the MR timer based on the t3346 backoff timer value, sent in RAU Rejects and Service Rejects, + 4 minutes.

If the t3346 backoff timer is less than the extended t3312 timer sent in Attach Accept and RAU Accept, then the SGSN modifies the MR timer based on the sent extended t3312 timer.

CSCuq37542 - Assertion failure at sess/sgsn/sgsn-app/pmm/pmm_fsm.c:6829

Feature Changes

New Iu release Disconnect Reasons and Statistics

**Previous Behavior:** Disconnect reasons and statistics are not available to track service requests received in direct transfer with unknown-ptmsi and local Intra-RAU received in direct transfer with unknown-ptmsi.

**New Behavior:** New Iu release disconnect reasons and corresponding statistics are added to track service requests received in direct transfer with unknown-ptmsi and local Intra-RAU received in direct transfer with unknown-ptmsi. The following Iu disconnect reasons are added:

- GMMSM_IU_REL_RSN_CURR_IU_UNK_PTMSI_SRV_REQ_DT: The current access released due to Service request received in direct transfer with unknown-ptmsi value.

- GMMSM_IU_REL_RSN_CURR_IU_UNK_PTMSI_INTRA_RAU_DT: The current access released due to Local Intra Rau received in direct transfer with unknown-ptmsi value.

Performance Indicator Changes

show gmm-sm statistics iups-service verbose

The following new statistics are added to track service requests received in direct transfer with unknown-ptmsi and local Intra-RAU received in direct transfer with unknown-ptmsi:

- cur-iu-srv-req-dt-ukn-ptmsi: This counter is incremented when the current access is released due to Service request received in direct transfer with unknown-ptmsi value.

- cur-iu-intra-rau-dt-ukn-ptmsi: This counter is incremented when current access is released due to local Intra-RAU received in direct transfer with unknown-ptmsi value.
CSCuq63874 - Increase the number of APN in remapping table

Feature Changes

Increase APN Entries for Remap Table

**Previous Behavior:** 100 was the maximum number of remap entries that could be created in an APN remap table.

**New Behavior:** The APN remap table entries limit has been extended from 100 to 300. The operator can use the `apn-remap` command to create and configure up to 300 entries in a single APN remap table, with one APN Remap Table per operator policy and the possibility of 1000 operator policies per system.

CSCuq95642 - [QvPC-DI] unable to start GTPUMgr, insufficient unserved memory

Feature Changes

QvPC-DI System Capacity

**Previous Behavior:** All DI system capacities based on memory were treated in the same manner.

**New Behavior:** DI systems with memory less than 48Gb are treated as reduced capacity (Medium Model) systems.

CSCur94789 - CLI ‘statistics-backup sgsn mme backup-int 1’ not applied

Command Changes

**statistics-backup**

Using the modified `statistics-backup` command, in the Global configuration mode, enables this new feature with a default backup interval of every 5 minutes.

```
configure
  statistics-backup { mme | sgsn }
  no statistics-backup { mme | sgsn }
end
```

Notes:

- **backup-interval minutes** - The optional keyword has been deprecated in this release and replaced with the new `statistics-backup-interval` command.

**statistics-backup-interval**
Using the new `statistics-backup-interval` command, in the Global configuration mode, allows the operator to change the interval between backups.

```
configure

statistics-backup-interval minutes

end
```

Notes:

- `minutes` - Enter an integer from 1 to 60 to set the number of minutes between backups.
SGSN Enhancements for 17.0

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 *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 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

**CSCts49833, CSCua43669, CSCuj06794 - Location reporting in Connected mode for S4 SGSN**

**Feature Changes**

### Important:
This feature was originally made available for Lab/Trial testing in Release 16.0. This feature is now available as Deploy Quality.

**Location Change Reporting for S4-SGSN**

**Previous Behavior:** The Gn-SGSN supports 2G and 3G location change reporting via user location information (ULI) reporting to the GGSN.

**New Behavior:** S4-SGSN now supports 2G and 3G location change reporting per 3GPP 29.274 release 11.b, if the P-GW requests it and if the feature has been enabled in the configuration (see *Command Changes* below).
With this feature enhancement configured, the S4-SGSN is ready to perform ULI reporting per PDN connection via GTPv2. Reporting only begins after the S4-SGSN receives a reporting request from the P-GW. The P-GW generates a request based on charging enforcement and policy enforcement from the policy and charging rules function PCRF. Location Change Reporting is configured and enabled/disabled per APN.

This feature has been further enhanced with a network sharing option. If the network sharing license is installed and if the network sharing feature is enabled, then the operator can configure which PLMN information the SGSN sends to the P-GW in the ULI or Serving Network IEs.

**Important:** The S3/S4 license is required to enable S4 functionality. The new “Location-reporting in connected-mode” license is required to enable Location Change Reporting functionality for the S4-SGSN. This new license is now required for Location Change Reporting on the Gn-SGSN.

## Command Changes

### location-reporting

To configure location change reporting via ULI IE per APN for an S4-SGSN, the operator must use this *new* command as part of the configuration of an APN profile.

```bash
configure

apn-profile profile_name

  location-reporting access-type { gprs | umts }

  remove location-reporting access-type { gprs | umts }

end
```

**Notes:**
- `remove` disables the location reporting configuration in the APN profile.
- `{ gprs | umts }` allows the operator to select location report for the 2G and/or the 3G subscribers. Two configuration entries are created whether both access types are included in a single command or in two commands.

### egtp

This new command enables the operator to select the type of PLMN sent in either the ULI IE or the Serving Network IE.

```bash
configure

call-control-profile ccpprofile_name

  egtp network-sharing-plmn { serving-network { use-common-plmn | use-selected-plmn | use-ue-plmn } | uli { use-common-plmn | use-selected-plmn | use-ue-plmn } }

  remove egtp network-sharing-plmn { serving-network | uli }

end
```
Notes:

- \{ serving

- \} selects the type of information element (IE) the PLMN information is added to.

- \texttt{use-common-plmn} instructs the SGSN to identify the Common PLMN for the shared network.

- \texttt{use-selected-plmn} instructs the SGSN to identify the Selected PLMN for the shared network.

- \texttt{use-ue-plmn} instructs the SGSN to identify the UE selected PLMN that is available in the shared network.

- The selections made for this configuration must match those configured for the call control profile’s GTP configuration.

CSCts82739 - LORC feature shall be supported over S4 interface

Feature Changes

LORC Subscriber Overcharging Protection on S4-SGSN

Previous Behavior: Subscriber Overcharging Protection was only available for the Gn-SGSN.

New Behavior: With Release 17.0, the SGSN’s Subscriber Overcharging Protection feature has been enhanced and now extends to the S4-SGSN to prevent both 2G and 3G subscribers from being overcharged when a loss of radio coverage (LORC) occurs over the S4 interface.

As part of the new functionality, the operator needs to configure all cause codes on the SGSN so that if the SGSN receives a cause code, via Gb/Iu interface, that matches one of the configured cause does, then the SGSN includes the ARRL (Abnormal Release of Radio Link) bit in Release Access Bearer Request sent on Iu-Release Request (3G) or Radio Status Bad (2G).

Customer Impact: This feature ensures more accurate billing by protecting the subscriber from overcharging in instances where abnormal radio resource release occurs.

Command Changes

\texttt{s4-overcharge-protection}

Use this new command, in the SGSN Service configuration mode, to

- enable or disable Subscriber Overcharging Protection feature for the S4-SGSN in the 3G network.

- associate a cause code group, defined with the LTE Policy command \texttt{cause-code-group} (described later in this section), with the SGSN Service configuration.

\begin{verbatim}
configure
  context context_name

sgsn-service service_name

  s4-overcharge-protection ranap-cause-code-group group_name

no s4-overcharge-protection
\end{verbatim}
end

Notes:

- **group_name**: Enter an alphanumeric string up to 16 characters long to identify the cause code group.
- **no**: When included with the command disables the Subscriber Overcharging Protection functionality for the 3G service. Disabled is the default.

**Important**: This CLI does not have any control over Release Access Bearer Initiation. If Release Access Bearer is going out of the S4-SGSN, the ARRL bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected. It is recommended to enable Release Access Bearer using the new CLI (refer to command section in CSCtz09826 for **release-access-bearer** before enabling this feature.

**s4-overcharge-protection**

Use this new command, in the GPRS Service configuration mode, to

- enable or disable Subscriber Overcharging Protection feature for the S4-SGSN in the 2G network.
- associate a cause code group, defined with the LTE Policy command **cause-code-group** (described later in this section), with the GPRS Service configuration.

```
configure

context context_name

gprs-service service_name

    s4-overcharge-protection bssgp-cause-code-group group_name

no s4-overcharge-protection

end
```

Notes:

- **group_name**: Enter an alphanumeric string up to 16 characters long to identify the cause code group.
- **no**: When included with the command disables the Subscriber Overcharging Protection functionality for the 2G service. Disabled is the default.

**Important**: This CLI does not have any control over release access bearer initiation. If Release Access Bearer is going out of the S4-SGSN, the ARRL bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected. It is recommended to enable Release Access Bearer using the new CLI (refer to command section in CSCtz09826 for **release-access-bearer** before enabling this feature.

**cause-code-group**

In support of the subscriber overcharging protection functionality for the S4-SGSN, it is now possible for the operator to use one of two new optional keywords under the LTE Policy configuration mode, **BSSGP** or **RANAP**, to define the cause codes received over the Gb interface for GPRS 2G service (BSSGP) and/or over Iu interface for UMTS 3G service (RANAP) when the SGSN initiates Release Access Bearer Request with ARRL bit set.
configure
lte-policy

    cause-code-group group_name protocol [ bssgp | ranap ]

    no cause-code-group group_name protocol [ bssgp | ranap ]

Notes:

- Under LTE Policy, the maximum number of cause code groups supported is 4. Note that this means that the total number of cause code groups available across all the services (SGSN+GPRS+MME) is 4.
- A single cause code group can be used for different protocol cause codes, but it is recommended to use a single group for each protocol.
- group_name: Enter an alphanumeric string up to 16 characters long.
- no: When no is included with the command then the identified cause code group, all related cause codes, and the identified protocol are deleted from the LTE Policy configuration. If all cause codes had been deleted from the group, then the group is automatically deleted.
- bssgp:
  - When included in the command, creates a sub-configuration mode for cause codes for the 2G service
  - Presents a prompt similar to the following: [local]sgsn-test(bssgp-cause-code)#
- ranap:
  - When included in the command, creates a sub-configuration mode for cause codes for the 3G service
  - Presents a prompt similar to the following: [local]sgsn-test(ranap-cause-code)#.

radio-cause

This new command, in the new BSSGP Cause Code configuration mode, enables the operator to define multiple cause codes for the 2G service so that

- if the BSSGP radio cause code configured by the operator matches with the radio cause received in the Radio Status message, and
- if the Subscriber Overcharging Protection feature is enabled for 2G service in the GPRS-Service configuration (see command information above),
- then the S4-SGSN includes ARRL (Abnormal Release of Radio Link) bit in Release Access Bearer Request message Initiated on Ready-to-Standby state transition.

configure
lte-policy

    cause-code-group group_name protocol bssgp

    radio-cause cause_code

    radio-cause cause_code

    radio-cause cause_code
no radio-cause cause_code
end

Notes:

- **radio-cause**: A maximum of 16 BSSGP protocol radio cause codes can be defined per group. **Note** that under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.

- **cause_code**: Enter an integer from 0 to 255 to identify a BSSGP protocol radio cause code, as defined in the *Radio Cause* section of the 3GPP TS 48.028 specification.

- **no**: When included with the command, the specified cause code is deleted from the group. If all cause codes are deleted from the group then the group is automatically deleted.

**Important**: The SGSN does not support Enhanced Radio Status functionality; therefore, the SGSN treats cause code values 0x03 and 0x04 as “Radio contact lost with MS”. Therefore, the valid configurable cause codes values are 0, 1, and 2.

**configure**

```
lte-policy

cause-code-group group_name protocol ranap

  cause cause_code

  cause cause_code

  cause cause_code

  no cause cause_code

end
```

Notes:

- **cause**: A maximum of 16 RANAP protocol cause codes can be defined per group. **Note** that under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.

- **cause_code**: Enter an integer from 1 to 512 to identify a cause code. Valid options are listed in 3GPP TS 25.413 v11.5.0 (or later version), subsection on *Cause* in subsection for *Radio Network Layer Related IEs.*
• no: When included with the command, the specified cause code is deleted from the group. If all cause codes are deleted from the group then the group is automatically deleted.

Performance Indicator Changes

show s4-sgsn statistics

In support of this new functionality, two counters have been added to the output generated by this command, under the section for S4 Overcharge Protection Statistics:

• 3G Release Access Bearer with ARRL bit set
• 2G Release Access Bearer with ARRL bit set

CSCty44479 - APN Restriction on S4-SGSN

Feature Changes

APN Restriction Extended to S4-SGSN

Previous Behavior: The Gns-SGSN supports the APN Restriction feature.

New Behavior: Support for APN Restriction is required on the S4-SGSN. The reception, storage, and transfer of APN Restriction values is used to determine whether a UE is allowed to establish PDP Context or EPS bearers with other APNs.

During default bearer activation, the S4-SGSN sends the current maximum APN restriction value for the UE to the P-GW in a Create Session Request (CSR). The P-GW retains an APN restriction value for each APN. The UE’s APN Restriction value determines the type of application data the subscriber is allowed to send. If the maximum APN restriction of the UE (received in the CSR) and the APN Restriction value of the APN (for which activation is being request) do not concur, then the P-GW rejects activation. The maximum APN restriction for a UE is the most restrictive based on all already active default EPS bearers.

APN Restriction for S4-SGSN is enabled/disabled in the call-control-profile configuration using the existing apn-restriction command -- this command also enables APN Restriction for the Gn-SGSN. This feature provides the operator with increased control to restrict certain APNs to UEs based on the type of APN. This feature requires no special license other than the S3/S4 license needed to enable the S4-SGSN.

Command Changes

apn-restriction

This command was used to enable APN Restriction for the Gns-SGSN, this command is now also used by the S4-SGSN to enable APN restriction feature.

configure

call-control-profile profile_name

apn-restriction update-policy deactivate restriction

default apn-restriction
Notes:

- The least or most restrictive values of the APN restriction are applicable only for the Gn SGSN, as the APN restriction can be present in UPCQ/UPCR for Gn SGSN and this configuration is required to determine the PDN to be de-activated when an APN restriction violation occurs during modification procedures in the Gn SGSN.

- In the case of S4-SGSN, the APN restriction arrives at the S4-SGSN only in Create Session Request Response during activation. During activation in S4-SGSN, a PDN connection that violates the current Maximum APN restriction is always de-activated. Therefore in the case of S4-SGSN, this CLI is used only for enabling or disabling APN restriction.

Performance Indicator Changes

**show subscribers sgsn-only full/ show subscribers gprs-only full**

The show output of these commands display the APN Restriction value of each PDP Context.

**show session disconnect-reasons verbose**

The disconnect reason `sgsn-apn-restrict-vio` is used to track the APN restriction.

**show gmm-sm statistics verbose**

The following counters related to the cause “APN restriction value incompatible with active PDP context” are displayed on executing the command `show gmm-sm statistics verbose`:

- Deactivation Causes Tx
- 3G-APN Restr val Incomp With Ctx
- 2G-APN Restr val Incomp With Ctx
- Activate Primary PDP Context Denied
- 3G-APN-Restriction Incompatible
- 2G-APN-Restriction Incompatible

CSCty82285 - Increasing Lawful interception capacity on SGSN

Feature Changes

Lawful Interception Capacity Enhanced

In a full ASR5K chassis with PSC2 cards the maximum number of attached users is about “4” million. In previous releases, it was possible to configure and intercept 20000 camp-on users on the chassis. With this feature enhancement the lawful interception capacity has been increased to 4% of the maximum number of attached users, that is 160,000 camp-on users (4% of 4 million subscribers). It is now possible to configure and intercept 160000 camp-on users on the chassis.

**Previous Behavior**: The lawful interception capacity is limited to 20000 intercepts.
New Behavior: The lawful interception capacity is now increased to 160000 intercepts.

Customer Impact: Additional CPU is required to simultaneously intercept more number of users, therefore the overall throughput supported by the chassis may drop. The average throughput per user on the LI interface may reduce when many users are being intercepted simultaneously. Additional memory is required at the Session Manager to store the intercepts.

CSCtz09826 - Need a cli to control ‘Release Access Bearers Request’

Feature Changes

Configurable RAB Cause

To enhance the S4-SGSN functionality of the LORC Subscriber Overcharging Protection now extended to the S4 interface (refer to CSCts82739), a new CLI command enables the operator to configure the Release Access Bearer cause code to be included with the ARRL (Abnormal Release of Radio Link) bit in the Release Access Bearer Request.

Previous Behavior: Upon RNC failure or Iu-Release, the SGSN preserves non-GBR PDPs (interactive or background) by default.

- In the case of either DT (direct tunnel) or ISR for 3G, the SGSN already supported the sending of Release Access Bearer Request on Iu-Release.
- By default, in 2G upon Ready-to-Standy the SGSN preserved non-GBR PDPs (interactive or background).
- For ISR, the S4-SGSN already sent Release Access Bearer Request on Ready-to-Standy state transition.

New Behavior: With a new CLI command (see section below), the S4-SGSN can send Release Access Bearer Request on Iu-Release for non-DT and non-ISR subscribers in 3G and on Ready-to-Standy or Radio-Status-Bad for non-ISR subscribers in 2G. And in compliance with 3GPP TS 23.060 v11.7.0, the S4-SGSN now optionally sends Release Access Bearer Request to the S-GW to remove the downlink user plane on the S4 interface for non-DT and non-ISR scenario.

Command Changes

release-access-bearer

This new S4-SGSN-specific command, release-access-bearer in the Call-Control Profile configuration mode, provides the operator with CLI configuration control to enable or disable the sending of Release Access Bearer Request:


configure

call-control-profile profile_name

release-access-bearer [ on-iu-release | on-ready-to-standby ]

remove release-access-bearer [ on-iu-release | on-ready-to-standby ]
Notes:

- **on-iu-release**: This optional keyword instructs the SGSN to send Release Access Bearer upon Iu-Release in a 3G network so that Release Access Bearer will be initiated for non-ISR and non-DT subscribers upon Iu-Release. For ISR and DT subscribers, Release Access Bearer will be initiated unconditionally.

- **on-ready-to-standby**: This optional keyword instructs the SGSN to send Release Access Bearer on Ready-to-Standby transition in a 2G network so that Release Access Bearer will be initiated for non-ISR subscribers on Ready-to-Standby transition. For ISR subscribers, Release Access Bearer will be initiated unconditionally.

- If no optional keywords are included with the `release-access-bearer` command, then the S4-SGSN applies Release Access Bearer for both 2G and 3G networks.

- When enabled, either/both `release-access-bearer on-iu-release` or/and `release-access-bearer on-ready-to-standby` will display in the output generated by the `show configuration [ verbose ]` command.

- **remove**: When included with the command, `remove` disables sending Release Access Bearer in either the selected (with optional keyword) 2G or 3G environment or both environments (with no keyword included).

- By default, Release Access Bearer initiation on Iu-Release or Ready-to-Standby transition is not enabled. When disabled or prior to being enabled, either/both `remove release-access-bearer on-iu-release` or/and `remove release-access-bearer on-ready-to-standby` will display in the output generated by the `show configuration [ verbose ]` command.

---

**CSCud63677, CSCui21269, CSCuh77293 - SM application changes for PGW restart notification**

**Feature Changes**

**P-GW Restart Notification**

The purpose of enabling PGW Restart Notification (PRN) in S4-SGSN is to provide a simple and optimized solution for handling the signaling overload on SGSN when a PGW failure occurs. Until release 10, an SGW used to send Delete Bearer Request for every PDN connection activated through the failed PGW. This will cause a signaling overload on SGSN. Since 3GPP Release 10 specifications, it is possible for an SGW to indicate a PGW failure through a single PGW Restart Notification message to an SGSN.

When an SGW detects that a peer PGW has restarted it shall delete all PDN connections bearer contexts associated with the peer node that fails as well as freeing any internal SGW resources associated with those PDN connections.

An SGW will send PGW Restart Notification only to the SGSN's that indicated their support through the Echo Request -> Node Features IE -> PRN bit. When the S4-SGSN receives this message, according to the control plane IP address of the restarted PGW and the control plane IP address of the SGW on the S4 interface included in the message, S4-SGSN should delete all PDN connection contexts associated with the SGW and the restarted PGW as well as freeing any internal resources associated with those PDN connections.

The S4-SGSN sends a PGW Restart Notification Acknowledge message in response to the PGW Restart Notification message sent by SGW.

**Previous Behavior**: PGW Restart Notification (PRN) is not enabled on S4-SGSN.

**New Behavior**: PGW Restart Notification is now enabled on S4-SGSN.
Command Changes

gtpc

This is an existing command, now supported by S4-SGSN. The command option **node-feature pgw-restart-notification** has to be configured in order to inform SGW that S4-SGSN supports receiving PRN.

configure

    context context_name
    egtp_service service_name

        gtpc { allow-on-congestion { apn-name apn_name | arp priority_level } | bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval seconds [ dynamic [ smooth-factor multiplier ] ] | echo-retransmission-timeout seconds | error-response-handling | ip qos-dscp { forwarding_type } | max-retransmissions num | node-feature pgw-restart-notification | path-failure detection-policy echo | private-extension overcharge-protection | retransmission-timeout seconds }

    no gtpc { allow-on-congestion { apn-name apn_name | arp priority_level } | bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval | error-response-handling | node-feature pgw-restart-notification | path-failure detection-policy | private-extension overcharge-protection }

    default gtpc { echo-interval | echo-retransmission-timeout | ip qos-dscp | max-retransmissions | node-feature pgw-restart-notification | path-failure detection-policy | retransmission-timeout }

end

apn-restoration priority

This new command is used to configure the APN restoration priority value.

configure

    apn-profile profile_name

        apn-restoration priority priority_value

    remove apn-restoration priority

end

Notes:

- The PGW Restart Notification (PRN) message is sent by the S-GW when it detects a peer P-GW has re-started. The S4-SGSN on receiving the PRN message, uses the default apn-restoration priority value, if priority value is not available in HSS Subscription to prioritize the affected PDN connections for restoration. To restore PDN it is mandatory to get priority value from HSS in subscription record or default value must be configured under apn-profile.
• The priority value is an integer value from 1 through 16. Where “1” is the highest priority and “16” is the lowest priority.

Performance Indicator Changes

show s4-sgsn statistics

The following PDP Deletion Statistics have been added to the `show s4-sgsn statistics` command:
• 3G S4 PDPs Deleted due to PGW Restart Notification
• 2G S4 PDPs Deleted due to PGW Restart Notification

show egtpc statistics

The following PGW Restart Notification statistics have been added to `show egtpc statistics`:
• PGW Restart Notification Request
• Total RX
• Initial RX
• Retrans RX
• PGW Restart Notification Ack
• Total TX
• Initial TX
• Accepted
• Denied
• Discarded

Notes:
• When APN Restoration priority value is available, either through local configuration or through subscription received from HSS, then the SGSN sends Deactivation Request with SM Cause "Reactivation Required" towards MS after PGW Restart Notification Request from SGW.
• When APN Restoration priority value is not available and the subscriber is in Idle/Standby state, the SGSN deletes the affected bearers locally and does not trigger Paging Request towards the MS to send Deactivation Request.
• When APN Restoration priority value is not available and the subscriber is in Connected/Ready state, the SGSN will send Deactivation Request.

show session disconnect-reasons verbose

The following disconnect reason is used to track both PGW Restart or path failure and SGW path failure:
• sgsn-gtpc-path-failure(267)
CSCud72320 - Allow unknown equipment on SGSN

Feature Changes

Support for Handling Unknown Equipment

Previous Behavior: In certain scenarios when EIR returns equipment status as “UNKNOWN_EQUIPMENT” in response to CHECK_IMEI requests, SGSN returns a failure and the ATTACH/RAU does not succeed. Unknown equipment's were not allowed in SGSN.

New Behavior: To support unknown equipment handling in SGSN, a new CLI option allow-unknown has been added in the gmm retrieve-equipment-identity command under the Call Control Profile configuration. Based on the configuration of this command the SGSN either accepts or rejects the requests from unknown equipment. If this option is configured, SGSN will ignore the “UNKNOWN_EQUIPMENT” equipment status received from EIR and will allow the call to continue, otherwise if the keyword is not configured in cli, SGSN will reject the unknown equipment as per its default behavior.

Command Changes

gmm retrieve-equipment-identity

A new keyword allow-unknown is added to the gmm retrieve-equipment-identity to support handling of unknown equipment. If this keyword is configured the SGSN allows requests from unknown equipment. This keyword is not configured by default.

configure

call-control-profile profile_name

gmm retrieve-equipment-identity { imei | imeisv [ unciphered ] [ then-imei ] } [ verify-equipment-identity [ deny-greylisted ] [ allow-unknown ] ]

default gmm retrieve-equipment-identity
end

CSCuh75222 - SGSN to display number of HSPA subscribers

Feature Changes

High Speed Pack Access (HSPA) Subscribers Statistics Added

Previous Behavior: The SGSN does not display any statistics related to High Speed Pack Access (HSPA) subscribers.

New Behavior: The SGSN now displays the statistics of High Speed Pack Access (HSPA) subscribers. The SGSN displays the breakdown of HSPA subscribers into different negotiated MBR ranges such as 16-32 Mbps, 32-64 Mbps, 64-128 Mbps and 128-256 Mbps. The SGSN uses the negotiated downlink MBR value to derive these statistics. This enhancement is currently supported only on Gn SGSN for 3G or UMTS subscribers. The show command show gmm-sm statistics is updated with new statistics and new bulk statistics are added to the SGSN schema to support this feature enhancement.
Performance Indicator Changes

SGSN Schema

The following new bulk statistics have been added in the SGSN Schema to support the display HSPA subscriber statistics:

- `actsubs-16-32-mbps`
- `actsubs-32-64-mbps`
- `actsubs-64-128-mbps`
- `actsubs-128-256-mbps`
- `actctx-16-32-mbps`
- `actctx-32-64-mbps`
- `actctx-64-128-mbps`
- `actctx-128-256-mbps`

The following new counters have been added in the show command `show gmm-sm statistics` to support the display HSPA subscriber statistics:

- Activated HSPA Subscribers
- Activated HSPA subscribers (16-32Mbps)
- Activated HSPA subscribers (32-64Mbps)
- Activated HSPA subscribers (64-128Mbps)
- Activated HSPA subscribers (128-256Mbps)
- Activated HSPA PDP Contexts
- Activated HSPA PDP Contexts (16-32Mbps)
- Activated HSPA PDP Contexts (32-64Mbps)
- Activated HSPA PDP Contexts (64-128Mbps)
- Activated HSPA PDP Contexts (128-256Mbps)

CSCuh89000 - S6d/Gr interface selection based on UE capability

Feature Changes

Interface Selection Based on UE Capability

Currently the SGSN selects either the S6d interface or the Gr interface based on whether HSS- Peer Service or MAP Service is configured in call control profile. If both are associated, then the selection is based on the `prefer subscription-interface` configuration in the call control profile. If MAP and HSS services are not configured under call control profile then SGSN and GPRS services are checked to select the interface. With this feature
enhancement, the SGSN now allows selection of S6d interface only if the UE is EPC capable. A new CLI option \texttt{epc-ue} is added to the command prefer subscription-interface under the Call Control Profile mode for this enhancement. If this keyword is configured the S6d interface is selected only if UE is EPC capable. If this keyword is not configured then SGSN follows existing logic for interface selection.

**Previous Behavior:** The SGSN does not have specific CLI configuration to enable selection HSS interface for EPC UEs.

**New Behavior:** A new CLI option is introduced in the \texttt{prefer subscription-interface} command under the Call Control Profile mode to enable selection of an HSS interface for EPC UEs.

**Customer Impact:** Increased accuracy of interface selection.

### Command Changes

\texttt{prefer subscription-interface}

A new keyword \texttt{epc-ue} is introduced to enable selection of selection of HSS interface only for EPC capable subscribers.

\texttt{configure}

\texttt{call-control-profile profile_name}

\texttt{prefer subscription-interface \{ hlr | hss [ epc-ue ] \}}

\texttt{end}

**Notes:**
- Configure this keyword to select the HSS interface for EPC capable subscribers. For other subscribers the MAP interface will be selected.
- This keyword will be applicable only when both MAP and HSS interfaces are configured in the Call-control profile. If this keyword is not configured then SGSN follows existing logic for interface selection.

### Performance Indicator Changes

\texttt{show configuration}

The \texttt{show configuration} displays \texttt{prefer subscription-interface hss epc-ue} if \texttt{epc-ue} is configured under the Call Control Profile.

\texttt{show call-control-profile full all}

The preferred subscription interface is displayed as \texttt{Preferred Subscription Interface : hss for epc-ue} if \texttt{prefer subscription-interface hss epc-ue} is configured under the Call Control Profile.
CSCuj88489 - Enhancement for SGSN behavior with RAU response

Feature Changes

Follow On Proceed (FOP) Bit in RAU Accept Messages

The SGSN behavior in setting the Follow On Proceed (FOP) bit in Routing Area Update message is now modified as per the 3GPP TS 24.008 (Release 11, Version 11.11.0, Section 4.7.5.1.3). In Iu mode, if the network wishes to prolong the PS signaling connection (for example, if the mobile station has indicated “follow-on request pending” in ROUTING AREA UPDATE REQUEST message) the network shall indicate the “follow-on proceed” in the ROUTING AREA UPDATE ACCEPT message. If the network wishes to release the PS signalling connection, the network shall indicate “no follow-on proceed” in the ROUTING AREA UPDATE ACCEPT message.

Previous Behavior: The SGSN sets the FOP bit to “0” in Routing Area Update Accept Message in the following scenarios:
- If UE indicated “follow-on request pending” in Routing Area Update Request.
- In iups-service, “iu-hold-connection always” is configured.

New Behavior: A new CLI command `gmm rau-accept` has been introduced in the Call Control Profile mode, when this CLI is enabled the FOP bit is set to “0” in the following scenarios:
- If UE indicated “follow-on request pending” in Routing Area Update Request.
- In Iu-service, “iu-hold-connection always” is configured.
- If RAB was setup by SGSN as part of SRNS or RAU.
- If there was a follow on network initiated procedure (HLR or GGSN init modification) following RAU procedure (in release 17.0 this is supported for only new SGSN RAU and new SGSN SRNS scenarios).

If the new CLI command is disabled, no change in SGSN behavior will be observed. The SGSN will set the FOP bit to “0”, if UE indicated “follow-on request pending” in Routing Area Update Request or if in iups-service, “iu-hold-connection always” is configured.

Command Changes

`gmm rau-accept`

A new command `gmm rau-accept` is introduced, this command provides the configuration to set the Follow-On Proceed (FOP) bit in the Routing Area Update Accept (RAU) message.

```
configure

call-control-profile profile_name

    gmm rau-accept follow-on-proceed { on-following-nw-procedure | only-on-ue-request }

remove gmm rau-accept follow-on-proceed

end
```

Notes:
Use this command to configure the setting of Follow On Proceed bit in Routing Area Accept Message. The FOP bit can be set only when the UE requests for it by configuring the command option `only-on-ue-request` or the FOP bit can be set when there is a following network procedure by configuring the CLI option `on-following-nw-procedure`. By default, the configuration is `gmm rau-accept follow-on-proceed only-on-ue-request`.

CSCul17198, CSCul17195 - GTP echo and GTP message retry number shall be configured separately.

Feature Changes

Separate Configuration for GTP Echo and GTP Message Retry Numbers

Previously, the GTP echo and GTP message retry timer could be configured separately, but the number of GTPC echo requests could not. The maximum retry number can now be configured separately along similar lines as the timer configuration. Both in egtp-service and peer-profile modes, the `echo-max-retransmissions` keyword is added to allow the separate configuration of GTPC echo retransmissions.

**Previous Behavior:** The `max-retry` option is common for both GTPC Service Configuration Mode and Peer-Profile Configuration modes.

**New Behavior:** The `echo-max-retransmissions` is introduced explicitly for the configuration of echo max re-transmissions in both GTPC Service Configuration Mode and Peer-Profile Configuration Mode.

Command Changes

```plaintext
echo-max-retransmissions

The `echo-max-retransmissions` keyword is now available in both EGTP Service Configuration Mode and Peer Profile Configuration Mode. This keyword is available to allow for the separate configuration of GTP echo retransmissions in each mode.

```configure

```
context context_name

egtp-service egtp_service_name
gtpc echo-max-retransmissions number

default gtpc echo-max-retransmissions
end
```

```configure

peer-profile service-type service_type

egtp-service egtp_service_name
gtpc echo-max-retransmissions number

default gtpc echo-max-retransmissions
end
```
Notes:

**echo-max-retransmissions**: Configures the maximum retries for GTP Echo requests. This option must be an integer from 0 to 15. The default is 4. If echo-max-retransmissions configuration option is not configured, then the max-retransmissions configuration will be used for maximum number of echo retries.

**Performance Indicator Changes**

*show egtp-service [ all | name service_name ]*

The output of this command has been enhanced to show the configured number of GTPC echo max retransmissions.

- GTPC Echo Max Retransmission

*show peer-profile full [ all | name service_name ]*

The output of this command has been enhanced to show the configured number of GTPC echo max re-transmissions.

- GTPC Echo Max Retransmission

**CSCul29734 - Support of pooled and non-pooled RNCs/BSCs**

**Feature Changes**

**Different NRIs for Pooled and Non-pooled RNCs/BSCs**

The SGSN adds support for configuring different NRIs for pooled and non-pooled areas in order to load-balance subscribers coming from non-pooled RNCs to pooled RNCs.

Consider a scenario when two SGSNs support pooling and a RNC/BSC controlled by a SGSN is in pool but not the other, and both RNCs/BSCs are given same NRI(s), this leads to imbalance in subscriber distribution between the SGSNs. With this enhancement if an NRI is configured for both pooled and non-pooled, then the SGSN reuses the same NRI when moving from pooled to non-pooled areas and vice versa.

A new keyword **non-pooled-nri-value** is introduced in the NRI configuration for GPRS and SGSN services to configure set of NRI which should be used for non-pooled RNCs/BSCs. The NRIs configured under the existing keyword **nri-value** will be used for pooled RNCs/BSCs. If the new keyword **non-pooled-nri-value** is not configured, then NRIs configured under the keyword **nri-value** will be used for both pooled and non-pooled RNCs/BSCs.

If the new keyword **non-pooled-nri-value** is configured without pooling enabled at SGSN (null-nri-value is not configured), then SGSN will use NRIs under **non-pooled-nri-value** irrespective of BSC/RNCs being pooled or non-pooled, till pooling is enabled at SGSN. After pooling is enabled, NRIs under keyword **nri-value** will be for pooled RNC/BSCs and **non-pooled-nri-value** will be for non-pooled RNC/BSCs. This is applicable for both SGSN and GPRS service.

**Previous Behavior**: It is not possible to configure different NRIs for pooled and non-pooled areas.

**New Behavior**: The SGSN now allows configuring different NRIs for pooled and non-pooled areas. A new keyword **non-pooled-nri-value** is introduced in NRI configuration for GPRS and SGSN services to specify NRI(s) for non-pooled areas.

**Customer Impact**: Enables the re-balancing of resources between pooled and non-pooled RNCs to enhance operational efficiency.
Command Changes

nri

The `nri` command in the GPRS service is updated to include a new keyword `non-pooled-nri-value` to enable configuration of values of NRIs to be used for non-pooled area.

```
configure
   context  context_name
       gprs-service  service_name
           nri length  nri_length  { nri-value  nri_value  | null-nri-value  null_nri_value
           non-broadcast-lac  lac_id  rac  rac_id  [ nri-value  value  ][ non-pooled-nri-value  value ] }
end
```

Notes:
- The same NRI can be configured using both the keywords `nri-value` and `non-pooled-nri-value`, this implies the NRI can be used either in pooled area or non-pooled area. If an NRI is configured for both pooled and non-pooled areas, then the SGSN re-uses the same NRI when moving from pooled to non-pooled areas and vice versa.
- The NRIs configured using the `nri-value` keyword will be used only in pooled area if the keyword `non-pooled-nri-value` is configured, else the NRIs configured using the `nri-value` keyword will be used for both pooled and non-pooled areas.

nri length

The `nri length` command in the SGSN service is updated to include a new keyword `non-pooled-nri-value` to enable configuration of values of NRIs to be used for non-pooled area.

```
configure
   context  context_name
       sgsn-service  service_name
           nri length  nri_length  [ nri-value  nri_value  | null-nri-value  null_nri_value
           non-broadcast  mcc  mnc  mcc  mnc  lac  lac_id  rac  rac_id  nri-value  value  non-pooled-nri-value  value ]
end
```

Notes:
- The same NRI can be configured using both the keywords `nri-value` and `non-pooled-nri-value`, this implies the NRI can be used either in pooled area or non-pooled area. If an NRI is configured for both pooled and non-pooled areas, then the SGSN re-uses the same NRI when moving from pooled to non-pooled areas and vice versa.
• The NRIs configured using the **nri-value** keyword will be used only in pooled area if the keyword **non-pooled-nri-value** is configured, else the NRIs configured using the **nri-value** keyword will be used for both pooled and non-pooled areas.

**Performance Indicator Changes**

**show gprs-service**

The following new parameters are added to the *show gprs-service* command to display statistics related to NRIs configured for Pooled and Non-pooled RNCs/BSCs:

- NRI(s) that will be used in NON-POOLED area
- Gprs NRI value
- NRI(s) that will be used in POOLED area
- NRI(s) that will be used in POOLED & NON-POOLED area

**show sgsn-service**

The following new parameters are added to the *show sgsn-service* command to display statistics related to NRIs configured for Pooled and Non-pooled RNCs/BSCs:

- NRI(s) that will be used in NON-POOLED area
- Sgsn NRI value
- NRI(s) that will be used in POOLED area
- NRI(s) that will be used in POOLED & NON-POOLED area

**CSCul86798 - SGSN per RA level stats**

**Feature Changes**

**Pegging Key 2G Statistics at the RA Level**

**Previous Behavior:** SGSN GMM-SM statistics for Ongoing-procedure failures and internal failures during Attach, Inter RAU and Intra RAU procedures, are not being displayed at the Routing Area (RA) Level. The counters are currently pegged only at the service level. Bulk statistics variables are not available for counters related to internal failures during Inter RAU and Intra RAU procedures, and there is no support to peg the counters at the RA level, in all the relevant scenarios.

**New Behavior:** SGSN GMM-SM statistics for Ongoing-procedure failures and internal failures during Attach, Inter RAU and Intra RAU procedures, are now available at the Routing Area Level. Support has been added to peg the following counters at the RA level:

- attach\_2g\_simp\_fail\_internal\_failure
- attach\_2g\_comb\_fail\_internal\_failure
- attach\_2g\_simp\_fail\_ongoing\_proc
- attach\_2g\_comb\_fail\_ongoing\_proc
• inter_rau_2g_simp_fail_internal_failure
• inter_rau_2g_simp_fail_ongoing_proc
• inter_rau_2g_comb_fail_ongoing_proc
• inter_rau_2g_comb_fail_internal_failure
• intra_rau_2g_simp_fail_internal_failure
• intra_rau_2g_simp_fail_ongoing_proc
• intra_rau_2g_comb_fail_ongoing_proc
• intra_rau_2g_comb_fail_internal_failure

The following bulk statistics variables were present, but were not being pegged at RA level. Support has been added to peg these appropriately:

• 2G-attach-fail-ongoing-proc
• 2G-attach-fail-ongoing-proc-comb
• 2G-inter-rau-fail-ongoing-proc
• 2G-inter-comb-rau-fail-ongoing-proc
• 2G-intra-ra-upd-rau-fail-ongoing-proc
• 2G-intra-comb-rau-fail-ongoing-proc
• 2G-attach-fail-internal-failure
• 2G-attach-fail-comb-internal-failure

The following bulk statistics counters have been newly introduced and support has been added to peg these appropriately:

• 2G-inter-rau-fail-internal-failure
• 2G-inter-rau-fail-comb-internal-failure
• 2G-intra-ra-fail-internal-failure
• 2G-intra-ra-fail-comb-internal-failure

Performance Indicator Changes

SGSN Schema

The following new bulk statistics have been added:

• 2G-inter-rau-fail-internal-failure
• 2G-inter-rau-fail-comb-internal-failure
• 2G-intra-ra-fail-internal-failure
• 2G-intra-ra-fail-comb-internal-failure
CSCum14414 - Inconsistency seen when Deactivate sent with and without tear down

Feature Changes

Reduced Signaling to MS during 3G Intra-SRNS

This behavior change relates to the SGSN’s response to the uplink signaling message from the MS when intra SRNS is in progress in a 3G environment.

Previous Behavior: For the MS-initiated PDP Deactivation Request, without tear down set during intra SRNS in 3G, SGSN responded with an SM Status message with cause = 98.

New Behavior: For the MS initiated PDP Deactivation Request, without/with tear down set during intra SRNS in 3G, the SGSN now ignores the message and displays an sm-app level warning log if logging is enabled.

Customer Impact: In the scenario noted above, now there will be no unnecessary signaling towards the MS for an old Iu and corresponding counters tracking the number of outbound SM Status messages will not be pegged.

CSCum47774, CSCum50056 - M2M Features to be supported by SGSN

Feature Changes

Machine Type Communications Support on the SGSN

With this StarOS release, the SGSN supports several of the 3GPP TS23.060 R10 machine type communications (MTC) overload control mechanisms to be used in the handling of signaling bursts from machine-to-machine (M2M) devices. The MTC mechanisms the SGSN will now support are:

- MTC Congestion Control - This functionality enhances the SGSN’s support for congestion control so that the SGSN can reject or drop Requests based on
  - the LAPI (low access priority indicator) indicated by the subscriber, and/or
  - the APN.

- APN-based Congestion Control - APN-based Mobility Management (MM) or Session Management (SM) congestion control allows the operator to restrict the load from the UEs based on Subscribed APN.

- General or Global NAS (Network Access Stratum) Congestion Control - applicable only for MM (Mobility Management) messages.

- Subscribed Periodic RAU/TAU Timer (Extended T3312 Timer), refer to CSCum67205 for details. As well, the SGSN now supports the Subscribed Periodic RAU/TAU Timer Withdrawn flag in MAP DSD (Delete Subscriber Data) messages, refer to CSCuo92276 for additional information on this flag and relevance to the Subscribed Periodic RAU/TAU Timer.

- Reject Causes with MM (Mobility Management) T3346 - MM Backoff Timer and SM (Session Management) T3396 - SM Backoff Timer - Under congestion, the SGSN can assign MM or SM backoff timers to the UEs and request the UE not to access the network for a given period of time.

- Low Access Priority Indicator (LAPI) in S-CDRs - The SGSN now allows for the use of the LAPI bit in S-CDRs of the custom24 dictionary. Use of this functionality is CLI controlled. For details about this new functionality, refer to the GTPP Enhancements for 17.0 section of these Release Notes.
This feature set allows the operator to handle the signaling storm, that MTC devices can bring to the network, thus ensuring a more robust network and more efficient resource utilization.

The operator defines the congestion-detection thresholds for each of the three congestion levels (critical, major, minor) for:

- **system CPU utilization** - this is applicable to congestion control for both MM and SM messages (only APN-based congestion control for SM messages).
- **system memory utilization** - this is applicable to congestion control for MM messages.
- **service control CPU utilization** - this is applicable to congestion control for MM messages.

Thresholds are defined using the existing (unmodified) `congestion-control threshold` command in the Global Configuration mode.

**Important:** For SM congestion to work, the **apn-based** option must be configured with the **sm-messages reject** command (please see information in Command Changes section below).

### Command Changes

A range of new commands or new keywords (for existing commands) have been created to enable you to configure and control the various MTC congestion control functionalities. The commands and keywords are briefly described below. For more detail about the congestion control commands, refer to the *Command Line Interface Reference: Version 17* or higher. For more information about the MTC Congestion Control feature and the various supported functionalities, refer to the *MTC Congestion Control* chapter in the *SGSN Administration Guide*.

**congestion-control**

This Global Configuration mode command enables or disables global congestion control for the SGSN and the IMSIMgr. The syntax for this command has not been modified but the underlying behavior of the command has been expanded to enable support for the SGSN’s new congestion-control functionalities.

**Important:** Enabling global congestion control with this `congestion-control` command is mandatory for any congestion control functionality to be enabled.

**configure**

```
congestion-control

no congestion-control

end
```

Notes:

- **no**: Disables global congestion control when this filter is added to the command.
- Either ‘enabled’ or ‘disabled’ displays as the configured congestion-control status in the first line of the output of the `show congestion-control configuration` command.

**congestion-control policy**
With the modified **policy** keyword, the operator associates the SGSN’s congestion-response action-profile with each of 3 possible levels of congestion - critical, major, and minor.

```plaintext
configure

congestion-control policy { critical | major | minor } sgsn-service action-profile
action_profile_name

no congestion-control policy { critical | major | minor } sgsn-service

end
```

Notes:

- **no**: Removes the configured congestion-control policy information.
- **critical | major | minor**: Identifies the level of congestion to associate with a congestion-control response policy. The threshold levels for critical, major and minor congestion levels are all set using the `congestion-control_threshold`.
- **sgsn-service**: Identifies the StarOS service type; in this case, the SGSN (Gn-SGSN and/or S4-SGSN).
- **action_profile_name**: Enter a string of 1 to 64 alphanumeric characters to identify the congestion-action-profile to associate with the congestion-control policy. Refer to the `congestion-action-profile` command in the SGSN-Global Configuration mode to create or review the congestion-action-profiles which define the congestion response actions to be taken when thresholds are exceeded for the SGSN.
- This command can be repeated to associate a congestion-action-profile for each level of congestion severity: critical, major, minor.
- Use the `show congestion-control configuration` command to display the SGSN’s congestion-control policy with the congestion-action-profile names association with the level of congestion severity; for example:

```
sgsn-service:

Critical Action-profile : actprof1
```

**congestion-control**

New configuration command in the SGSN-Global configuration mode define congestion control practices for the SGSN as a whole. All of the new modes and commands within the SGSN-Global configuration mode will be identified and defined in this section.

**Important**: Remember, it is the **congestion-control** command in the Global Configuration mode that enables/disables congestion control.

```plaintext
configure

sgsn-global

congestion-control

[ no ] congestion-action-profile action_profile_name

end
```
Notes:
- A maximum of 16 action-profiles can be defined.
- no: When this filter is added to the command, the SGSN deletes the congestion-control-profile from the configuration.
- congestion-control: Opens the Congestion-Control configuration mode, in which the congestion control action-profile can be created.
- congestion-action-profile action_profile_name: Enter a string of 1 to 64 alphanumeric characters to create or identify a congestion-action-profile and/or to open the Congestion-Action-Profile configuration mode, which accesses the commands that define the congestion responses for:
  - active calls
  - new calls
  - SM messages
- Use the show sgsn-mode command to display the SGSN’s congestion-control configuration defined with the command listed above.

active-call-policy

This command instructs the SGSN to drop or reject any active call messages when congestion occurs during an active call. The active call instructions in the congestion-action-profile can be refined to only drop or reject active call messages with LAPI.

configure
sgsn-global
congestion-control
congestion-action-profile action_profile_name
active-call-policy { rau | service-req } { drop | reject } [ low-priority-ind-ue ]

no active-call-policy { rau | service-req }

Notes:
- no: When this filter is added to the command, the SGSN deletes the active call policy definitions from the congestion-action-profile.
- rau | service-req: Defines congestion response for Routing Area Update messages or Service Request messages.
- drop | reject: Defines the congestion response action, drop or reject, to be taken when RAU or Service Request messages are received during an active call.
- low-priority-ind-ue: Instructs the SGSN to only take defined action if messages include LAPI.
- Use the show sgsn-mode command to display the SGSN’s congestion-control configuration defined with the command listed above.

new-call-policy
This command instructs the SGSN to drop or reject any new calls (Attach Request messages or new Inter SGSN RAU messages) if new call messages are received during congestion. The new call instructions in the congestion-action-profile can be refined to only drop or reject new call messages with low access priority indicator (LAPI).

```
configure
sgsn-global
  congestion-control
  congestion-action-profile action_profile_name
    new-call-policy { drop | reject } [ low-priority-ind-ue ] [ apn-based ]
    no new-call-policy
```

Notes:
- **no**: When this filter is added to the command, the SGSN deletes the new call policy definitions from the congestion-action-profile.
- **drop | reject**: Defines the congestion response action, drop or reject, to be taken when new call (Attach Request or new Inter SGSN RAU) messages are received during congestion.
- **low-priority-ind-ue**: Instructs the SGSN to only take defined action if messages include low access priority indicator (LAPI).
- **apn-based**: Instructs the SGSN to reject a new call based on the subscribed APN if congestion control is configured for that APN under an applicable Operator Policy.
- If both the LAPI and APN-based options are included in the action-profile, then the call event will only be rejected if both conditions are matched.
- Use the `show sgsn-mode` command to display the SGSN’s congestion-control configuration defined with the command listed above.

```
sm-messages
```

This command instructs the SGSN to reject any SM signaling messages (activation or modification) during congestion. The congestion-action-profile parameter can be refined to only reject SM signaling messages with LAPI.

```
configure
sgsn-global
  congestion-control
  congestion-action-profile action_profile_name
    sm-messages reject [ low-priority-ind-ue ] [ apn-based ]
    no sm-messages
```

Notes:
- **no**: When this filter is added to the command, the SGSN deletes the sm-messages definition from the congestion-action-profile.
• **low-priority-ind-ue**: Instructs the SGSN to only take defined action if messages include low access priority indicator (LAPI).

• **apn-based**: Instructs the SGSN to reject sm-messages based on the APN if congestion control is configured for that APN under an applicable Operator Policy.

• If both the LAPI and APN-based options are included in the action-profile, then the call event will only be rejected if both conditions are matched.

• Use the `show sgsn-mode` command to display the SGSN’s congestion-control configuration defined with the command listed above.

**apn**

A new keyword, *congestion-control*, enables the operator to associate congestion control functionality with a specific APN so that congestion responses can be applied per APN.

**configure**

```
operator-policy name op_policy_name

[ no ] apn network-identifier apn_name congestion-control

end
```

Notes:

• **no**: When this filter is added to the command, the SGSN deletes the APN network-identifier configuration associated with congestion control from the Operator Policy.

• **op_policy_name**: Enter a string of 1 to 64 alphanumeric characters to create or identify an operator policy.

• **apn_name**: Enter a string of 1 to 63 characters, including dots (.) and dashes (-), to identify a specific APN network ID.

• **congestion-control**: Including this keyword associates congestion control functionality with the identified APN.

• During an Attach Request, new Inter SGSN RAU, or when receiving sm-messages, all subscribed APNs for mobility management (MM) or selected APNs for session management (SM) will be checked to determine if any of them is configured for congestion control, in which case the new call or sm-messages would be rejected.

**sgsn trigger-congestion**

For operations and maintenance purposes (e.g., testing), this command triggers a congestion state at the global level.

```
sgsn trigger-congestion level { critical | major | minor }
```

Notes:

• **critical | major | minor**: Selecting one of the three congestion severity levels indicates the associated congestion-action-profile to be chosen and applied. Reminder: the profile is associated with the severity level with the `congestion-control policy` command.

**sgsn clear congestion**

For operations and maintenance purposes (e.g., testing), this command clears congestion triggered using the `sgsn trigger congestion` command.
sgsn clear-congestion

Notes:
- If the command is applied then the SGSN resumes normal operations and does not apply any congestion control policy.

gmm t3346

The `gmm` command includes a new keyword to set the MM T3346 backoff timer for either or both the GPRS Service (2G) and/or SGSN Service (3G).

configure

context context_name

{ gprs-service | sgsn-service } service_name

  gmm t3346 min minimum_minutes max maximum_minutes

  no gmm t3346

end

Notes:
- `no`: Including this filter with the command removes the MM backoff timer definition from the service configuration.
- `minimum_minutes`: Enter an integer from 1 to 15 to identify the minimum number of minutes; default is 15 minutes.
- `maximum_minutes`: Enter an integer from 1 to 30 to identify the maximum number of minutes; default is 30 minutes.
- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The MM backoff timer value sent will be chosen randomly from within the configured T3346 timer value range.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.
- If T3346 timer value is configured in a Call-Control Profile then that value will override the backoff timer values defined for this GPRS Service configurations.

gmm t3346

The `gmm` command includes a new keyword to set the MM T3346 backoff timer for a Call-Control Profile.

configure

call-control-profile ccpolicy_name

  gmm t3346 min minimum_minutes max maximum_minutes

  no gmm t3346

end
Notes:

- **no**: Including this filter with the command removes the MM backoff timer definition from the Call-Control Profile configuration.

- **minimum_minutes**: Enter an integer from 1 to 15 to identify the minimum number of minutes; default is 15 minutes.

- **maximum_minutes**: Enter an integer from 1 to 30 to identify the maximum number of minutes; default is 30 minutes.

- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The backoff timer value sent will be chosen randomly from within the configured T3346 timer value range.

- If T3346 timer value is configured in a Call-Control Profile then it will override the backoff timer values defined for either the SGSN Service or GPRS Service configurations.

- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.

**sm t3396**

The `sm` command includes a new keyword to set the SM T3396 backoff timer for either or both the GPRS Service (2G) and/or SGSN Service (3G).

```
configure

context context_name

{ gprs-service | sgsn-service } service_name

    sm t3396 min minimum_minutes max maximum_minutes cause cause_code

    no sm t3396

end
```

Notes:

- **no**: Including this filter with the command removes the SM backoff timer definition from the Service configuration.

- **minimum_minutes**: Enter an integer from 1 to 15 to identify the minimum number of minutes; default is 15 minutes.

- **maximum_minutes**: Enter an integer from 1 to 4320 to identify the maximum number of minutes.

- **cause_code**: Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.

- The command can be repeated to define a maximum of 16 cause codes.

- During congestion, the SGSN randomly chooses a T3396 value from the configured range and sends that timer value to the UE in the Reject message with the cause code #26.

**sm t3396**

The `sm` command includes a new keyword to set the SM T3396 backoff timer for the APN Profile.
configure

apn-profile profile_name

   sm t3396 min minimum_minutes max maximum_minutes cause cause_code

   remove sm t3396

   end

Notes:

- **remove**: Including this filter with the command removes the SM backoff timer definition from the APN Profile configuration.
- **minimum_minutes**: Enter an integer from 1 to 15 to identify the minimum number of minutes; default is 15 minutes.
- **maximum_minutes**: Enter an integer from 1 to 4320 to identify the maximum number of minutes.
- **cause_code**: Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.
- The command can be repeated to define a maximum of 16 cause codes.
- During congestion, the SGSN randomly chooses a T3396 value from the configured range and sends that timer value to the UE in the Reject message with the cause code #26.
- T3396 configured in an APN Profile will override a T3396 value configured for either an SGSN Service or a GPRS Service.

Performance Indicator Changes

Counters and Stats

For a list of new congestion control statistics and display counters, please refer to CSCup11529 and CSCup71741.

Disconnect Reasons

For information on disconnect reason(s) created to support the MTC functionality, refer to CSCup82824.

CSCum62444 - SGSN to backup counters and recover them after session manager crash

Feature Changes

Backup and Recovery of Key KPI Statistics

**Previous Behavior**: The counter values were not recovered after a session manager crash, hence the KPI values which depend on these counter values were affected. Backing up all possible counters is not feasible as this would have an impact on memory and also on session recovery time.
New Behavior: This feature allows the backup of a small set of KPI counters for recovery of the counter values after a session manager crash.

Using the new statistics-backup sgsn backup-interval command, in the Global configuration mode, the operator can enable the feature and define the frequency of the backup; range 1-60 minutes.

In support of this new functionality, four new schemas have been defined with stats, derived from the SGSN and SGTP schemas, that will be backed up for recovery.

Table 1. New Backup Statistics Schemas

<table>
<thead>
<tr>
<th>Schemas</th>
<th>Keys</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iups-bk</td>
<td>vpn-id</td>
<td>This schema is used for 3G GMM-SM counters which are backed up. The counters in this schema are pegged per IuPS service. Each line of output is per IuPS service. Additionally, there will be one set of consolidated counters for all IuPS services which is displayed with the SGSN service name.</td>
</tr>
<tr>
<td></td>
<td>vpnname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>servname</td>
<td></td>
</tr>
<tr>
<td>gprs-bk</td>
<td>vpn-id</td>
<td>This schema is used for 2G GMM-SM counters which are backed up. The counters in this schema are pegged per GPRS service. Each line of output is per GPRS service. Additionally, there will be one set of consolidated counters for all GPRS services which is displayed with the SGSN service name.</td>
</tr>
<tr>
<td></td>
<td>vpnname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>servname</td>
<td></td>
</tr>
<tr>
<td>map-bk</td>
<td>vpn-id</td>
<td>This schema is used for MAP and SMS counters which are backed up. The counters in this schema are pegged per MAP service. Each line of output is per MAP service.</td>
</tr>
<tr>
<td></td>
<td>vpnname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>servname</td>
<td></td>
</tr>
<tr>
<td>sgp-bk</td>
<td>vpn-id</td>
<td>This schema is used for GTPU counters which are backed up. The counters in this schema are pegged per IuPS and SGTP service, one per line. Additionally, there will be one line of output which represents the counters consolidated for all IuPS and SGTP services.</td>
</tr>
<tr>
<td></td>
<td>vpnname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>servname</td>
<td></td>
</tr>
</tbody>
</table>

Command Changes

statistics-backup sgsn

Using the new statistics-backup sgsn command, in the Global configuration mode, enables this new feature and makes it possible for the operator to optionally define the frequency of the backup; ranging from 1 to 60 minutes:

configure

statistics-backup sgsn [ backup-interval minutes ]

no statistics-backup sgsn

end

Notes:
- backup-interval minutes defines the interval as 1 to 60 minutes, with default of 5 minutes.

Displaying Backed-up Statistics

To view the recovered counter values, a new keyword has been added to the show commands - recovered-values keyword option:

- show gmm-sm statistics [ recovered-values ] [ verbose ]
• show gmm-sm statistics sgsn-service sgsn_service_name [ recovered-values ] [ verbose ]
• show gmm-sm statistics gprs-service gprs_service_name [ recovered-values ] [ verbose ]
• show gmm-sm statistics iups-service iups_service_name [ recovered-values ] [ verbose ]
• show map-statistics [ recovered-values ]
• show map statistics map-service map_service_name [ recovered-values ]
• show sgtpu statistics [ recovered-values ]
• show sgtpu statistics iups-service iups_service_name [ recovered-values ]
• show sgtpu statistics sgtp-service sgtp_service_name [ recovered-values ]
• show sms statistics [ recovered-values ]
• show sms statistics name map_service_name [ recovered-values ]

Notes:
• When the new keyword is used, only the recovered values will be displayed.
• If no session manager crash has occurred, the above commands output displays with the normal counter values.
• If a session manager crash has happened, the above commands display the cumulative value so far (including the backed up value).
• The display of the counters will be similar to the show gmm-sm statistics command output with respect to naming and indentation. Only the subset of counters which are backed up will be displayed with the recovered-values option.

The list of counters and statistics that will be backed up are listed in the section below.

Clearing Backed-up Statistics

To clear the backed-up counter values, use one of the following commands with the new recovered-values keyword option:

• clear gmm-sm statistics [ recovered-values ]
• clear gmm-sm statistics [ recovered-values ] sgsn-service sgsn_service_name
• clear gmm-sm statistics [ recovered-values ] gprs-service gprs_service_name
• clear gmm-sm statistics [ recovered-values ] iups-service iups_service_name
• clear map-statistics [ recovered-values ]
• clear map statistics name map_service_name [ recovered-values ]
• clear sgtpu statistics [ recovered-values ]
• clear sgtpu statistics iups-service iups_service_name [ recovered-values ]
• clear sgtpu statistics sgtp-service sgtp_service_name [ recovered-values ]
• clear sms statistics [ recovered-values ]
• clear sms statistics name map_service_name [ recovered-values ]
SGSN Changes in Release 17

SGSN Enhancements for 17.0

Notes:
- When the new keyword is used, only the recovered values will be cleared.

Performance Indicator Changes

gprs-bk Schema

The following statistics will be backed up for recovery. They are derived from the SGSN schema and perform the same functions as the statistics of similar (with noted exceptions) names minus the -bk extension. For example, the 2G-attached-bk listed below performs the same functions as the 2G-attached statistic in the SGSN schema - unless the SGSN stat exception is noted:

- vpnnname
- vpnid
- servname
- 2G-attached-bk
- 2G-home-subscribers-bk
- 2G-visiting-national-bk
- 2G-visiting-foreign-bk
- 2G-attached-with-pdp-bk
- 2G-total-num-actv-pdp-bk
- 2G-total-num-actv-pdp-on-s4-bk
- 2G-total-attach-req-bk (2G-total-attach-req-all)
- 2G-attach-req-gprs-bk (2G-total-attach-req)
- 2G-attach-req-comb-bk (2G-total-comb-attach-req)
- 2G-attach-req-imsi-gprs-bk (2G-IMSI-Attch)
- 2G-attach-req-imsi-comb-bk (2G-IMSI-Attch-Combined)
- 2G-attach-req-ptmsi-gprs-bk (2G-ptmsi-Attch)
- 2G-attach-req-ptmsi-comb-bk (2G-ptmsi-Attch-Combined)
- 2G-attach-req-local-ptmsi-gprs-bk (2G-local-ptmsi-Attch)
- 2G-attach-req-local-ptmsi-comb-bk (2G-local-ptmsi-Attch-comb)
- 2G-attach-req-remote-ptmsi-gprs-bk (2G-remote-ptmsi-Attch)
- 2G-attach-req-remote-ptmsi-comb-bk (2G-remote-ptmsi-Attch-comb)
- 2G-attach-accept-gprs-bk (2G-attach-accept)
- 2G-attach-accept-comb-bk (2G-comb-attach-accept)
- 2G-attach-reject-bk (2G-attach-reject-all)
- 2G-attach-reject-gprs-bk (2G-attach-reject)
- 2G-attach-reject-comb-bk (2G-attach-reject-comb)
SGSN Enhancements for 17.0

- 2G-attach-rej-imsi-unknown-at-hlr-bk
- 2G-attach-rej-illegal-ms-bk
- 2G-attach-rej-illegal-me-bk
- 2G-gprs-service-not-allowed-bk
- 2G-gprs-and-non-gprs-service-not-allowed-bk
- 2G-attach-rej-msid-not-derived-by-nwt-bk
- 2G-attach-rej-implicitly-detach-bk
- 2G-attach-rej-plmn-not-allowed-bk
- 2G-attach-rej-la-not-allowed-bk
- 2G-roaming-not-allowed-in-this-location-area-bk
- 2G-gprs-service-not-allowed-in-this-plmn-bk
- 2G-no-suitable-cells-in-location-area-bk
- 2G-attach-rej-msc-not-reachable-bk
- 2G-attach-rej-network-failure-bk
- 2G-attach-rej-network-failure-congestion-thrtl-bk
- 2G-attach-rej-network-failure-opr-policy-failure-bk
- 2G-attach-rej-network-failure-ext-bk
- 2G-attach-rej-network-failure-int-bk
- 2G-attach-rej-mac-failure-bk
- 2G-attach-rej-sync-failure-bk
- 2G-attach-rej-congestion-bk
- 2G-attach-rej-gsm-auth-unacceptable-bk
- 2G-attach-rej-no-pdp-ctx-activated-bk
- 2G-attach-rej-retry-from-new-cell-bk
- 2G-attach-rej-sem-wrong-msg-bk
- 2G-attach-rej-invalid-mand-info-bk
- 2G-attach-rej-msg-type-not-exist-bk
- 2G-attach-rej-msg-type-not-comp-prot-state-bk
- 2G-attach-rej-ie-non-existent-bk
- 2G-attach-rej-conditional-ie-err-bk
- 2G-attach-rej-msg-not-comp-prot-state-bk
- 2G-attach-rej-protocol-error-bk
- 2G-attach-rej-unknown-cause-bk
- 2G-comb-attach-rej-imsi-unknown-at-hlr-bk
- 2G-comb-attach-rej-illegal-ms-bk
- 2G-comb-attach-rej-illegal-me-bk
- 2G-comb-gprs-service-not-allowed-bk
- 2G-comb-gprs-and-non-gprs-svc-not-allow-bk
- 2G-comb-attach-rej-implicitly-detach-bk
- 2G-comb-attach-rej-plmn-not-allowed-bk
- 2G-comb-attach-rej-la-not-allowed-bk
- 2G-comb-roam-not-allow-in-loc-area-bk
- 2G-comb-gprs-svc-not-allow-in-plmn-bk
- 2G-comb-no-suitable-cells-in-loc-area-bk
- 2G-comb-attach-rej-msc-not-reachable-bk
- 2G-comb-attach-rej-network-failure-bk
- 2G-comb-attach-rej-network-failure-congestion-thrtl-bk
- 2G-comb-attach-rej-network-failure-opr-policy-failure-bk
- 2G-comb-attach-rej-network-failure-ext-bk
- 2G-comb-attach-rej-network-failure-int-bk
- 2G-comb-attach-rej-mac-failure-bk
- 2G-comb-attach-rej-sync-failure-bk
- 2G-comb-attach-rej-congestion-bk
- 2G-comb-attach-rej-gsm-auth-unacceptable-bk
- 2G-comb-attach-rej-no-pdp-ctx-activated-bk
- 2G-comb-attach-rej-retry-from-new-cell-bk
- 2G-comb-attach-rej-sem-wrong-msg-bk
- 2G-comb-attach-rej-invalid-mand-info-bk
- 2G-comb-attach-rej-msg-type-not-exist-bk
- 2G-comb-attach-rej-msg-type-not-comp-pstate-bk
- 2G-comb-attach-rej-ie-non-existent-bk
- 2G-comb-attach-rej-conditional-ie-err-bk
- 2G-comb-attach-rej-msg-not-comp-prot-state-bk
- 2G-comb-attach-rej-protocol-error-bk
- 2G-comb-attach-rej-unknown-cause-bk
- 2G-attach-fail-ongoing-proc-comb-bk
- 2G-total-attach-fail-gprs-bk (2G-total-attach-fail)
- 2G-total-attach-fail-comb-bk
- 2G-total-attach-fail-all-bk
- 2G-intra-rau-bk
- 2G-intra-comb-rau-bk
- 2G-periodic-rau-bk
- 2G-inter-sgsn-rau-bk
- 2G-inter-sgsn-comb-rau-bk
- 2G-rau-accept-intra-gprs-bk (2G-rau-accept-intra)
- 2G-rau-accept-intra-comb-bk (2G-comb-upd-rau-accept-intra)
- 2G-rau-accept-periodic-bk
- 2G-rau-accept-inter-gprs-bk (2G-rau-accept-inter)
- 2G-rau-accept-inter-comb-bk (2G-comb-upd-rau-accept-inter)
- 2G-rau-complete-bk
- 2G-intra-rau-reject-gprs-bk (2G-intra-rau-reject)
- 2G-intra-rau-reject-comb-bk (2G-comb-rau-reject)
- 2G-periodic-rau-reject-bk
- 2G-inter-rau-reject-gprs-bk (2G-inter-rau-reject)
- 2G-inter-rau-reject-comb-bk (2G-comb-inter-rau-reject)
- 2G-inter-rau-rej-imsi-unknown-hlr-bk
- 2G-intra-rau-rej-illegal-ms-bk
- 2G-intra-rau-rej-illegal-me-bk
- 2G-intra-rau-rej-gprs-svc-not-allow-bk
- 2G-intra-rau-rej-nongprs-svc-not-allow-bk
- 2G-intra-rau-rej-msid-not-derived-by-nw-bk
- 2G-intra-rau-rej-implicitly-detach-bk
- 2G-intra-rau-rej-plmn-not-allowed-bk
- 2G-intra-rau-rej-loc-area-not-allow-bk
- 2G-intra-rau-rej-roam-not-allow-larea-bk
- 2G-intra-rau-rej-gprs-svc-not-allow-plmn-bk
- 2G-intra-rau-rej-no-cells-in-loc-area-bk
- 2G-intra-rau-rej-msc-not-reachable-bk
- 2G-intra-rau-rej-network-failure-bk
- 2G-intra-rau-rej-mac-failure-bk
- 2G-intra-rau-rej-syn-failure-bk
- 2G-intra-rau-rej-congestion-bk
- 2G-intra-rau-rej-gsm-auth-unacceptable-bk
- 2G-intra-rau-rej-no-pdp-ctx-actv-bk
- 2G-intra-rau-rej-retry-from-new-cell-bk
- 2G-intra-rau-rej-inval-mand-info-bk
- 2G-intra-rau-rej-msg-type-non-exist-bk
- 2G-intra-rau-rej-mtype-incompat-pstate-bk
- 2G-intra-rau-rej-ie-non-existent-bk
- 2G-intra-rau-rej-cond-ie-error-bk
- 2G-intra-rau-rej-msg-incompat-prot-state-bk
- 2G-intra-rau-rej-prot-error-bk
- 2G-intra-rau-rej-unknown-error-bk
- 2G-intra-prau-rej-imsi-unknown-hlr-bk
- 2G-intra-prau-rej-illegal-ms-bk
- 2G-intra-prau-rej-illegal-me-bk
- 2G-intra-prau-rej-gprs-svc-not-allow-bk
- 2G-intra-prau-rej-nongprs-svc-not-allow-bk
- 2G-intra-prau-rej-msid-not-derived-by-nw-bk
- 2G-intra-prau-rej-implicitly-detach-bk
- 2G-intra-prau-rej-plmn-not-allowed-bk
- 2G-intra-prau-rej-loc-area-not-allowed-bk
- 2G-intra-prau-rej-roam-not-allowed-larea-bk
- 2G-intra-prau-rej-gprs-svc-not-allowed-plmn-bk
- 2G-intra-prau-rej-no-cells-in-loc-area-bk
- 2G-intra-prau-rej-msc-not-reachable-bk
- 2G-intra-prau-rej-network-failure-bk
- 2G-intra-prau-rej-mac-failure-bk
- 2G-intra-prau-rej-syn-failure-bk
- 2G-intra-prau-rej-congestion-bk
- 2G-intra-prau-rej-gsm-auth-unacceptable-bk
- 2G-intra-prau-rej-no-pdp-ctx-actv-bk
- 2G-intra-prau-rej-retry-from-new-cell-bk
- 2G-intra-prau-rej-sem-wrong-msg-bk
- 2G-intra-prau-rej-inval-mand-info-bk
- 2G-intra-prau-rej-msg-type-non-exist-bk
- 2G-intra-prau-rej-mtype-incompat-pstate-bk
- 2G-intra-prau-rej-ie-non-existent-bk
- 2G-intra-prau-rej-cond-ie-error-bk
- 2G-intra-prau-rej-msg-incompat-pstate-bk
- 2G-intra-prau-rej-prot-error-bk
- 2G-intra-prau-rej-unknown-error-bk
- 2G-comb-prau-rej-imsi-unknown-hlr-bk
- 2G-comb-prau-rej-illegal-ms-bk
- 2G-comb-prau-rej-illegal-me-bk
- 2G-comb-prau-rej-gprs-svc-not-allow-bk
- 2G-comb-prau-rej-nongprs-svc-not-allow-bk
- 2G-comb-prau-rej-msid-not-derived-by-nw-bk
- 2G-comb-prau-rej-implicitly-detach-bk
- 2G-comb-prau-rej-plmn-not-allowed-bk
- 2G-comb-prau-rej-loc-area-not-allowed-bk
- 2G-comb-prau-rej-roam-not-allowed-larea-bk
- 2G-comb-prau-rej-gprs-svc-not-allowed-plmn-bk
- 2G-comb-prau-rej-no-cells-in-loc-area-bk
- 2G-comb-prau-rej-msc-not-reachable-bk
- 2G-comb-prau-rej-network-failure-bk
- 2G-comb-prau-rej-mac-failure-bk
- 2G-comb-prau-rej-syn-failure-bk
- 2G-comb-prau-rej-congestion-bk
- 2G-comb-prau-rej-gsm-auth-unacceptable-bk
- 2G-comb-prau-rej-no-pdp-ctx-actv-bk
- 2G-comb-prau-rej-retry-from-new-cell-bk
- 2G-comb-prau-rej-sem-wrong-msg-bk
- 2G-comb-prau-rej-inval-mand-info-bk
- 2G-comb-rau-rej-msg-type-non-exist-bk
- 2G-comb-rau-rej-mtype-incompat-pstate-bk
- 2G-comb-rau-rej-ie-non-existent-bk
- 2G-comb-rau-rej-cond-ie-error-bk
- 2G-comb-rau-rej-msg-incompat-pstate-bk
- 2G-comb-rau-rej-prot-error-bk
- 2G-comb-rau-rej-unknown-error-bk
- 2G-inter-rau-rej-imsi-unknown-hlr-bk
- 2G-inter-rau-rej-illegal-ms-bk
- 2G-inter-rau-rej-illegal-me-bk
- 2G-inter-rau-rej-gprs-svc-not-allow-bk
- 2G-inter-rau-rej-nongprs-svc-not-allow-bk
- 2G-inter-rau-rej-msid-not-derived-by-nw-bk
- 2G-inter-rau-rej-implicitly-detach-bk
- 2G-inter-rau-rej-plmn-not-allowed-bk
- 2G-inter-rau-rej-loc-area-not-allowed-bk
- 2G-inter-rau-rej-roam-not-allowed-larea-bk
- 2G-inter-rau-rej-gprs-svc-not-allowed-plmn-bk
- 2G-inter-rau-rej-no-cells-in-location-area-bk
- 2G-inter-rau-rej-msc-not-reachable-bk
- 2G-inter-rau-rej-network-failure-bk
- 2G-inter-rau-rej-mac-failure-bk
- 2G-inter-rau-rej-syn-failure-bk
- 2G-inter-rau-rej-congestion-bk
- 2G-inter-rau-rej-gsm-auth-unacceptable-bk
- 2G-inter-rau-rej-no-pdp-ctx-actv-bk
- 2G-inter-rau-rej-retry-from-new-cell-bk
- 2G-inter-rau-rej-sem-wrong-msg-bk
- 2G-inter-rau-rej-inval-mand-info-bk
- 2G-inter-rau-rej-msg-type-non-exist-bk
- 2G-inter-rau-rej-mtype-incompat-pstate-bk
- 2G-inter-rau-rej-ie-non-existent-bk
- 2G-inter-rau-rej-cond-ie-error-bk
- 2G-inter-rau-rej-msg-not-compat-pstate-bk
- 2G-inter-rau-rej-prot-error-bk
- 2G-inter-rau-rej-unknown-error-bk
- 2G-comb-rau-rej-imsi-unknown-hlr-bk
- 2G-comb-rau-rej-illegal-ms-bk
- 2G-comb-rau-rej-illegal-me-bk
- 2G-comb-rau-rej-gprs-svc-not-allow-bk
- 2G-comb-rau-rej-nongprs-svc-not-allow-bk
- 2G-comb-rau-rej-msid-not-derived-by-nw-bk
- 2G-comb-rau-rej-implicitly-detach-bk
- 2G-comb-rau-rej-plmn-not-allowed-bk
- 2G-comb-rau-rej-roam-area-not-allowed-bk
- 2G-comb-rau-rej-gprs-svc-not-allowed-larea-bk
- 2G-comb-rau-rej-no-cells-in-location-area-bk
- 2G-comb-rau-rej-msc-not-reachable-bk
- 2G-comb-rau-rej-network-failure-bk
- 2G-comb-rau-rej-mac-failure-bk
- 2G-comb-rau-rej-syn-failure-bk
- 2G-comb-rau-rej-congestion-bk
- 2G-comb-rau-rej-gsm-auth-unacceptable-bk
- 2G-comb-rau-rej-no-pdp-ctx-actv-bk
- 2G-comb-rau-rej-retry-from-new-cell-bk
- 2G-comb-rau-rej-sem-wrong-msg-bk
- 2G-comb-rau-rej-inval-mand-info-bk
- 2G-comb-rau-rej-msg-type-non-exist-bk
- 2G-comb-rau-rej-mtype-incompat-pstate-bk
- 2G-comb-rau-rej-ie-non-existent-bk
- 2G-comb-rau-rej-cond-ie-error-bk
- 2G-comb-rau-rej-msg-not-compat-pstate-bk
- 2G-comb-rau-rej-prot-error-bk
- 2G-comb-rau-rej-unknown-error-bk
- ps-inter-rat-rau-2g-bk
- comb-inter-rat-rau-2g-bk
- ps-inter-rat-rau-acc-2g-bk
- comb-inter-rat-rau-acc-2g-bk
- ps-inter-rat-rau-rej-2g-bk
- comb-inter-rat-rau-rej-2g-bk
- ps-inter-rat-rau-fail-2g-bk
- comb-inter-rat-rau-fail-2g-bk
- 2G-irat-ps-rej-imsi-unknown-hlr-bk
- 2G-irat-ps-rej-illegal-ms-bk
- 2G-irat-ps-rej-illegal-me-bk
- 2G-irat-ps-rej-gprs-svc-not-allow-bk
- 2G-irat-ps-rej-nongprs-svc-not-allow-bk
- 2G-irat-ps-rej-msid-not-derived-by-nw-bk
- 2G-irat-ps-rej-implicitly-detach-bk
- 2G-irat-ps-rej-plmn-not-allowed-bk
- 2G-irat-ps-rej-loc-area-not-allowed-bk
- 2G-irat-ps-rej-roam-not-allowed-larea-bk
- 2G-irat-ps-rej-gprs-svc-not-allowed-plmn-bk
- 2G-irat-ps-rej-no-cells-in-location-area-bk
- 2G-irat-ps-rej-msc-not-reachable-bk
- 2G-irat-ps-rej-network-failure-bk
- 2G-irat-ps-rej-mac-failure-bk
- 2G-irat-ps-rej-syn-failure-bk
- 2G-irat-ps-rej-congestion-bk
- 2G-irat-ps-rej-gsm-auth-unacceptable-bk
- 2G-irat-ps-rej-no-pdp-ctx-actv-bk
- 2G-irat-ps-rej-retry-from-new-cell-bk
- 2G-irat-ps-rej-sem-wrong-msg-bk
- 2G-irat-ps-rej-inval-mand-info-bk
- 2G-irat-ps-rej-msg-type-non-exist-bk
- 2G-irat-ps-rej-mtype-incompat-pstate-bk
- 2G-irat-ps-rej-ie-non-existent-bk
- 2G-irat-ps-rej-cond-ie-error-bk
- 2G-irat-ps-rej-msg-not-compat-pstate-bk
- 2G-irat-ps-rej-prot-error-bk
- 2G-irat-ps-rej-unknown-error-bk
- 2G-irat-comb-rej-imsi-unknown-hlr-bk
- 2G-irat-comb-rej-illegal-ms-bk
- 2G-irat-comb-rej-illegal-me-bk
- 2G-irat-comb-rej-gprs-svc-not-allow-bk
- 2G-irat-comb-rej-nongprs-svc-not-allow-bk
- 2G-irat-comb-rej-msid-not-derived-by-nw-bk
- 2G-irat-comb-rej-implicitly-detach-bk
- 2G-irat-comb-rej-plmn-not-allowed-bk
- 2G-irat-comb-rej-loc-area-not-allowed-bk
- 2G-irat-comb-rej-roam-not-allowed-larea-bk
- 2G-irat-comb-rej-gprs-svc-not-allowed-plmn-bk
- 2G-irat-comb-rej-no-cells-in-location-area-bk
- 2G-irat-comb-rej-msc-not-reachable-bk
- 2G-irat-comb-rej-network-failure-bk
- 2G-irat-comb-rej-mac-failure-bk
- 2G-irat-comb-rej-syn-failure-bk
- 2G-irat-comb-rej-congestion-bk
- 2G-irat-comb-rej-gsm-auth-unacceptable-bk
- 2G-irat-comb-rej-no-pdp-ctx-actv-bk
- 2G-irat-comb-rej-retry-from-new-cell-bk
- 2G-irat-comb-rej-sem-wrong-msg-bk
- 2G-irat-comb-rej-inval-mand-info-bk
- 2G-irat-comb-rej-msg-type-non-exist-bk
- 2G-irat-comb-rej-mtype-incompat-pstate-bk
- 2G-irat-comb-rej-ie-non-existent-bk
- 2G-irat-comb-rej-cond-ie-error-bk
- 2G-irat-comb-rej-msg-not-compat-pstate-bk
- 2G-irat-comb-rej-prot-error-bk
- 2G-irat-comb-rej-unknown-error-bk
- 2G-intra-rau-failure-gprs-bk (2G-total-intra-rau-failure)
- 2G-intra-rau-failure-comb-bk (2G-total-intra-rau-failure-comb)
- 2G-periodic-rau-failure-bk (2G-total-periodic-rau-failure)
- 2G-inter-rau-failure-gprs-bk (2G-total-inter-rau-failure)
- 2G-inter-rau-failure-comb-bk (2G-total-comb-inter-rau-failure)
- 2G-intra-ra-upd-rau-fail-ongoing-proc-bk
- 2G-inter-rau-fail-ongoing-proc-bk
- 2G-intra-comb-rau-fail-ongoing-proc-bk
- 2G-inter-comb-rau-fail-ongoing-proc-bk
- 2G-intra-perio-rau-fail-ongoing-proc-bk
- 2G-inter-rau-fail-internal-failure-bk
- 2G-inter-rau-fail-comb-internal-failure-bk
- 2G-intra-rau-fail-internal-failure-bk
- 2G-intra-rau-fail-comb-internal-failure-bk
- 2G-paging-request-bk
- 2G-paging-success-bk
- 2G-auth-cipher-response-bk
- 2G-auth-cipher-request-bk
- 2G-auth-cipher-mac-fail-bk
- 2G-auth-cipher-syn-fail-bk
- 2G-auth-unacceptable-bk
- 2G-imsi-identity-request-bk
- 2G-imsi-identity-response-bk
- 2G-ms-init-detach-bk
- 2G-nw-init-detach-bk
- 2G-ms-init-detach-accept-bk
- 2G-nw-init-detach-accept-bk
- 2G-total-actv-req-bk
- 2G-total-actv-accept-bk
- 2G-primary-actv-accept-bk
- 2G-secondary-actv-accept-bk
- 2G-total-actv-reject-bk
- 2G-primary-actv-reject-bk
- 2G-secondary-actv-reject-bk
- 2G-actv-rej-odb-bk
- 2G-actv-rej-insufficient-resources-bk
- 2G-actv-rej-network-failure-bk
- 2G-actv-rej-missing-or-unknown-apn-bk
- 2G-actv-rej-unknown-pdp-addr-type-bk
SGSN Changes in Release 17

- 2G-actv-rej-usr-auth-failed-bk
- 2G-actv-rej-by-ggsn-bk
- 2G-actv-rej-unspecified-error-bk
- 2G-actv-rej-service-not-supported-bk
- 2G-actv-rej-service-not-subscribed-bk
- 2G-actv-rej-svc-opt-tmp-out-of-order-bk
- 2G-actv-rej-apn-restriction-incompatible-bk
- 2G-actv-rej-semantically-incorrect-bk
- 2G-actv-rej-invalid-mandatory-info-bk
- 2G-actv-rej-msg-type-non-existent-bk
- 2G-actv-rej-ie-non-existent-bk
- 2G-actv-rej-conditional-ie-err-bk
- 2G-actv-rej-recovery-on-timer-expiry-bk
- 2G-actv-rej-prot-err-unspecified-bk
- 2G-sec-actv-rej-odb-bk
- 2G-sec-actv-rej-insufficient-resources-bk
- 2G-sec-actv-rej-by-ggsn-bk
- 2G-sec-actv-rej-unspecified-error-bk
- 2G-sec-actv-rej-service-not-supported-bk
- 2G-sec-actv-rej-service-not-subscribed-bk
- 2G-sec-actv-rej-semantically-incorrect-bk
- 2G-sec-actv-rej-invalid-mandatory-info-bk
- 2G-sec-actv-rej-conditional-ie-err-bk reject-bk
- 2G-sec-actv-rej-service-not-supported-bk
- 2G-sec-actv-rej-service-not-subscribed-bk
- 2G-sec-actv-rej-semantically-incorrect-bk
- 2G-sec-actv-rej-invalid-mandatory-info-bk
- 2G-sec-actv-rej-msg-type-non-existent-bk
- 2G-sec-actv-rej-ie-non-existent-bk
- 2G-sec-actv-rej-conditional-ie-err-bk
- 2G-sec-actv-rej-recovery-on-timer-expiry-bk
- 2G-sec-actv-rej-prot-err-unspecified-bk
- 2G-sec-actv-rej-semantic-error-tft-operation-bk
- 2G-sec-actv-rej-unknown-pdp-context-bk
- 2G-sec-actv-rej-pdp-notft-actv-bk
- 2G-total-actv-fail-bk
- 2G-primary-actv-fail-bk
- 2G-secondary-actv-fail-bk
- 2G-actv-fail-guard-timer-expiry-bk
- 2G-actv-fail-duplicate-activation-bk
- 2G-actv-fail-other-ongoing-procedure-bk
- 2G-actv-fail-tunnel-deactivation-bk
- 2G-actv-fail-handoff-before-activate-over-bk
- 2G-actv-fail-detach-before-activate-over-bk
- 2G-actv-fail-phase-2-offload-bk
- 2G-actv-fail-invalid-msg-content-bk
- 2G-ms-modify-req-bk
- 2G-ms-modify-accept-bk
- 2G-ms-modify-rej-bk
- 2G-nw-modify-req-bk
- 2G-nw-modify-accept-bk
- 2G-nw-modify-rej-bk
- 2G-ms-deactv-accept-bk
- 2G-ms-deactv-reject-bk
- 2G-hlr-init-deact-acc-bk
- 2G-hlr-init-deact-rej-bk
- 2G-sgsn-init-deact-acc-bk
- 2G-sgsn-init-deact-rej-bk
- 2G-ggsn-init-deact-acc-bk
- 2G-ggsn-init-deact-rej-bk

**iups-bk Schema**
The following statistics will be backed up for recovery. They are derived from the SGSN schema and perform the same functions as the statistics of similar (with noted exceptions) names minus the -bk extension. For example, the 3G-home-subscribers-bk listed below performs the same functions as the 3G-home-subscribers statistic in the SGSN schema - unless the SGSN stat exception is noted:

- vpnname
- vpnid
- servname
- 3G-attached-bk
- 3G-home-subscribers-bk
- 3G-visiting-national-bk
- 3G-visiting-foreign-bk
- 3G-attached-with-pdp-bk
- 3G-total-num-actv-pdp-bk
- 3G-total-num-actv-pdp-on-s4-bk
- 3G-total-attach-req-bk (3G-total-attach-req-all)
- 3G-attach-req-gprs-bk (3G-total-attach-req)
- 3G-attach-req-comb-bk (3G-total-comb-attach-req)
- 3G-attach-req-imsi-gprs-bk (3G-IMSI-Attch)
- 3G-attach-req-imsi-comb-bk (3G-IMSI-Attch-Combined)
- 3G-attach-req-ptmsi-gprs-bk (3G-ptmsi-Attch)
- 3G-attach-req-ptmsi-comb-bk (3G-ptmsi-Attch-Combined)
- 3G-attach-req-local-ptmsi-gprs-bk (3G-local-ptmsi-Attch)
- 3G-attach-req-local-ptmsi-comb-bk (3G-local-ptmsi-Attch-comb)
- 3G-attach-req-remote-ptmsi-gprs-bk (3G-remote-ptmsi-Attch)
- 3G-attach-req-remote-ptmsi-comb-bk (3G-remote-ptmsi-Attch-comb)
- 3G-attach-accept-gprs-bk (3G-attach-accept)
- 3G-attach-accept-comb-bk (3G-comb-attach-accept)
- 3G-attach-reject-bk (3G-attach-reject-all)
- 3G-attach-reject-gprs-bk (3G-attach-reject)
- 3G-attach-reject-comb-bk (3G-attach-reject-comb)
- 3G-attach-rej-imsi-unknown-at-hlr-bk
- 3G-attach-rej-illegal-ms-bk
- 3G-attach-rej-illegal-me-bk
- 3G-gprs-service-not-allowed-bk
- 3G-gprs-and-non-gprs-service-not-allowed-bk
SGSN Changes in Release 17

- 3G-attach-rej-msid-not-derived-by-nwt-bk
- 3G-attach-rejimplicitly-detach-bk
- 3G-attach-rej-plmn-not-allowed-bk
- 3G-attach-rej-la-not-allowed-bk
- 3G-roaming-not-allowed-in-this-location-area-bk
- 3G-gprs-service-not-allowed-in-this-plmn-bk
- 3G-no-suitable-cells-in-location-area-bk
- 3G-attach-rej-msc-not-reachable-bk
- 3G-attach-rej-network-failure-bk
- 3G-attach-rej-network-failure-no-data-from-hlr-bk
- 3G-attach-rej-network-failure-congestion-thrtl-bk
- 3G-attach-rej-network-failure-opr-policy-failure-bk
- 3G-attach-rej-network-failure-check-imei-timeout-eir-bk
- 3G-attach-rej-network-failure-mnc-ovld-bk
- 3G-attach-rej-network-failure-more-ius-same-imsi-bk
- 3G-attach-rej-network-failure-no-resource-intl-failure-bk
- 3G-attach-rej-network-failure-ext-bk
- 3G-attach-rej-network-failure-int-bk
- 3G-attach-rej-mac-failure-bk
- 3G-attach-rej-sync-failure-bk
- 3G-attach-rej-congestion-bk
- 3G-attach-rej-gsm-auth-unacceptable-bk
- 3G-attach-rej-no-pdp-ctx-activated-bk
- 3G-attach-rej-retry-from-new-cell-bk
- 3G-attach-rej-sem-wrong-msg-bk
- 3G-attach-rej-invalid-mand-info-bk
- 3G-attach-rej-msg-type-not-exist-bk
- 3G-attach-rej-msg-type-not-comp-prot-state-bk
- 3G-attach-rej-ie-non-existent-bk
- 3G-attach-rej-conditional-ie-err-bk
- 3G-attach-rej-msg-not-comp-prot-state-bk
- 3G-attach-rej-protocol-error-bk
- 3G-attach-rej-unknown-cause-bk
- 3G-comb-attach-rej-imsi-unknown-at-hlr-bk
- 3G-comb-attach-rej-illegal-ms-bk
- 3G-comb-attach-rej-illegal-me-bk
- 3G-comb-gprs-service-not-allowed-bk
- 3G-comb-gprs-and-non-gprs-svc-not-allow-bk
- 3G-comb-attach-rej-msid-not-derived-by-nwt-bk
- 3G-comb-attach-rej-implicitly-detach-bk
- 3G-comb-attach-rej-plmn-not-allowed-bk
- 3G-comb-attach-rej-la-not-allowed-bk
- 3G-comb-roam-not-allow-in-loc-area-bk
- 3G-comb-gprs-svc-not-allow-in-plmn-bk
- 3G-comb-no-suitable-cells-in-loc-area-bk
- 3G-comb-attach-rej-msc-not-reachable-bk
- 3G-comb-attach-rej-network-failure-bk
- 3G-comb-attach-rej-network-failure-no-data-from-hlr-bk
- 3G-comb-attach-rej-network-failure-congestion-thrtl-bk
- 3G-comb-attach-rej-network-failure-opr-policy-failure-bk
- 3G-comb-attach-rej-network-failure-check-imei-timeout-eir-bk
- 3G-comb-attach-rej-network-failure-rnc-ovld-bk
- 3G-comb-attach-rej-network-failure-more-ius-same-imsi-bk
- 3G-comb-attach-rej-network-failure-ext-bk
- 3G-comb-attach-rej-network-failure-int-bk
- 3G-comb-attach-rej-mac-failure-bk
- 3G-comb-attach-rej-sync-failure-bk
- 3G-comb-attach-rej-congestion-bk
- 3G-comb-attach-rej-protocol-error-bk
- 3G-comb-attach-rej-unknown-cause-bk
- 3G-attach-fail-iu_release-gprs-bk (3G-attach-fail-iu_release)
- 3G-attach-fail-iu_release-external-bk
- 3G-attach-fail-iu_release-internal-bk
- 3G-attach-fail-ongoing-proc-gprs-bk (3G-attach-fail-ongoing-proc)
- 3G-attach-fail-iu_release-comb-bk
- 3G-attach-fail-iu_release-comb-external-bk
- 3G-attach-fail-iu_release-comb-internal-bk

SGSN Changes in Release 17
- 3G-attach-fail-ongoing-proc-comb-bk
- 3G-total-attach-fail-gprs-bk (3G-total-attach-fail)
- 3G-total-attach-fail-comb-bk
- 3G-total-attach-fail-all-bk
- 3G-intra-rau-bk
- 3G-intra-comb-rau-bk
- 3G-periodic-rau-bk
- 3G-inter-sgsn-rau-bk
- 3G-inter-sgsn-comb-rau-bk
- 3G-rau-accept-intra-gprs-bk (3G-rau-accept-intra)
- 3G-rau-accept-intra-comb-bk (3G-comb-upd-rau-accept-intra)
- 3G-rau-accept-periodic-bk
- 3G-rau-accept-inter-gprs-bk (3G-rau-accept-inter)
- 3G-rau-accept-inter-comb-bk (3G-comb-upd-rau-accept-inter)
- 3G-rau-complete-bk
- 3G-intra-rau-reject-gprs-bk (3G-intra-rau-reject)
- 3G-intra-rau-reject-comb-bk (3G-comb-rau-reject)
- 3G-periodic-rau-reject-bk
- 3G-inter-rau-reject-gprs-bk (3G-inter-rau-reject)
- 3G-inter-rau-reject-comb-bk (3G-comb-inter-rau-reject)
- 3G-intra-rau-rej-imsi-unknown-hlr-bk
- 3G-intra-rau-rej-illegal-ms-bk
- 3G-intra-rau-rej-illegal-me-bk
- 3G-intra-rau-rej-gprs-svc-not-allow-bk
- 3G-intra-rau-rej-nongprs-svc-not-allow-bk
- 3G-intra-rau-rej-msid-not-derived-by-nw-bk
- 3G-intra-rau-rej-implicitly-detach-bk
- 3G-intra-rau-rej-plmn-not-allowed-bk
- 3G-intra-rau-rej-loc-area-not-allow-bk
- 3G-intra-rau-rej-roam-not-allow-larea-bk
- 3G-intra-rau-rej-gprs-svc-not-allow-plmn-bk
- 3G-intra-rau-rej-no-cells-in-loc-area-bk
- 3G-intra-rau-rej-msc-not-reachable-bk
- 3G-intra-rau-rej-network-failure-bk
• 3G-intra-rau-rej-mac-failure-bk
• 3G-intra-rau-rej-syn-failure-bk
• 3G-intra-rau-rej-congestion-bk
• 3G-intra-rau-rej-gsm-auth-unacceptable-bk
• 3G-intra-rau-rej-no-pdp-ctx-actv-bk
• 3G-intra-rau-rej-retry-from-new-cell-bk
• 3G-intra-rau-rej-inval-mand-info-bk
• 3G-intra-rau-rej-msg-type-non-exist-bk
• 3G-intra-rau-rej-mtype-incompat-pstate-bk
• 3G-intra-rau-rej-ie-non-existent-bk
• 3G-intra-rau-rej-cond-ie-error-bk
• 3G-intra-rau-rej-msg-incompat-prot-state-bk
• 3G-intra-rau-rej-prot-error-bk
• 3G-intra-rau-rej-unknown-error-bk
• 3G-intra-prau-rej-imsi-unknown-hlr-bk
• 3G-intra-prau-rej-illegal-ms-bk
• 3G-intra-prau-rej-illegal-me-bk
• 3G-intra-prau-rej-gprs-svc-not-allow-bk
• 3G-intra-prau-rej-nongprs-svc-not-allow-bk
• 3G-intra-prau-rej-msid-not-derived-by-nw-bk
• 3G-intra-prau-rej-implicitly-detach-bk
• 3G-intra-prau-rej-plmn-not-allowed-bk
• 3G-intra-prau-rej-loc-area-not-allowed-bk
• 3G-intra-prau-rej-roam-not-allowed-larea-bk
• 3G-intra-prau-rej-gprs-svc-not-allowed-plmn-bk
• 3G-intra-prau-rej-no-cells-in-loc-area-bk
• 3G-intra-prau-rej-msc-not-reachable-bk
• 3G-intra-prau-rej-network-failure-bk
• 3G-intra-prau-rej-mac-failure-bk
• 3G-intra-prau-rej-syn-failure-bk
• 3G-intra-prau-rej-congestion-bk
• 3G-intra-prau-rej-gsm-auth-unacceptable-bk
• 3G-intra-prau-rej-no-pdp-ctx-actv-bk
• 3G-intra-prau-rej-retry-from-new-cell-bk
- 3G-intra-prau-rej-sem-wrong-msg-bk
- 3G-intra-prau-rej-inval-mand-info-bk
- 3G-intra-prau-rej-msg-type-non-exist-bk
- 3G-intra-prau-rej-mtype-incompat-pstate-bk
- 3G-intra-prau-rej-ie-non-existent-bk
- 3G-intra-prau-rej-cond-ie-error-bk
- 3G-intra-prau-rej-msg-incompat-pstate-bk
- 3G-intra-prau-rej-prot-error-bk
- 3G-intra-prau-rej-unknown-error-bk
- 3G-comb-prau-rej-imsi-unknown-hlr-bk
- 3G-comb-prau-rej-illegal-ms-bk
- 3G-comb-prau-rej-illegal-me-bk
- 3G-comb-prau-rej-gprs-svc-not-allow-bk
- 3G-comb-prau-rej-nongprs-svc-not-allow-bk
- 3G-comb-prau-rej-msid-not-derived-by-nw-bk
- 3G-comb-prau-rej-implicit-detach-bk
- 3G-comb-prau-rej-plmn-not-allowed-bk
- 3G-comb-prau-rej-loc-area-not-allowed-bk
- 3G-comb-prau-rej-roam-not-allowed-larea-bk
- 3G-comb-prau-rej-gprs-svc-not-allowed-plmn-bk
- 3G-comb-prau-rej-no-cells-in-loc-area-bk
- 3G-comb-prau-rej-msc-not-reachable-bk
- 3G-comb-prau-rej-network-failure-bk
- 3G-comb-prau-rej-mac-failure-bk
- 3G-comb-prau-rej-syn-failure-bk
- 3G-comb-prau-rej-congestion-bk
- 3G-comb-prau-rej-gsm-auth-unacceptable-bk
- 3G-comb-prau-rej-no-pdp-ctx-activ-bk
- 3G-comb-prau-rej-retry-from-new-cell-bk
- 3G-comb-prau-rej-sem-wrong-msg-bk
- 3G-comb-prau-rej-inval-mand-info-bk
- 3G-comb-prau-rej-msg-type-non-exist-bk
- 3G-comb-prau-rej-mtype-incompat-pstate-bk
- 3G-comb-prau-rej-ie-non-existent-bk
• 3G-comb-rau-rej-cond-ie-error-bk
• 3G-comb-rau-rej-msg-incompat-pstate-bk
• 3G-comb-rau-rej-prot-error-bk
• 3G-comb-rau-rej-unknown-error-bk
• 3G-inter-rau-rej-imsi-unknown-hlr-bk
• 3G-inter-rau-rej-illegal-ms-bk
• 3G-inter-rau-rej-illegal-me-bk
• 3G-inter-rau-rej-gprs-svc-not-allow-bk
• 3G-inter-rau-rej-nongprs-svc-not-allow-bk
• 3G-inter-rau-rej-msid-not-derived-by-nw-bk
• 3G-inter-rau-rej-implicitly-detach-bk
• 3G-inter-rau-rej-plmn-not-allowed-bk
• 3G-inter-rau-rej-loc-area-not-allowed-bk
• 3G-inter-rau-rej-roam-not-allowed-larea-bk
• 3G-inter-rau-rej-gprs-svc-not-allowed-plmn-bk
• 3G-inter-rau-rej-no-cells-in-location-area-bk
• 3G-inter-rau-rej-msc-not-reachable-bk
• 3G-inter-rau-rej-network-failure-bk
• 3G-inter-rau-rej-mac-failure-bk
• 3G-inter-rau-rej-syn-failure-bk
• 3G-inter-rau-rej-congestion-bk
• 3G-inter-rau-rej-gsm-auth-unacceptable-bk
• 3G-inter-rau-rej-no-pdp-ctx-actv-bk
• 3G-inter-rau-rej-retry-from-new-cell-bk
• 3G-inter-rau-rej-sem-wrong-msg-bk
• 3G-inter-rau-rej-inval-mand-info-bk
• 3G-inter-rau-rej-msg-type-non-exist-bk
• 3G-inter-rau-rej-mtype-incompat-pstate-bk
• 3G-inter-rau-rej-ie-non-existent-bk
• 3G-inter-rau-rej-cond-ie-error-bk
• 3G-inter-rau-rej-msg-not-compat-pstate-bk
• 3G-inter-rau-rej-prot-error-bk
• 3G-inter-rau-rej-unknown-error-bk
• 3G-comb-irau-rej-imsi-unknown-hlr-bk
- 3G-comb-irau-rej-illegal-ms-bk
- 3G-comb-irau-rej-illegal-me-bk
- 3G-comb-irau-rej-gprs-svc-not-allow-bk
- 3G-comb-irau-rej-nongprs-svc-not-allow-bk
- 3G-comb-irau-rej-msid-not-derived-by-nw-bk
- 3G-comb-irau-rej-implicitly-detach-bk
- 3G-comb-irau-rej-plmn-not-allowed-bk
- 3G-comb-irau-rej-loc-area-not-allowed-bk
- 3G-comb-irau-rej-roam-not-allowed-larea-bk
- 3G-comb-irau-rej-gprs-svc-not-allowed-plmn-bk
- 3G-comb-irau-rej-no-cells-in-location-area-bk
- 3G-comb-irau-rej-msc-not-reachable-bk
- 3G-comb-irau-rej-network-failure-bk
- 3G-comb-irau-rej-mac-failure-bk
- 3G-comb-irau-rej-syn-failure-bk
- 3G-comb-irau-rej-congestion-bk
- 3G-comb-irau-rej-gsm-auth-unacceptable-bk
- 3G-comb-irau-rej-no-pdp-ctx-actv-bk
- 3G-comb-irau-rej-retry-from-new-cell-bk
- 3G-comb-irau-rej-sem-wrong-msg-bk
- 3G-comb-irau-rej-inval-mand-info-bk
- 3G-comb-irau-rej-msg-type-non-exist-bk
- 3G-comb-irau-rej-mtype-incompat-pstate-bk
- 3G-comb-irau-rej-ie-non-existent-bk
- 3G-comb-irau-rej-cond-ie-error-bk
- 3G-comb-irau-rej-msg-not-compat-pstate-bk
- 3G-comb-irau-rej-prot-error-bk
- 3G-comb-irau-rej-unknown-error-bk
- ps-inter-rat-rau-3g-bk
- comb-inter-rat-rau-3g-bk
- ps-inter-rat-rau-acc-3g-bk
- comb-inter-rat-rau-acc-3g-bk
- ps-inter-rat-rau-rej-3g-bk
- comb-inter-rat-rau-rej-3g-bk
- ps-inter-rat-rau-fail-3g-bk
- comb-inter-rat-rau-fail-3g-bk
- 3G-irat-ps-rej-imsi-unknown-hlr-bk
- 3G-irat-ps-rej-illegal-ms-bk
- 3G-irat-ps-rej-illegal-me-bk
- 3G-irat-ps-rej-gprs-svc-not-allow-bk
- 3G-irat-ps-rej-nongprs-svc-not-allow-bk
- 3G-irat-ps-rej-msid-not-derived-by-nw-bk
- 3G-irat-ps-rej-implicitly-detach-bk
- 3G-irat-ps-rej-plmn-not-allowed-bk
- 3G-irat-ps-rej-loc-area-not-allowed-bk
- 3G-irat-ps-rej-roam-not-allowed-larea-bk
- 3G-irat-ps-rej-gprs-svc-not-allowed-plmn-bk
- 3G-irat-ps-rej-no-cells-in-location-area-bk
- 3G-irat-ps-rej-msc-not-reachable-bk
- 3G-irat-ps-rej-network-failure-bk
- 3G-irat-ps-rej-mac-failure-bk
- 3G-irat-ps-rej-syn-failure-bk
- 3G-irat-ps-rej-congestion-bk
- 3G-irat-ps-rej-gsm-auth-unacceptable-bk
- 3G-irat-ps-rej-no-pdp-ctx-actv-bk
- 3G-irat-ps-rej-retry-from-new-cell-bk
- 3G-irat-ps-rej-sem-wrong-msg-bk
- 3G-irat-ps-rej-inval-mand-info-bk
- 3G-irat-ps-rej-msg-type-non-exist-bk
- 3G-irat-ps-rej-mtype-incompat-pstate-bk
- 3G-irat-ps-rej-ie-non-existent-bk
- 3G-irat-ps-rej-cond-ie-error-bk
- 3G-irat-ps-rej-msg-not-compat-pstate-bk
- 3G-irat-ps-rej-prot-error-bk
- 3G-irat-ps-rej-unknown-error-bk
- 3G-irat-comb-rej-imsi-unknown-hlr-bk
- 3G-irat-comb-rej-illegal-ms-bk
- 3G-irat-comb-rej-illegal-me-bk
- 3G-irat-comb-rej-gprs-svc-not-allow-bk
- 3G-irat-comb-rej-nongprs-svc-not-allow-bk
- 3G-irat-comb-rej-msid-not-derived-by-nw-bk
- 3G-irat-comb-rej-implicitly-detach-bk
- 3G-irat-comb-rej-plmn-not-allowed-bk
- 3G-irat-comb-rej-loc-area-not-allowed-bk
- 3G-irat-comb-rej-roam-not-allowed-larea-bk
- 3G-irat-comb-rej-gprs-svc-not-allowed-plmn-bk
- 3G-irat-comb-rej-no-cells-in-location-area-bk
- 3G-irat-comb-rej-msc-not-reachable-bk
- 3G-irat-comb-rej-network-failure-bk
- 3G-irat-comb-rej-mac-failure-bk
- 3G-irat-comb-rej-syn-failure-bk
- 3G-irat-comb-rej-congestion-bk
- 3G-irat-comb-rej-gsm-auth-unacceptable-bk
- 3G-irat-comb-rej-no-pdp-ctx-actv-bk
- 3G-irat-comb-rej-retry-from-new-cell-bk
- 3G-irat-comb-rej-sem-wrong-msg-bk
- 3G-irat-comb-rej-inval-mand-info-bk
- 3G-irat-comb-rej-msg-type-non-exist-bk
- 3G-irat-comb-rej-mtype-incompat-pstate-bk
- 3G-irat-comb-rej-ie-non-existent-bk
- 3G-irat-comb-rej-cond-ie-error-bk
- 3G-irat-comb-rej-msg-not-compat-pstate-bk
- 3G-irat-comb-rej-prot-error-bk
- 3G-irat-comb-rej-unknown-error-bk
- 3G-intra-rau-failure-gprs-bk (3G-total-intra-rau-failure)
- 3G-intra-rau-failure-comb-bk (3G-total-intra-rau-failure-comb)
- 3G-periodic-rau-failure-bk (3G-total-periodic-rau-failure)
- 3G-inter-rau-failure-gprs-bk (3G-total-inter-rau-failure)
- 3G-inter-rau-failure-comb-bk (3G-total-comb-inter-rau-failure)
- 3G-intra-ra-upd-rau-fail-iu_release-bk
- 3G-intra-ra-upd-rau-fail-ongoing-proc-bk
- 3G-intra-comb-rau-fail-iu_release-bk
- 3G-intra-comb-rau-fail-ongoing-proc-bk
- 3G-intra-perio-rau-fail-iu_release-bk
- 3G-intra-perio-rau-fail-ongoing-proc-bk
- 3G-inter-rau-fail-iu_release-bk
- 3G-inter-rau-fail-ongoing-proc-bk
- 3G-inter-comb-rau-fail-iu_release-bk
- 3G-inter-comb-rau-fail-ongoing-proc-bk
- 3G-paging-request-bk
- 3G-paging-success-bk
- 3G-auth-cipher-response-bk
- 3G-auth-cipher-request-bk
- 3G-auth-cipher-mac-fail-bk
- 3G-auth-cipher-syn-fail-bk
- 3G-auth-unacceptable-bk
- 3G-imsi-identity-request-bk
- 3G-imsi-identity-response-bk
- new-connection-rejected-overload-bk
- exist-conn-proc-rej-overload-bk
- 3G-ms-init-detach-bk
- 3G-nw-init-detach-bk
- 3G-ms-init-detach-accept-bk
- 3G-nw-init-detach-accept-bk
- 3G-total-actv-req-bk
- 3G-total-actv-accept-bk
- 3G-primary-actv-accept-bk
- 3G-secondary-actv-ace-bk
- 3G-total-actv-reject-bk
- 3G-primary-actv-reject-bk
- 3G-secondary-actv-rej-bk
- 3G-actv-rej-odb-bk
- 3G-actv-rej-insufficient-resources-bk
- 3G-actv-rej-network-failure-bk
- 3G-actv-rej-missing-or-unknown-apn-bk
- 3G-actv-rej-unknown-pdp-addr-type-bk
SGSN Changes in Release 17

- 3G-actv-rej-usr-auth-failed-bk
- 3G-actv-rej-by-ggsn-bk
- 3G-actv-rej-unspecified-error-bk
- 3G-actv-rej-service-not-supported-bk
- 3G-actv-rej-service-not-subscribed-bk
- 3G-actv-rej-svc-opt-tmp-out-of-order-bk
- 3G-actv-rej-apn-restriction-incompatible-bk
- 3G-actv-rej-semantically-incorrect-bk
- 3G-actv-rej-invalid-mandatory-info-bk
- 3G-actv-rej-msg-type-non-existent-bk
- 3G-actv-rej-ie-non-existent-bk
- 3G-actv-rej-conditional-ie-err-bk
- 3G-actv-rej-msg-not-compatible-with-prot-state-bk
- 3G-actv-rej-recovery-on-timer-expiry-bk
- 3G-actv-rej-prot-err-unspecified-bk
- 3G-sec-actv-rej-odb-bk
- 3G-sec-actv-rej-insufficient-resources-bk
- 3G-sec-actv-rej-by-ggsn-bk
- 3G-sec-actv-rej-unspecified-error-bk
- 3G-sec-actv-rej-service-not-supported-bk
- 3G-sec-actv-rej-service-not-subscribed-bk
- 3G-sec-actv-rej-svc-opt-tmp-out-of-order-bk
- 3G-sec-actv-rej-semantically-incorrect-bk
- 3G-sec-actv-rej-invalid-mandatory-info-bk
- 3G-sec-actv-rej-msg-type-non-existent-bk
- 3G-sec-actv-rej-ie-non-existent-bk
- 3G-sec-actv-rej-conditional-ie-err-bk
- 3G-sec-actv-rej-msg-not-compat-prot-state-bk
- 3G-sec-actv-rej-recovery-on-timer-expiry-bk
- 3G-sec-actv-rej-prot-err-unspecified-bk
- 3G-sec-actv-rej-semantic-error-tft-operation-bk
- 3G-sec-actv-rej-unknown-pdp-context-bk
- 3G-sec-actv-rej-semantic-err-in-pkt-filter-bk
• 3G-sec-actv-rej-syntax-err-in-pkt-filter-bk
• 3G-sec-actv-rej-pdp-notft-actv-bk
• 3G-sec-actv-rej-coll-with-net-init-req-bk
• 3G-total-actv-fail-bk
• 3G-primary-actv-fail-bk
• 3G-secondary-actv-fail-bk
• 3G-actv-fail-iu-release-before-activate-bk
• 3G-actv-fail-gaurd-timer-expiry-bk
• 3G-actv-fail-duplicate-activation-bk
• 3G-actv-fail-other-ongoing-procedure-bk
• 3G-actv-fail-tunnel-deactivation-bk
• 3G-actv-fail-handoff-before-activate-over-bk
• 3G-actv-fail-detach-before-activate-over-bk
• 3G-actv-fail-phase-2-offload-bk
• 3G-actv-fail-invalid-message-content-bk
• 3G-ms-modify-req-bk
• 3G-ms-modify-accept-bk
• 3G-ms-modify-rej-bk
• 3G-nw-modify-req-bk
• 3G-nw-modify-accept-bk
• 3G-nw-modify-rej-bk
• 3G-ms-deactv-accept-bk
• 3G-ms-deactv-reject-bk
• 3G-hlr-init-deact-acc-bk
• 3G-hlr-init-deact-rej-bk
• 3G-sgsn-init-deact-acc-bk
• 3G-sgsn-init-deact-rej-bk
• 3G-ggsn-init-deact-acc-bk
• 3G-ggsn-init-deact-rej-bk
• 3G-nw-deactv-rej-tx-insuff-res-bk
• 3G-nw-deactv-rej-tx-actv-rej-ggsn-bk
• 3G-nw-deactv-rej-tx-actv-rej-unspec-bk
• 3G-nw-deactv-rej-tx-svc-opt-temp-out-order-bk
• 3G-nw-deactv-rej-tx-nsapi-already-used-bk
- 3G-nw-deactv-rej-tx-sem-err-tft-op-bk
- 3G-nw-deactv-rej-tx-syn-err-tft-op-bk
- 3G-nw-deactv-rej-tx-invalid-trans-id-bk
- 3G-nw-deactv-rej-tx-sem-incorrect-msg-bk
- 3G-nw-deactv-rej-tx-msg-non-existent-bk
- 3G-nw-deactv-rej-tx-ie-non-existent-bk
- 3G-nw-deactv-rej-tx-cond-ie-err-bk
- 3G-nw-deactv-rej-tx-prot-err-unspec-bk
- 3G-nw-deactv-rej-tx-msg-not-compat-prot-state-bk
- SRNS-ctxt-rsp-rcvd-bk
- SRNS-ctxt-req-sent-bk
- SRNS-ctxt-total-pdp-acc-bk
- SRNS-ctxt-total-pdp-rej-bk
- Relocation-request-bk
- Relocation-complete-bk
- rab-assign-req-bk
- rab-assign-rsp-bk
- rab-set-mod-req-bk
- rab-set-mod-acc-bk
- total-rab-rej-bk
- rab-rej-rab-preempt-bk
- rab-rej-reloc-overall-tmr-exp-bk
- rab-rej-reloc-prep-tmr-exp-bk
- rab-rej-reloc-complete-tmr-exp-bk
- rab-rej-queuing-tmr-exp-bk
- rab-rej-reloc-triggered-bk
- rab-rej-unable-to-est-reloc-bk
- rab-rej-unknown-target-rnc-bk
- rab-rej-reloc-cancel-bk
- rab-rej-reloc-success-bk
- rab-rej-cypher-algo-no-support-bk
- rab-rej-conflict-cypher-info-bk
- rab-rej-failure-radio-if-proc-bk
• rab-rej-rel-utran-reason-bk
• rab-rej-utran-inactivity-bk
• rab-rej-time-crit-relocation-bk
• rab-rej-req-traffic-class-unavail-bk
• rab-rej-invalid-rab-param-val-bk
• rab-rej-req-max-bit-rate-unavail-bk
• rab-rej-req-max-bit-rate-dl-unavail-bk
• rab-rej-req-max-bit-rate-ul-unavail-bk
• rab-rej-req-gbr-unavail-bk
• rab-rej-req-gbr-dl-unavail-bk
• rab-rej-req-gbr-ul-unavail-bk
• rab-rej-req-trans-delay-not-achievable-bk
• rab-rej-req-gbr-combo-val-bk
• rab-rej-violation-for-sdu-param-bk
• rab-rej-violation-traffic-handel-prio-bk
• rab-rej-violation-for-gbr-bk
• rab-rej-usr-plane-ver-unsupported-bk
• rab-rej-iu-up-failure-bk
• rab-rej-reloc-alloc-expiry-bk
• rab-rej-reloc-failure-target-system-bk
• rab-rej-invalid-rdb-id-bk
• rab-rej-no-remaining-rab-bk
• rab-rej-interaction-with-other-proc-bk
• rab-rej-integrity-check-fail-bk
• rab-rej-req-type-not-supported-bk
• rab-rej-req-superseded-bk
• rab-rej-rel-due-to-ue-sig-con-rel-bk
• rab-rej-res-optimization-reloc-bk
• rab-rej-req-info-unavail-bk
• rab-rej-reloc-due-to-radio-reason-bk
• rab-rej-reloc-unsupported-target-system-bk
• rab-rej-directed-retry-bk
• rab-rej-radio-con-with-ue-lost-bk
• rab-rej-rnc-unable-to-estab-all-rfcs-bk
• rab-rej-deciphering-keys-unavail-bk
• rab-rej-dedicated-assistance-data-unavail-bk
• rab-rej-reloc-target-not-allowed-bk
• rab-rej-location-reporting-congestion-bk
• rab-rej-reduce-load-in-serving-cell-bk
• rab-rej-no-radio-res-avail-in-target-cell-bk
• rab-rej-geran-iu-mode-failure-bk
• rab-rej-access-restrict-shared-nwtk-bk
• rab-rej-incoming-reloc-nwt-support-puesbine-bk
• rab-rej-traffic-target-more-source-cell-bk
• rab-rej-mbms-no-multicat-svc-for-ue-bk
• rab-rej-mbms-unknown-ue-id-bk
• rab-rej-mbms-sess-start-no-data-bearer-bk
• rab-rej-mbms-supereed-nnsf-bk
• rab-rej-mbms-ue-linking-already-done-bk
• rab-rej-mbms-ue-delinking-failure-bk
• rab-rej-tngi-unknown-bk
• rab-rej-ms-unspecifed-failure-bk

map-bk Schema

The following statistics will be backed up for recovery. They are derived from the SGSN schema and perform the same functions as the statistics of similar names minus the -bk extension. For example, the map-auth-succes-bk listed below performs the same functions as the map-auth-succes statistic in the SGSN schema:

• vpnname
• vpnid
• servname
• map-auth-succes-bk
• map-auth-succes-bk
• map-auth-fail-bk
• map-auth-timeouts-rcvd-bk
• mo-sms-in-progress-bk
• mt-sms-in-progress-bk
• mo-sms-attempted-bk
• mt-sms-attempted-bk
• mo-sms-successful-bk
SGSN Changes in Release 17

SGSN Enhancements for 17.0

1. mt-sms-successful-bk
2. map-gprs-update-loc-req-tx-bk
3. map-gprs-update-loc-rsp-tx-bk
4. map-gprs-update-loc-err-tx-bk
5. map-gprs-update-loc-timeouts-rx-bk
6. map-cancel-loc-req-rx-bk
7. map-cancel-loc-rsp-tx-bk
8. map-cancel-loc-err-tx-bk
9. map-del-subs-req-rx-bk
10. map-del-subs-rsp-tx-bk
11. map-del-subs-ret-tx-bk
12. map-imei-req-tx-bk
13. map-imei-success-bk
14. map-imei-fail-bk
15. map-imei-timeout-bk
16. map-auth-fail-rept-req-tx-bk
17. map-auth-fail-rept-rsp-rx-bk
18. map-auth-fail-rept-err-rx-bk
19. map-auth-fail-rept-timeouts-rcvd-bk
20. map-purge-req-tx-bk
21. map-purge-success-bk
22. map-purge-fail-bk
23. map-purge-timeouts-rcvd-bk

**sgtp-bk Schema**

The following statistics will be backed up for recovery. They are derived from the SGTP schema and perform the same functions as the statistics of similar names minus the `-bk` extension. For example, the `sgtpu-ggsn-byts-sent-bk` listed below performs the same functions as the `sgtpu-ggsn-byts-sent` statistic in the SGTP schema:

1. vpnid
2. vpnname
3. servname
4. sgtpu-ggsn-byts-sent-bk
5. sgtpu-rnc-byts-sent-bk
6. sgtpu-sgsn-byts-sent-bk
7. sgtpu-ggsn-byts-rcvd-bk
SGSN Changes in Release 17

- sgtpu-rnc-byts-rcvd-bk
- sgtpu-sgsn-byts-rcvd-bk

CSCum67205, CSCup61646 - S6d AVP support for MTC feature

Feature Changes

Extended T3312 Timer

This work is done as part of the SGSN’s MTC support in this release, please refer to CSCum47774, CSCum50056.

**Previous Behavior:** The SGSN did not support sending Extended T3312 timer value in Attach Accept and/or RAU Accept messages.

**New Behavior:** The SGSN supports the Extended T3312 timer value for Attach Accept and/or RAU Accept messages if the MS indicates support for extended periodic timer in the MS Network Feature Support.

With this release, for both Gn-SGSN and S4-SGSN a longer periodic RAU timer can be assigned to the M2M UEs based on subscription. The following timer AVP is now supported for the “Subscribed Period TAU/RAU Timer” via the SGSN’s S6d interface: Subscribed-Period-RAU-TAU-Timer AVP. The Subscribed Period TAU/RAU Timer value can be included in the ISD (Insert Subscriber Data) from the HLR or in the ULA (Update Location Answer) from the HSS.

The maximum value for a standard T3312 timer value is 186 minutes and the new Extended T3312 timer maximum value is 18600 minutes. Using the longer value for routing area updates reduces network load from periodic RAU signaling.

**Important:** Now, despite enabling the Extended T3312 timer in the SGSN’s configuration, the SGSN may be prevented from sending the Extended T3312 timer value in messages as the SGSN now also supports the “Subscribed Periodic TAU/RAU Timer Withdrawn” flag (see CSCuo92276 for details).

**Important:** Now for both Gn-SGSN and S4-SGSN, no matter the configuration for the Extended T3312 timer, the SGSN no longer automatically sends Extended T3312 timer values in Attach/RAU Accept messages when offloading is enabled.

Command Changes

```
gmm Extended-T3312-timeout
```

A new `gmm` command keyword, *Extended-T3312-timeout*, enables the operator to determine how the SGSN handles Extended T3312 timer values in a 2G GPRS network environment.

```
cfg
    context context_name

    gprs-service service_name

    gmm Extended-T3312-timeout { value exT3312_minutes | when-subscribed } [ low-priority-ind-ue ]
```
no gmm Extended-T3312-timeout
end

Notes:

- **value**: This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.

- **exT3312_minutes**: Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.

- **when-subscribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in “MS Network Feature Support”.

- **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the “MS Device Properties”.

- **no**: This command filter instructs the SGSN to remove the Extended T3312 configuration from the GPRS Service configuration.

**gmm Extended-T3312-timeout**

A new **gmm** command keyword, **Extended-T3312-timeout**, enables the operator to determine how the SGSN handles Extended T3312 timer values in a 3G UMTS network environment.

configure

context context_name

    sgsn-service service_name

    Extended-T3312-timeout { value exT3312_minutes | when-subscribed } [ low-priority-ind-ue ]

    no gmm Extended-T3312-timeout

end

Notes:

- **value**: This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.

- **exT3312_minutes**: Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.

- **when-subscribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in “MS Network Feature Support”.
• **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the “MS Device Properties”.

• **no**: This command filter instructs the SGSN to remove the Extended T3312 configuration from the SGSN Service configuration.

### gmm Extended-T3312-timeout

A new `gmm` command, **Extended-T3312-timeout**, enables the operator to determine how the SGSN handles Extended T3312 timer values at the Call-Control Profile level.

(Reminder: a configuration in the Call-Control Profile would override an **Extended-T3312-timeout** done for either the GPRS or SGSN services. As well, a Call-Control Profile configuration enables the operator to finetune for Homers and Roamers.)

```plaintext
configure
call-control-profile profile_name
gmm Extended-T3312-timeout { value exT3312Minutes | when-subscribed } [ low-priority-ind-ue ]
no gmm Extended-T3312-timeout
end
```

**Notes:**

• **value**: This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.

• **exT3312Minutes**: Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.

• **when-subscribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in “MS Network Feature Support”.

• **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the “MS Device Properties”.

• **no**: This command filter instructs the SGSN to remove the Extended T3312 configuration from the Call-Control Profile configuration.

---

**CSCuo54664 - Port 21/1 reported errors, LMI down**

**Feature Changes**

**Loopback Command Deprecated**
**Previous Behavior:** The `loopback` command under the Channelized Port Configuration Mode is used to configure the type of loopback mode used for diagnostic testing.

**New Behavior:** The `loopback` command under the Channelized Port Configuration Mode is now deprecated. The command will not be visible under the listing of available commands for Channelized Port Configuration Mode. If the command is executed accidentally, the following error message is displayed:

**Warning:** `loopback` cli not supported for optical ports

**Customer Impact:** The loopback command for optical cards is now concealed. If the command is accidentally executed a warning message is displayed.

---

**Command Changes**

`loopback`

The `loopback` command under the Channelized Port Configuration Mode is now deprecated. The command will not be visible under the listing of available commands for Channelized Port Configuration Mode. If the command is executed accidentally, the following error message is displayed:

**Warning:** `loopback` cli not supported for optical ports

---

**CSCuo88086 - Update Location Answer with 36 EPS and 36 GPRS subscription fails**

---

**Feature Changes**

**Limiting the Length of Incoming Messages on S6a/S6d Interface**

**Previous Behavior:** The length of incoming messages on S6a/S6d interface do not have a pre-defined limit. This results in crashes.

**New Behavior:** The length of incoming messages on S6a/S6d interface is now limited to “8192” bytes. If the message is a request, "UNABLE_TO_COMPLY" would be sent as a response. If it is a response, the message would be discarded.

**Customer Impact:** Messages like ULA and ISD needs to be sent in multiple messages each of the message length not more than “8192” bytes.

---

**CSCuo92276 - Support for 'Subscribed Periodic TAU/RAU Timer withdrawn' in MAP DSD**

---

**Feature Changes**

‘Subscribed Periodic TAU/RAU Timer Withdrawn’ Flag in MAP DSD Messages

This work is done as part of the functionality supporting the SGSN’s machine type communications (MTC) overload control mechanisms support in this release, please refer to CSCum47774, CSCum50056.
**Previous Behavior:** The SGSN did not support the "Subscribed Periodic TAU-RAU Timer Withdrawn" Flag in MAP DSD (delete subscriber data) messages.

**New Behavior:** The SGSN now supports the "Subscribed Periodic TAU-RAU Timer Withdrawn" Flag in MAP DSD messages. This flag indicates to the SGSN that the subscriber no longer has a subscription for the “subscribed periodic RAU/TAU timer” (Extended T3312 timer) value, so

- the SGSN will delete any subscribed periodic RAU/TAU timer value information when it is received from the HLR, and
- the SGSN will no longer send Extended T3312 in Attach/RAU Accept messages for that subscriber when gmm Extended-T3312-timeout when-subscribed is configured. (For command details, refer to CSCum67205 earlier in this Release Note.)

**CSCup06636 - UE cap in ctxt rsp,gtp ident rsp to be used for interface selection.**

**Feature Changes**

**UE Capability Used to Determine Interface Selection**

**Previous Behavior:** Only ms_network_capability received in RAU request was considered for interface selection.

**New Behavior:** The ms_network_capability received in context response and the forward re-location request will be considered for interface selection for RAU and SRNS scenarios. The ms_net_capability received in context response and forward re-location request will be considered only if ms_net_cap is not sent in RAU request.

**CSCup11529 - Statistics and bulkstats support for MTC**

**Feature Changes**

**Statistics Support for New MTC Functionality**

New bulk statistics and display counters have been added as part of the SGSN’s MTC congestion control support in this release, please refer to CSCum47774, CSCum50056.

**Performance Indicator Changes**

**SGSN Schema**

The following Mobility Management bulk statistics have been added to the SGSN:

- 3g-att-req-with-lapi
- 3g-att-req-without-lapi
- ret-3g-att-req-with-lapi
- ret-3g-att-req-without-lapi
- 3g-att-rej-with-lapi-cong
SGSN Changes in Release 17

- 3g-att-rej-without-lapi-cong
- 3g-att-rej-apn-based-cong
- 3g-rau-req-with-lapi
- 3g-rau-req-without-lapi
- ret-3g-rau-req-with-lapi
- ret-3g-rau-req-without-lapi
- 3g-rau-rej-with-lapi-cong
- 3g-rau-rej-without-lapi-cong
- 3g-rau-req-apn-based-cong
- 3g-serv-req-with-lapi
- 3g-serv-req-without-lapi
- ret-3g-serv-req-with-lapi
- ret-3g-serv-req-without-lapi
- 3g-serv-req-rej-with-lapi-cong
- 3g-serv-req-rej-without-lapi-cong
- 3G-service-rej-congestion
- 3g-serv-req-drop-with-lapi-cong
- 3g-serv-req-drop-without-lapi-cong
- 3g-rau-drop-with-lapi-cong
- 3g-rau-drop-without-lapi-cong
- 2g-attach-req-with-lapi
- 2g-attach-req-without-lapi
- 2g-attach-rej-cong-with-lapi
- 2g-attach-rej-cong-without-lapi
- 2g-attach-rej-cong-apn
- 2g-rau-req-with-lapi
- 2g-rau-req-without-lapi
- 2g-inter-sgsn-rau-rej-cong-with-lapi
- 2g-inter-sgsn-rau-rej-cong-without-lapi
- 2g-inter-sgsn-rau-rej-cong-apn
- 2g-intra-rau-req-cong
- 2g-intra-rau-req-cong-drop-with-lapi
- 2g-intra-rau-req-cong-drop-without-lapi
- 2g-intra-rau-rej-cong
- 2g-intra-rau-rej-with-lapi
SGSN Schema

The following Session Management bulk statistics have been added to the SGSN:

- 3g-activated-gn-with-lapi
- 3g-activated-gn-without-lapi
- 2g-activated-gn-with-lapi
- 2g-activated-gn-without-lapi
- 3g-activated-s4-with-lapi
- 3g-activated-s4-without-lapi
- 2g-activated-s4-with-lapi
- 2g-activated-s4-without-lapi
- 3g-activated-gn-pdp-ctx-with-lapi
- 3g-activated-gn-pdp-ctx-without-lapi
- 2g-activated-gn-pdp-ctx-with-lapi
- 2g-activated-gn-pdp-ctx-without-lapi
- 3g-activated-s4-pdp-ctx-with-lapi
- 3g-activated-s4-pdp-ctx-without-lapi
- 2g-activated-s4-pdp-ctx-with-lapi
- 2g-activated-s4-pdp-ctx-without-lapi
- 3g-activation-with-lapi-req
- 2g-activation-with-lapi-req
- 3g-primary-activation-with-lapi-req
- 2g-primary-activation-with-lapi-req
- 3g-secondary-activation-with-lapi-req
- 2g-secondary-activation-with-lapi-req
- 3g-primary-actv-congestion-reject
- 3g-primary-actv-congestion-lapi-reject
- 2g-primary-actv-congestion-reject
- 2g-primary-actv-congestion-lapi-reject
- 3g-secondary-actv-congestion-reject
- 3g-secondary-actv-congestion-lapi-reject
- 2g-secondary-actv-congestion-reject
- 2g-secondary-actv-congestion-lapi-reject
- 3g-modify-req-rx-with-lapi
- 2g-modify-req-rx-with-lapi
- 3g-modify-tx-congestion-reject
- 3g-modify-tx-congestion-lapi-reject
- 2g-modify-tx-congestion-reject
- 2g-modify-tx-congestion-lapi-reject

**show gmm-sm statistics verbose**

The following are the MM counters added in support of the new MTC congestion control functionality:

- 3G-Att-Req-with-LAPI
- 3G-Att-Req-without-LAPI
- Ret-3G-Req-With-LAPI
- Ret-3G-Req-Without-LAPI
- 3G-Att-Rej-Cong-With-LAPI
- 3G-Att-Rej-Cong-Without-LAPI
- 3G-Att-Rej-APN-Based-Cong
- 3G-RAU-Req-with-LAPI
- 3G-RAU-Req-without-LAPI
- Ret-3G-RAU-With-LAPI
- Ret-3G-RAU-Without-LAPI
- 3G-RAU-Rej-Cong-With-LAPI
- 3G-RAU-Rej-Cong-Without-LAPI
- 3G-RAU-Rej-APN-Based-Cong
- 3G-Serv-Req-With-LAPI
- 3G-Serv-Req-Without-LAPI
- Ret-3G-Req-With-LAPI
- Ret-3G-Req-Without-LAPI
- 3G-Serv-Rej-Cong-Without-LAPI
- 3G-Serv-Rej-Cong-Without-LAPI
- 3G-Congestion [under "Service Reject Causes:"
- Congestion (With LAPI) [under "Service Requests Drops"
- Congestion (non LAPI) [under "Service Requests Drops"
- Congestion (With LAPI) [ under "Routing Area Update Requests Drops:"
- Congestion (non LAPI) [ under "Routing Area Update Requests Drops:"
- Attach ReqsWith LAPI
- Attach ReqsWithout LAPI
- Attach Cong Rej(LAPI)
- Attach Cong Rej(non LAPI)
- Attach APN Cong Reject
- RAU ReqsWith LAPI
- RAU ReqsWithout LAPI
- RAU reject Cong LAPI
- RAU reject Cong non-LAPI
- RAU reject APN based Cong
- Dropped due to congestion
- With LAPI
- Without LAPI
- RAU reject Cong LAPI
- RAU reject Cong non-LAPI
- Inter RAT Congestion Reject
- Congestion rej with LAPI
- Congestion rej without LAPI
- Inter GPRS Srv Rau Cong Rej
- Congestion rej with LAPI
- Congestion rej without LAPI
- Inter RAT Congestion Drop
- Congestion drop with LAPI
- Congestion drop without LAPI
- Inter GPRS Srv Rau Cong Drop
- Congestion drop with LAPI
- Congestion drop without LAPI

**show gmm-sm statistics verbose**

The following are the SM counters added in support of the new MTC congestion control functionality:

- Activated Subscribers 3G Activated Gn Interface
- Activated Subscribers 3G Activated Gn Interface
- Activated Subscribers 2G Activated Gn Interface
- Activated Subscribers 2G Activated Gn Interface
- Activated Subscribers 3G Activated S4 Interface
- Activated Subscribers 3G Activated S4 Interface
- Activated Subscribers 2G Activated S4 Interface
- Activated Subscribers 2G Activated S4 Interface
- Activate PDP Contexts 3G-Actv Pdp Ctx Gn Interface
- Activate PDP Contexts 3G-Actv Pdp Ctx Gn Interface
- Activate PDP Contexts 2G-Actv Pdp Ctx Gn Interface
- Activate PDP Contexts 2G-Actv Pdp Ctx Gn Interface
- Activate PDP Contexts 3G-Actv Pdp Ctx S4 Interface
- Activate PDP Contexts 3G-Actv Pdp Ctx S4 Interface
- Activate PDP Contexts 2G-Actv Pdp Ctx S4 Interface
- Activate PDP Contexts 2G-Actv Pdp Ctx S4 Interface
- Activate Context Request 3G-Actv-Request
- Activate Context Request 2G-Actv-Request
- Activate Context Request 3G-Secondary-Actv-Request Secondary-Actv-Request
- Activate Context Request 2G-Secondary-Actv-Request Secondary-Actv-Request
- Activate Context Reject Primary-Actv-Reject
- Activate Context Reject Primary-Actv-Reject
- Activate Context Reject Secondary-Actv-Reject
- Activate Context Reject Secondary-Actv-Reject
- Activate Context Reject Secondary-Actv-Reject
- Activate Context Reject Secondary-Actv-Reject
- Modify Context Request Modify-Request Rx 3G-Modify-Request Rx
- Modify Context Request Modify-Request Rx 2G-Modify-Request Rx
- Modify Context Reject Modify-Reject Tx
- Modify Context Reject Modify-Reject Tx
- Modify Context Reject Modify-Reject Tx
- Modify Context Reject Modify-Reject Tx

CSCup39995 - Reduce the number of SF failures to trigger CARD reboot

Feature Changes

PSC Card Re-boot during SF Monitoring Failures

**Previous Behavior:** Switch Fabric failures are resulting in more outage. Repeated Switch Fabric (SF) monitoring failures are resulting in npumgr re-starts. Hardware issues in the switch fabric hardware on the PSC lead to SF monitoring packet loss and thus npumgr re-starts. The PSC card reboot is triggered on the sixth occurrence of SF monitoring failure.

**New Behavior:** The PSC card reboot is now triggered on the second occurrence of SF monitoring failure.

**Customer Impact:** The customer can now experience less outage time due to PSC hardware issues which resulted in Switch Fabric monitoring failures.

CSCup46980 - SGSN not sending the Equipment status in show subscriber output

Feature Changes

Display Output of “Equipment Status” updated

**Previous Behavior:** When an unknown equipment gets attached to the SGSN, the “Equipment status” in the show outputs `show subscribers sgsn-only full` and `show subscribers gprs-only full` was displayed as N/A.

**New Behavior:** The “Equipment status” in the show outputs `show subscribers sgsn-only full` and `show subscribers gprs-only full` is now updated to display “Unknown Equipment” when an unknown equipment gets attached to the SGSN.

Performance Indicator Changes

`show subscribers sgsn-only full`, `show subscribers gprs-only full`

The “Equipment status” in the show outputs `show subscribers sgsn-only full` and `show subscribers gprs-only full` is now updated to display “Unknown Equipment” when an unknown equipment gets attached to the SGSN.
CSCup71741 - Congestion-Control: SM stats implementation required with LAPI

Performance Indicator Changes

show gmm-sm statistics sm-only

With this release, new counters have been added to provide LAPI statistics for Activate Request, Secondary Activate Request, Modf Request in both 2G and 3G.

Under the Activate Context Request heading:

- Total-Actv-Request:
- 3G-Actv-Request:
- 2G-Actv Request:
- With-LAPI-Request:
- With-LAPI-Request:
- PDP Type IPv4v6:
- PDP Type IPv4v6:
- Primary-Actv-Request:
- 3G-Primary-Actv-Request:
- 2G-Primary-Actv-Request:
- With-LAPI-Request:
- With-LAPI-Request:
- Secondary-Actv-Request:
- 3G-Secondary-Actv-Request:
- 2G-Secondary-Actv-Request:
- With-LAPI-Request:
- With-LAPI-Request:

CSCup79825 - Unexpected Data Value stats not pegged when check_imei_resp as UDV

Feature Changes

New Failure Cause in “show map statistics”

Previous Behavior: Only three failure causes were present in show map statistics command for Check IMEI Request. They were System Failure, Unexpected Data Value, and Unknown Equipment.
New Behavior: The “Unexpected Data value” (UDV) is a valid error cause in response to Check IMEI request in MAP version 1 only. “Data missing” along with “Unknown equipment” and “System Failure” are valid error causes from MAP version 2 onwards. A new failure cause “Data Missing” has been added for Check IMEI Request in the show map statistics output.

Performance Indicator Changes

show map statistics

The following failure cause has been added in the show map statistics output in response to Check IMEI requests:

- Data Missing

CSCup82824 - New disconnect reason for MM APN based congestion control

Feature Changes

Disconnect Reason for MM APN-based Congestion Control

This work is done as part of the functionality supporting the SGSN’s machine type communications (MTC) overload control mechanisms support in this release, please refer to CSCum47774, CSCum50056.

New Behavior: The SGSN now supports a new disconnect reason mm-apn-congestion-control(567) that will be pegged when Attach or new Inter-SGSN RAU calls are rejected because of APN-based Mobility Management congestion control. Statistics will be displayed when issuing the show session disconnect-reasons [verbose | sgsn-only | gprs-only] command.

CSCup99278 - Support for supported features negotiation with HSS is required

Feature Changes

Supported-features Negotiation with HSS

Previous Behavior: Supported-features were not negotiated with the HSS; the SGSN sent a hardcoded list of supported-features to the HSS during ULR.

New Behavior: Now the SGSN will negotiate the supported-features values with the HSS during ULR/ULA.

If the first ULA responds with diameter error code 5011, then the SGSN selects common features supported by both the SGSN and the HSS - selection based on comparison of feature lists at the SGSN and the HSS. And, then a new ULR will be initiated with an updated feature list value. The negotiated supported-features value will be sent in all subsequent messages.

Feature list negotiation will happen only once, so if the ULA for the 2nd ULR has an error response, then the call will be rejected.
CSCzn37980 - S4 SGSN functionality to be implemented

Feature Change

Excluding UTEID in MBR

In accordance with 3GPP TS 23.401 v11.8.0, if the SGSN and the S-GW are configured to release S4 U-Plane when the EPS bearer contexts associated with the released RABs are to be preserved, then the SGSN should not send SGSN address and TEID for U-Plane in the Modify Bearer Request (MBR).

Command Changes

rau-inter exclude-uteid-in-mbr

If RABs are not established at the target SGSN, then the new keyword exclude-uteid-in-mbr in the Call-Control Profile configuration mode, enables/disables the sending of the user plane fully qualified TEID (tunnel end-point identifier) in the MBR (Modify Bearer Request) during a new SGSN RAU over S16/S3. The following command has been updated in compliance with 3GPP TS 23.401 v11.8.0.

configure

    call-control-profile profile_name

    rau-inter exclude-uteid-in-mbr

    remove rau-inter exclude-uteid-in-mbr

    end

Notes:

- By default, the SGSN sends UTEID in the MBR.
- exclude-uteid-in-mbr : Keyword disables the SGSN from sending the UTEID in the MBR.
- remove : Included with the command, returns the SGSN to default functionality with regard to the sending of UTEID in the MBR.
Chapter 22
S-GW Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from S-GW in StarOS 17 software releases.

**Corrections have been made** to the following items:

- CSCum37090 - CSCuh34589 - MME restoration support at S-GW. Information has been added detailing **MME Restoration Standards Extension**.
S-GW Enhancements for 17.5

There are no S-GW enhancements for this release.
S-GW Enhancements for 17.4

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
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

**CSCut14324** - SGW sending PDP Reject with No resources on 3G Attach dual Bearer.

**Feature Changes**

**Behavior Change Due to Implementation of Fix for CSCut14324**

The fix for CSCut14324 has resulted in a behavior change.

**Previous Behavior:** When two Create Session Requests are received back to back with zero TEID from the MME/SGSN, the second CSReq is rejected by SGW with cause "No Resources Available."

**New Behavior:** When two Create Session Requests are received back to back with zero TEID from the MME/SGSN, the SGW handles both CSReqs and sends a CSRsp with cause "Request Accepted" for both PDNs.

**Customer Impact:** Operators can see that both the PDNs are successfully created.
CSCuu37427, CSCut14324 - Assertion failure
egtpc_handle_create_sess_req_msg_at_sgw_ingress

Feature Changes

Parallel Create Session Requests Processed Correctly

The fix implemented for CSCuu37427 and CSCut14324 has resulted in a behavior change.

**Previous Behavior:** When two parallel Create Session Requests (CSReqs) with different EBI and 0 TEID were received from the S4-SGSN, the second CSReq was rejected from the S-GW with the cause “No Resource Available.”

**New Behavior:** When two parallel CSReqs with different EBI and 0 TEID are received from the S4-SGSN, both of the CSReqs are processed and the PDNs are created successfully at the S-GW.

1. Operators will see that both the PDNs are created successfully after the fix if the two CSReqs are received from the S4-SGSN with 0 TEID and different EBI.
2. If two parallel CSReqs are received from the MME, then the old behavior of rejecting the second CSReq with the cause “No Resource Available” is applicable.
3. If one CSReq is received from the MME and the other from the S4-SGSN, or vice-versa, with the same or different EBI, then context replacement is triggered and the second CSReq results in the replacement of the existing PDN with a new PDN.
S-GW Enhancements for 17.3

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
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

CSCut14324 - SGW sending PDP Reject with No resources on 3G Attach dual Bearer.

Feature Changes

Behavior Change Due to Implementation of Fix for CSCut14324

The fix for CSCut14324 has resulted in a behavior change.

Previous Behavior: When two Create Session Requests are received back to back with zero TEID from the MME/SGSN, the second CSReq is rejected by SGW with cause "No Resources Available."

New Behavior: When two Create Session Requests are received back to back with zero TEID from the MME/SGSN, the SGW handles both CSReqs and sends a CSRsp with cause "Request Accepted" for both PDNs.

Customer Impact: Operators can see that both the PDNs are successfully created.
S-GW Enhancements for 17.2

There are no S-GW enhancements for this release.
S-GW Enhancements for 17.1

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

---

**CSCum88408, CSCum93286 - Separate Paging for IMS Service Inspection**

**Feature Changes**

**Support for Separate Paging for IMS Service Inspection**

When some operators add an additional IMS service besides VoLTE such as RCS, they can use the same IMS bearer between the two services. In this case, separate paging is supported at the MME using an ID which can be assigned from the S-GW according to the services, where the S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from using an ID which is assigned from SGW according to the services. The S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from (for example IP, Port and so on). After the MME receives this ID from the S-GW after IMS service inspection, the MME will do classified separate paging for each of the services as usual.

**Previous Behavior:** No private extension was present in Information Element in Downlink Data Notification message.
New Behavior: A new private extension is now present in Information Element in Downlink Data Notification message.

Important: This is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Command Changes

sgw-paging-profile three-tuple

This new command in Global Configuration Mode is used to create an S-GW paging profile for IMS paging and enter S-GW Paging Profile Configuration Mode.

```
configure
    sgu-paging-profile three-tuple
        no sgu-paging-profile three-tuple variable
    end
```

Notes:

- `no` removes the sgu-paging-profile.

ipv4 | ipv6 port protocol paging-identifier

These new commands in S-GW Paging Profile Configuration mode enable operators to specify a 3-tuple lookup (source IP address, source port and protocol) on the inner IP packet of the GTPU data packet at the S-GW.

```
configure
    sgu-paging-profile three-tuple
        {{ ipv4 ipv4-address | ipv6 ipv6_address }} port protocol {{ tcp | udp}} paging-identifier integer
        no {{ ipv4 ipv4-address | ipv6 ipv6_address }} port protocol {{ tcp | udp}}
    end
```

Notes:

- `ipv4 | ipv6` specifies the IP address to use for S-Separate Paging for IMS.
- `port` specifies the source port on the S-GW to use for IMS paging.
- `protocol` specifies the protocol type to which this SGW paging profile applies.
- `paging-identifier` specifies a service identifier for this SGW paging profile (for example, Data 0, VoLTE 1, RCS 2, and so on).

Example

```
configure
```
sgw-paging-profile three-tuple

    ipv4 address 1.1.1.1 port 30 protocol tcp paging-identifier 1
    ipv4 address 1.1.1.2 port 30 protocol tcp paging-identifier 2
    end

associate sgw-paging-profile three-tuple

The new `associate sgw-paging-profile three-tuple` command has been added in APN Profile Configuration mode to allow the association of an SGW Paging Profile with an APN profile on the S-GW.

```
configure

    apn-profile apn_profile_name

    associate sgw-paging-profile three-tuple

    remove associate sgw-paging-profile

    end
```

Notes:

- `remove` disables the SGW Paging Profile association.

**CSCup59406 - sesstrc task in over state during longevity/aggravator run**

**Feature Changes**

**Configuring Session Trace File Type**

To address the issues caused when the sesstrc task allocates memory over the allotted limit, under a random subscriber session trace load tests on P-GW/S-GW, support for B-type XML files is introduced in addition to the A-type files already supported.

**Previous Behavior:** The file type was A-type XML file and the type could not be changed.

**New Behavior:** The CLI has been modified (see `Command Changes` section) to allow the operator to select the file type generated by session trace. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. Each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

**Command Changes**

```
session trace network-element
```

The new `file-type` keyword enables the operator to determine which type of XML file is generated by the session trace:
configure

    session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw } [ file-type { a-type | b-type } ] [ collection-timer | tce-mode ]

    no session trace network-element { all | enb | ggsn | hnbgw | mme | pgw | sgw }

end

Notes:

• Default file-type is a-type.

• To keep the syntax simple, we recommend that you enter the file-type keyword prior to adding either of the other optional keywords to the command.

• To modify the session trace network-element configuration, you must first enter the no session trace network-element form of the command to remove the session trace configuration.

CSCur53899 - instance 5 should be sent in UL IDFT rsp from s.sgw to s.mme

Feature Changes

Send Correct Instance in IDFT Response from Source S-GW to Source MME During intra-EUTRAN HO

The fix implemented for CSCur53899 has introduced a behavior change.

Previous Behavior: Indirect Forwarding Tunnel Response (IDFT) Bearer Context Information Element (IE) from Source S-SGW to Source MME was not carrying instances 4 and 5 during an intra-E-UTRAN handover.

New Behavior: The IDFT Bearer Context IE from Source S-SGW to Source MME now includes instances 4 and 5 during an intra-E-UTRAN handover.
S-GW Enhancements for 17.0

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.

*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

**CSCue35977- EGTPC MME restoration support at SGW**

**Feature Changes**

**EGTPC MME restoration support at SGW**

EGTPC provides a new configuration option to enable Network Triggered Service Restoration (NTSR) capability in the Node Feature information element in the Echo message.

**Command Changes**

`network-triggered-service-restoration`

This new command has been added to EGTP Configuration Mode to option to enable Network Triggered Service Restoration capability (NTSR) in the Node Feature IE in the Echo message.
MME Restoration Support at the S-GW

MME restoration is a 3GPP specification-based feature designed to gracefully handle the sessions at S-GW once S-GW detects that the MME has failed or restarted. If the S-GW detects an MME failure based on a different restart counter in the Recovery IE in any GTP Signaling message or Echo Request / Response, it will terminate sessions and not maintain any PDN connections.

As a part of this feature, if a S-GW detects that a MME or S4-SGSN has restarted, instead of removing all the resources associated with the peer node, the S-GW shall maintain the PDN connection table data and MM bearer contexts for some specific S5/S8 bearer contexts eligible for network initiated service restoration, and initiate the deletion of the resources associated with all the other S5/S8 bearers.

The S5/S8 bearers eligible for network initiated service restoration are determined by the S-GW based on operator's policy, for example, based on the QCI and/or ARP and/or APN.

The benefit of this feature is that it provides support for the geo-redundant pool feature on the S4-SGSN/MME. In order to restore session when the MME receives a DDN, the S-GW triggers restoration when the serving MME is unavailable, by selecting another MME and sending DDN. This helps in faster service restoration/continuity in case of MME/S4-SGSN failures.

MME Restoration Standards Extension

The solution to recover from MME node failures proposed in the 3GPP standards rely on the deployment of MME pools where each pool services a coverage area. Following an MME failure, the S-GW and MSC/VLR nodes may select the same MME that used to service a UE, if it has restarted, or an alternate MME in the same pool to process Network-initiated signaling that it received in accordance with the NTSR procedures defined in 3GPP TS 23.007 Release 11.

For a failed MME, the S-GW will select an alternate MME from the associated NTSR pool in the round robin fashion in each sessmgr instance.
Command Changes

access-peer-map

This command has been added to S-GW Service Configuration Mode to associate the access/ingress side of the peer-map to the configured S-GW service.

```
configure
  context ingress_context_name
  sgw-service sgw_service_name
    associate access-peer-map map_name
  no associate access-peer-map cmd variable
end
```

Notes:

•

ntsr

This command has been added to APN Profile Configuration Mode to configure qci and arp in the apn-profile. The S-GW will decide to retain or release the bearer based on the configured qci/arp, after path failure is detected on ingress side of S-GW. The S-GW can configure a maximum of 2 qci and arp-priority-watermark per apn-profile. The apn-profile can also be configured to retain all bearers from that PDN.

```
configure
  apn-profile apn_profile_name
    ntsr { all | qci number arp-priority-watermark number }
end
```

Notes:

• ntsr enables the network triggered service restoration configuration.
• qci is the Quality of Class Identifier for this NTSR configuration.
• arp-watermark specifies the ARP watermark for the configuration.
• all specifies the NTSR configuration is enabled for all bearers with any qci or arp for MME restoration.

ntsr pool

This command is used in NTSR Pool Configuration Mode to configure a pool of IP addresses associated with a pool ID and pool type (either MME or S4-SGSN).

```
configure
  ntsr pool-id number pool-type [ mme | s4-sgsn ]
```
peer-ip-address \{ ipv4-address ipv4_address | ipv6-address ipv6_address \}
no peer-ip-address \{ ipv4-address ipv4_address | ipv6-address ipv6_address \}
end

Notes:
• **peer-ip-address** configures an IPv4/IPv6 address as part of an MME or S4-SGSN pool.

ntsr pool-id

This new command in Peer-Profile Configuration Mode enables network triggered service restoration (ntsr) and identifies the Pool ID to use for the feature.

configure

peer-profile service-type sgw-access name profile_name
  ntsr pool-id number
  no ntsr pool-id number
end

Notes:
• **ntsr pool-id** is the network triggered service restoration pool ID. Must be an integer from 1 to 65535.

ntsr session-hold timeout <number>

This command has been added to S-GW Service Configuration Mode to configure a timer to hold the session after path failure is detected during MME restoration.

configure

context ingress_context_name
  sgw-service sgw-service_name
    ntsr session-hold timeout duration_seconds
    no ntsr session-hold timeout
end

Notes:
• **ntsr session-hold timeout** configures the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration. Valid entries are from 1 to 3600 seconds.

peer-ip-address

This command configures the peer type for an MME or S4-SGSN pool.

configure
\texttt{ntsr pool number peer-type [ mme | s4-sgsn ]}

\texttt{end}

Notes:
- The \texttt{ntsr pool number} must be an integer from 1 to 65335.

\textbf{access-peer map}

This command has been added to S-GW Service Configuration Mode to enable the configuration of the network/egress side peer map for this S-GW service.

\texttt{configure}

\texttt{context egress\_context\_name}

\texttt{sgw-service sgw-service\_name}

\texttt{associate access-peer-map peer_map_name}

\texttt{no associate access-peer-map peer_map_name}

\texttt{end}

\textbf{sgw-access}

This new command has been added to Peer-Profile Configuration Mode to configure a profile for peer nodes of the S-GW towards the S4/S11 interfaces.

\texttt{configure}

\texttt{peer-profile service-type sgw-access name profile\_name}

\texttt{end}

Notes:
- Where \texttt{sgs-access} configures a profile for peer nodes of the S-GW towards the S4/S11 interfaces.

\section*{Performance Indicator Changes}

\textbf{S-GW Schema}

The following bulk statistics have been implemented to support the MME Restoration feature.

- \texttt{ntsr-peer-failure-pdn-retained}
- \texttt{ntsr-peer-failure-pdn-restored}
- \texttt{ntsr-peer-failure-pdn-released}
- \texttt{ntsr-peer-restart-pdn-retained}
- \texttt{ntsr-peer-restart-pdn-restored}
- \texttt{ntsr-peer-restart-pdn-released}
SAEGW Schema

The following bulk statistics have been implemented to support the MME Restoration feature.

- sgw-ntsr-peer-failure-pdn-retained
- sgw-ntsr-peer-failure-pdn-restored
- sgw-ntsr-peer-failure-pdn-released
- sgw-ntsr-peer-restart-pdn-retained
- sgw-ntsr-peer-restart-pdn-restored
- sgw-ntsr-peer-restart-pdn-released

**show apn-profile full all**

The output of this command has been enhanced to provide configuration information related to the qci and arp values in the APN profile.

- NTSR
  - QCI
    - <number>
    - <number>
  - ARP-priority-watermark
    - <number>
    - <number>

**show ???**

The output of this command has been enhanced to provide configuration information related to the NTSR session -hold timeout.

- EGTP: Enabled/Disabled
  - Session Hold Timer: Enabled/Disabled
    - Timeout: <value in seconds>

**show apn-profile full all**

The output of this command has been enhanced to provide configuration information related to the qci and arp values in the APN profile.

- NTSR
  - QCI
    - <number>
    - <number>
    - ALL
  - ARP-priority-watermark
- <number>
- <number>
- ALL

show ntsr-pool all

This command outputs configuration parameters for each configured NTSR pools on the S-GW

- NTSR pool-id <number>
- NTSR Pool type <MME or S4-SGSN>

show ntsr-pool full all

This command outputs all configuration parameters for all NTSR pools configured on the S-GW

- NTSR pool-id <number>
- NTSR Pool type <MME or S4-SGSN>
- peer-address-pairs
  - ipv4 (IPv4 addresses)
  - ipv6 (IPv6 addresses)

show ntsr-pool full pool-id <number>

This command outputs all configuration parameters for the specified NTSR pool on the S-GW

- NTSR pool-id <number>
- NTSR Pool type <MME or S4-SGSN>
- peer-address-pairs
  - ipv4 (IPv4 addresses)
  - ipv6 (IPv6 addresses)

show ntsr-pool pool-id <number>

This command outputs configuration parameters for the specified NTSR pool on the S-GW.

- NTSR pool-id <number>
- NTSR Pool type <MME or S4-SGSN>

show peer-profile full all

The output of this command has been enhanced to provide information related to S-GW Access Peer Profiles, including the peer-profile name and NTSR pool ID, if it is configured.

- SGW Access Peer Profiles
  - Peer Profile Name <name>
    - NTSR pool id <number>
show sgw-service name <name>

The output of this command has been enhanced to indicate the Access Peer Map associated with the S-GW service.

- Access Peer Map: <peer_map_name>

show sgw-service statistics all

The output of this command has been enhanced to provide PDN NTSR statistics.

- PDNs NTSR Statistics
  - Peer Failure
    - Retained
    - Released
    - Restored
  - Peer Restart
    - Retained
    - Released
    - Restored

show subscribers sgw-only full all

The output of this command has been enhanced to provide the NTSR state, and whether the bearer is capable for restoration.

- Ntsr state
  - Bearer capable for restoration: Yes/No

CSCul04397 - Network Provided Location Info (NPLI) for IMS

Feature Changes

NPLI (Network Provided Location Information) for IMS Support

In a Circuit Switched environment, the MSC gets the current Cell-ID information provided by the RNC/BSC. This location information is used for charging purposes and/or for recording the location of a subscriber for whom the government authority requests communication history. In a Packet Switched environment – when IMS is used – there may not be any control plane signaling. In IMS, the UE can provide location information but the information can’t be trusted. Even though the P-GW can provide the current Cell-ID, that is possible only when location change notification is enabled (which causes excessive network signaling). There is no mechanism in the network today to proactively or mid-session query for the user location information. NPLI is introduced by 3GPP to get location information for a subscriber based on the request from IMS core.
If the AF requests the PCRF to report the Access network information, the PCRF provides the requested Access network information indication (e.g. user location and/or user time zone information) to the PCEF within the Required-Access-Info AVP included within the Charging-Rule-Definition AVP of an appropriate PCC rule. The PCRF also provides the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP (if this event trigger is not yet set). If the ACCESS_NETWORK_INFO_REPORT event trigger is set, upon installation, modification and removal of any PCC rule(s) containing the Required-Access-Info AVP PGW determines if it can obtain the required location information for the used IP CAN type.

The P-GW provides the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-Time Zone AVP as requested by the PCRF; the PGW also provides the ACCESS_NETWORK_INFO_REPORT event trigger within the Event-Trigger AVP.

During bearer deactivation or a UE detach procedure, the P-GW shall provide the access network information to the PCRF within the 3GPP-User-Location-Info AVP and information on when the UE was last known to be in that location within User-Location-Info-Time AVP. If the PCRF requested User location info is part of the Required-Access-Info AVP and it is not available in the P-GW, the P-GW provides the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP.

The benefit of this feature is that it allows the EPC core to support an efficient way of reporting ULI and Time-Zone information of the subscriber to the IMS core.

**Important:** Use of NPLI requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

### CSCul17198 - [SGW] GTP echo and GTP message retry shall be configured separately

#### Feature Changes

**Separate Configuration for GTPC Echo and GTPC Non-Echo Messages**

Previously, the GTP echo and GTP message retry timer could be configured separately, but the number of GTPC echo requests could not. The maximum retry number now can be configured separately along similar lines as the timer configuration.

Both in egtp-service and peer-profile modes, the `echo-max-retransmissions` keyword is added to allow the separate configuration of GTPC echo retransmissions.

**Previous Behavior:** `max-retry` option is common for both GTPC Service Configuration Mode and Peer-Profile Configuration modes.

**New Behavior:** `echo-max-retransmissions` is introduced explicitly for the configuration of echo max retransmissions in both GTPC Service Configuration Mode and Peer-Profile Configuration Mode.

#### Command Changes

**echo-max-retransmissions**

The `echo-max-retransmissions` keyword is now available in both EGTP Service Configuration Mode and Peer Profile Configuration Mode. This keyword is available to allow for the separate configuration of GTP echo retransmissions in each mode.
configure

context context_name

egtp-service egtp_service_name

gtpc echo-max-retransmissions number

default gtpc echo-max-retransmissions
end

configure

peer-profile service-type sgw-access name peer_profile_name

egtp-service egtp_service_name

gtpc echo-max-retransmissions number

default gtpc echo-max-retransmissions
end

Notes:

- **echo-max-retransmissions**: Configures the maximum retries for GTP Echo requests. This option must be an integer from 0 to 15. The default is 4. If **echo-max-retransmissions** configuration option is not configured, then the **max-retransmissions** configuration will be used for maximum number of echo retries.

Performance Indicator Changes

**show egtp-service [ all | name service_name ]**

The output of this command has been enhanced to show the configured number of GTPC echo max retransmissions.

- GTPC Echo Max Retransmission

**show peer-profile full [ all | name service_name ]**

The output of this command has been enhanced to show the configured number of GTPC echo max retransmissions.

- GTPC echo max retransmissions

**CSCum61765 - [17.0] SGW support for PCSCF Discovery**

Feature Changes

**P-CSCF Discovery Support on the S-GW**

P-CSCF Discovery is now supported on the S-GW. Support for P-CSCF Recovery Indication in Private Extension has been implemented. The S-GW will forward this indication to the P-GW. The P-GW includes the PCSCF address in the PCO of the UBReq.

Previous Behavior: MBReq with P-CSCF Restoration was not supported.
New Behavior: MBReq with P-CSCF Restoration will be supported at S-GW.

CSCum65507, CSCum88401 - Support DDN Profile at SGW

Feature Changes

DDN Profile Support on the S-GW

As part of the implementation for CSCum88401, the S-GW now supports DDN profiles. Specifically, it allows the configuration of a ddn-apn-profile for DDN configuration of preferential bearers. The existing configuration at the APN configuration level is enhanced to associate a ddn-apn-profile which allows qci specific configuration. Only 4 QCI values are supported for configuration per ddn-apn-profile.

The existing configuration at sgw-service config level is enhanced to set the ddn success_action timer. This timer applies to the case where DDN Ack is received in response to DDN from S-GW. But, the subsequent DDN Failure is dropped on the wire. In such a case, S-GW is stuck waiting for MBR and does not come out of such a situation.

With this new timer, the S-GW would start it on receiving DDN Ack and on expiry, then reinitiate the DDN towards the UE. This time, it will start the timer once again to see if the MBR is received or not. If no MBR is received, all buffered data is cleared and S-GW goes into no data available state. So, only on new data, the paging will be initiated again.

Command Changes

associate ddn-apn-profile <profile_name>

This command has been added to APN Profile Configuration Mode to associate a DDN APN Profile with an APN Profile configuration.

configure

    apn-profile apn_profile_name

    associate ddn-apn-profile ddn_apn_profile_name

    remove associate ddn-apn-profile

    end

ddn-apn-profile

This command has been added to Global Configuration Mode to enter DDN APN Profile Configuration Mode.

configure

    ddn-apn-profile ddn-apn_profile_name

    no ddn-apn-profile ddn-apn_profile_name

    end

qci <value> ddn failure-action pkt-drop-timer <value>
This command has been added to DDN APN Profile Configuration Mode to configure the time for which no data for UE is buffered by S-GW. This timer kicks in the moment DDN failure is received.

```
configure

  ddn-apn-profile  ddn-apn_profile_name
  qci  value  ddn  failure-action  pkt-drop-timer  value
  remove  qci  value

end
```

Notes:

- This value supersedes the one configured at sgw-service-level.
- When DDN failure is received, the minimum of the pkt-drop-timer of all QCIs having data is started.

```
qci  <value>  ddn  ignore-ddn-timers
```

This command has been added to DDN APN Profile Configuration Mode so that if any DDN timer (DDN delay or DDN failure) is started and data arrives on a bearer with QCI for which this flag is set, then S-GW will stop that timer and send DDN again. This helps S-GW to send DDN for preferential bearers immediately on receiving new data.

```
configure

  ddn-apn-profile  ddn-apn_profile_name
  qci  value  ddn  ignore-ddn-timers
  remove  qci  value

end
```

```
qci  <value>  ddn  min-buf-size  <number>
```

This command has been added to ddn-profile-configuration mode to configure a buffer allocated for storing data packets for each bearer when the UE is in idle state. This field is used to set higher buffer value for preferential bearers.

```
configure

  ddn-apn-profile  ddn-apn_profile_name
  qci  value  ddn  min-buf-size  value
  remove  qci  value

end
```

Notes:

- This is the buffer allocated for storing data packets for each bearer when the UE is in idle state. This field is used to set higher buffer value for preferential bearers. Valid entries are from 2 to 4 KB.
- Set this field to a value higher than 2Kb only for QCI values corresponding to preferential bearers (like VoLTE). If the default buffer size of all QCI values is increased, it would decrease the system performance due to higher memory consumption and such a configuration is NOT recommended.

```
ddn success-action no-user-connect ddn-retry-timer <value>
```

This command has been added to S-GW Service Configuration Mode to resend the DDN if no MBR is received within the specified timer value.

```
configure
    sgw-service sgw_service_name
    ddn success-action no-user-connect ddn-retry-timer value
    default ddn success-action no-user-connect ddn-retry-timer
end
```

Notes:
- The value of DDN retry timer is 60sec. Valid entries are from 60 to 300 seconds. After receiving DDN Ack, this timer is started and when it expires, S-GW sends one DDN and restarts the timer for same value. If no MBR is received within this time, S-GW clears the data buffers and waits for new data to trigger a new DDN.

```
isr-sequential-paging
```

This command has been added to DDN APN Profile Configuration Mode to configure Idle Mode Signaling Reduction (ISR) sequential paging. The behavior is similar to R16.0. ISR Sequential Paging is disabled by default and only when set will result in enabling of this feature for that particular APN.

```
configure
    ddn-apn-profile ddn-apn_profile_name
        isr-sequential-paging
        remove isr-sequential-paging
end
```

**Performance Indicator Changes**

**show apn-profile full**

This enhanced command provides the name(s) of the configured ddn-apn-profile(s).
- ddn-apn-profile

**show ddn-apn-profile all**

This new command provides all configuration parameters for configured ddn-apn-profiles on the S-GW.
- DDN-APN-profile name
- ISR Sequential Paging (enabled / disabled)
• QCI <value>
• Minimum buffer size for buffering idle mode data
• ddn failure-action pkt-drop-timer
• Stop paging timers

**show sgw-service <all | name>**

This CLI is enhanced to show the ddn-success-action no-user-connect ddn-retry-timer setting.
• ddn-success-action no-user-connect ddn-retry-timer

**show sgw-service statistics**

This CLI is enhanced to show the dropped data packets/bytes distribution based on reason of dropping.
• Data Discarded by Reason-Type
• Shared Buffer Full
  • Packets Discarded
  • Bytes Discarded
• Dedicated Buffer Full
  • Packets Discarded
  • Bytes Discarded
• S1U State Inactive
  • Packets Discarded
  • Bytes Discarded
• Paging Throttled
  • Packets Discarded
  • Bytes Discarded
• Paging Failure
  • No User Connect Data Flushed
    • Packets Discarded
    • Bytes Discarded
  • Buffered Data Flushed
    • Packets Discarded
    • Bytes Discarded

**show sgw-service statistics <all | name> verbose**

This CLI is enhanced to show the number of times no-user-connect DDN was triggered and expired.
• No User Connect Triggered
• No User Connect Expired
**CSCum79565 - MTC-Feature: CDR support for including LAPI (signaling priority)**

**Feature Changes**

**CDR Support for Including LAPI (Signaling Priority)**

This feature is related to M2M support. 3GPP has added the LAPI (signaling priority) indication being sent in the GTP messages, to indicate that the PDN is a low priority bearer and thus can be treated accordingly. Changes are done to support this indication in S-GW/P-GW/SAEGW. APN backoff timer support based on LAPI indication is not yet supported, and is planned for a future release.

3GPP has also added a new AVP in CDR defined in TS 32.298 named “lowPriorityIndicator”. If S-GW/P-GW receives LAPI indicator in GTP, SGW-CDR and PGW-CDR generated will contain LAPI indication.

The benefit of this feature is that it provides support for carrying the LAPI attribute in SGW-CDR and PGW-CDRs, so that billing system can then accordingly bill for that PDN.

**CSCum88387 - Graceful PDN Shutdown**

**Feature Changes**

**Intelligent Graceful Shutdown Support for VoLTE Calls**

In 16.0, the Graceful Shutdown feature was added. There are likely to be cases where an Operator would need to shutdown a P-GW/S-GW/SAEGW for upgrade/maintenance purpose, while doing so there is a need for a means by which the VoLTE calls on such nodes are cleaned up in a graceful manner, so that ongoing calls are not interrupted, thus improving user experience.

In 16.0 an external script or manual effort was needed to do graceful shutdown by executing the enhanced “clear subscriber” CLI (“clear subscriber non-volte”). In 17.0, complete automation of Graceful shutdown is performed so that there is no need for an external script or manual intervention.

**CSCum88401, CSCum65507 - Packet drop timer for Volte bearer**

**Feature Changes**

**Packet Drop Timer for VoLTE Bearer**

A Packet Drop Timer for VoLTE bearers has been implemented. Previously, the S-GW dropped data packets for a configurable time period upon receiving DDN failure notification for a call. The same timer period was applicable across all bearers. Now this time period can be made configurable on the basis of the QCI and/or ARP value of the bearer. This will help to have more aggressive paging for some QCIs and/or ARPs as compared to others. This will help mainly for IMS calls, where for IMS signaling bearers with specific QCI-ARP operators can have a lower time period for IMS signaling bearer as compared to other bearers, in order to increase the likelihood of a UE response after returning from out of coverage.
CSCup42450 - SGW TRAFPOL: counters for default bearer aren't getting updt

Feature Changes

S-GW Traffic Policing

The fix for CSCup42450 has introduced a behavior change.

**Previous Behavior:** Traffic policy was applied based on bearer QCI value. (for non gbr qci range was qci >=5 and =<9 and for gbr bearer qci range was (qci < 5) || (qci > 9). This was the default behavior.

**New Behavior:** S-GW Traffic policing will be applicable to all the bearers regardless of their QCI values. For non-standard QCI also Traffic policy will be applied. GBR and non-GBR differentiation is based on the apn ambr value. As per the configured gbr and non-gbr traffic policy, for all the bearers regardless of their QCI values traffic policy will be applied.

**Customer Impact:** Traffic policy is applied to all the bearers irrespective of their QCI values. For non-standard QCI also Traffic policy will be applied.

CSCuq55963 - SGW ISR paging is not initiated for bearer activation for ISR sesison

Feature Changes

Support for Sending LBI in DDN Request for Control-Paging on Create Bearer Request

The fix for CSCuq55963 has resulted in a behavior change.

**Previous Behavior:** The S-GW did not include the LBI in the DDN request for control-paging on a Create Bearer Request.

**New Behavior:** The S-GW now includes the LBI in the DDN request for control-paging on a Create Bearer Request.
Chapter 23
SNMP MIB Changes in Release 17

This chapter identifies SNMP MIB objects and alarms added to, modified for, or deprecated from StarOS 17 software releases.
SNMP MIB Object Changes for 17.5

This section provides information on SNMP MIB object changes in release 17.5.

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 17.5.

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 17.5.

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 17.5.

The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 17.5

This section provides information on SNMP MIB alarm changes in release 17.5.

⚠️ **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 17.5.

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 17.5.

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 17.5.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 17.5

This section provides information on SNMP MIB conformance changes in release 17.5.

**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 17.5.

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 17.5.

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 17.5.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 17.4

This section provides information on SNMP MIB object changes in release 17.4.

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 17.4.

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 17.4.

The following objects have been modified in this release:
starPhyPortId

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 17.4.

The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 17.4

This section provides information on SNMP MIB alarm changes in release 17.4.

**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 17.4.

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 17.4.

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 17.4.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 17.4

This section provides information on SNMP MIB conformance changes in release 17.4.

**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 17.4.

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 17.4.

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 17.4.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 17.3

This section provides information on SNMP MIB object changes in release 17.3.

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 17.3.

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 17.3.

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 17.3.

The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 17.3

This section provides information on SNMP MIB alarm changes in release 17.3.

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 17.3.

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 17.3.

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 17.3.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 17.3

This section provides information on SNMP MIB conformance changes in release 17.3.

⚠️ 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 17.3. 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 17.3. 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 17.3. The following units of conformance have been deprecated in this release:

None in this release.
SNMP Command Changes for 17.3

CSCur13393 - Cisco ASR5000 SAE-GW High CPU Utilisation Vulnerability

Command Changes

```
snmp runtime-debug
```

This command enables or disables runtime SNMP debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.

This command also supports optional DEBUGMSG MIB tokens that represent textual MIB files that are to be found and parsed. The list of supported tokens is limited to those that appear in the CLI.

```
configure

snmp runtime-debug [ debug-tokens token_id token_id...token_id ]

no snmp runtime-debug
```

Notes:

- **no**: Disables SNMP runtime debugging.
- **[ debug-tokens token_id token_id...token_id ]**

   Enables DEBUGMSG tokens from the list of supported tokens appearing below. Multiple token IDs can be specified.

   - `agentx` – `agentx(12)` token
   - `disman` – `disman(11)` token
   - `dumpf` – `dumpf(13)` token
   - `dumpv` – `dumpv` token
   - `init_mib` – `init_mib(14)` token
   - `mib_init` – `mib_init(1)` token
   - `parse-file` – `parse-file(2)` token
   - `parse-mibs` – `parse-mibs(3)` token
   - `read_config` – `read_config(4)` token
   - `snmp` – `snmp(5)` token
   - `snmpd` – `snmpd(6)` token
   - `snmprapd` – `snmprapd(7)` token
   - `transport` – `transport(9)` token
- **trap** – trap(8) token
- **usm** – usm(10) token

The numbers appearing in parentheses above will appear in the output of the `show snmp server` command for “Runtime Debug Token.”
SNMP MIB Object Changes for 17.2

This section provides information on SNMP MIB object changes in release 17.2.

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 17.2.
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 17.2.
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 17.2.
The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 17.2

This section provides information on SNMP MIB alarm changes in release 17.2.

**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 17.2.

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 17.2.

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 17.2.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 17.2

This section provides information on SNMP MIB conformance changes in release 17.2.

**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 17.2.

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 17.2.

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 17.2.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 17.1

This section provides information on SNMP MIB object changes in release 17.1.

**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 17.1.

The following objects are new in this release:

- starGTPCRLFSessMgrInst
- starGTPCRLFVVPNName
- starGTPCRLFVPNId
- starGTPCRLFContextName
- starGTPCRLFCurrAppTPS
- starGTPCRLFCurrAppDelayTol
- starBGPPeerIpv6Address
- starMMEEMBMSServiceVpnName
- starMMEEMBMSServiceServName

### Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 17.1.

The following objects have been modified in this release:

- starCardOperState
- starServiceType
- starSRPSwitchReason

### Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 17.1.

The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes for 17.1

This section provides information on SNMP MIB alarm changes in release 17.1.

**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 17.1.

The following alarms are new in this release:

- starGILANServiceStart
- starGILANServiceStop
- starGTPCRLFOverThreshold
- starGTPCRLFOverLimit
- starGTPCRLFOverThresholdClear
- starGTPCRLFOverLimitClear
- starS102ServiceStart
- starS102ServiceStop
- starBGPPeerSessionIPv6Up
- starBGPPeerSessionIPv6Down
- starMMEEMBMSServiceStart
- starMMEEMBMSServiceStop
- starMCEAssocDown
- starMCEAssocUp

### Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 17.1.

The following alarms have been modified in this release:

- starIuBcTcpConnDown
- starIuBcTcpConnUp

### Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 17.1.
The following alarms have been deprecated in this release:
None in this release.
SNMP MIB Conformance Changes for 17.1

This section provides information on SNMP MIB conformance changes in release 17.1.

**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 17.1.

The following units of conformance are new in this release:

- starBGPPeerSessionIPv6Up
- starBGPPeerSessionIPv6Down
- starMMEEMBMSServiceStart
- starMMEEMBMSServiceStop
- starMCEAssocDown
- starMCEAssocUp
- starGILANServiceStart
- starGILANServiceStop

### Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 17.1.

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 17.1.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 17.0

This section provides information on SNMP MIB object changes in release 17.0.

**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 17.0.

The following objects are new in this release:

- starPhyPortId

### Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 17.0.

The following objects have been modified in this release:

- StarentCardType
- starChassisType

### Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 17.0.

The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes for 17.0

This section provides information on SNMP MIB alarm changes in release 17.0.

**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 17.0.

The following alarms are new in this release:

- starThreshNATPktDrop
- starThreshClearNATPktDrop
- starBFDSessUp
- starBFDSessDown
- starSRPSwitchoverOccured

### Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 17.0.

The following alarms have been modified in this release:

- starChassisCrashListFull

### Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 17.0.

The following alarms have been deprecated in this release:

- starThreshTpoRtoTimeout
- starThreshClearTpoRtoTimeout
- starThreshTpoDnsFailure
- starThreshClearTpoDnsFailure
- starThreshTpoLowCompressionGain
- starThreshClearTpoLowCompressionGain
SNMP MIB Conformance Changes for 17.0

This section provides information on SNMP MIB conformance changes in release 17.0.

**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 17.0. The following units of conformance are new in this release:

- starHENBGWServiceTLRI
- starNpudriverECCError
- starBFDSessUp
- starBFDSessDown
- starThreshNATPktDrop
- starThreshClearNATPktDrop

### Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 17.0. 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 17.0. The following units of conformance have been deprecated in this release:

- starThreshTpoRtoTimeout
- starThreshClearTpoRtoTimeout
- starThreshTpoDnsFailure
- starThreshClearTpoDnsFailure
- starThreshTpoLowCompressionGain
- starThreshClearTpoLowCompressionGain
Chapter 24
System Changes in Release 17

This chapter identifies ASR 5x00 and virtual platform system-level features and functionality added to, modified for, or deprecated from StarOS 17 software releases.
System and Platform Enhancements for Release 17.3

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.

CSCuq86655 - TACACS Privilege Level needs to support Security Admin

**Applicable Products:** All products

**Associated CDETS ID:** CSCuu72188

**Feature Changes**

**StarOS Authorizations for TACACS+ Users**

**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.
ncli – Denies access to the StarOS CLI.
noecs – Denies access to ECS commands
noftp – Denies use of FTP.
ncli-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.

```
configure
  tacacs mode
    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.
System and Platform Enhancements for Release 17.2

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.

**CSCus04073 - Update support for Russian Timezones**

**Applicable Products:** All  
**Related CDETS ID:** CSCuq90891 - Russia timezone update

**Feature Changes**

**Correction for Russian Timezone 1**

When the new Russian timezones were supported in Release 17.1, “RTZ 1” also appeared in the europe-eastern (GMT+2:00) timezone. Russian Timezone 1 does not support Daylight Savings Time, as do the other countries in europe-eastern (GMT+2:00). Therefore, “(RTZ 1)” has been removed from the europe-eastern timezone.
System and Platform Enhancements for Release 17.1

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.

---

**CSCuo84268 - show egtpc peers needs to be added to the SSD**

**Applicable Products:** All

**Feature Changes**

Add show egtpc peers Command to List of SDR Strings

The `show egtpc peers` command has been added to the list of available Support Data Record (SDR) strings that can appear in the list of `show` commands output by the SSD (show support details).

**Performance Indicator Changes**

show support collection definitions

The following `show` command strings have been added to the output of this command:

- “show egtpc peers” [Enabled]
- “show egtpc statistics interface cgw-egress” [Enabled]
- “show egtpc statistics interface epdg-egress” [Enabled]

---

**CSCuq62755 - Force an SRP switchover when a configured EGQ Discard Threshold occurs**

**Applicable Products:** FSC, ASR 5500

**Feature Changes**

Force SRP Switchover When EGQ Threshold is Exceeded
An SRP (Service Redundancy Protocol) switchover of an FSC (Fabric Storage Card) now occurs when an EGQ threshold has been exceeded. The EGQ threshold is associated with the fabric chip set. This threshold can be set and observed via hidden StarOS commands.

**CSCuq88798 - Block SRP manual switchover to system with bad RAID**

**Applicable Products:** All products supporting ICSR

**Feature Changes**

**Block SRP Manual Switchover for Bad RAID**

**Previous Behavior:** A manually initiated SRP switchover to the backup ICSR chassis would occur even if the backup chassis had a bad RAID storage subsystem.

**New Behavior:** A manual SRP switchover will be blocked if the backup ICSR chassis has a bad RAID subsystem.

**CSCuq90891 - Russia timezone update**

**Applicable Products:** All

**Feature Changes**

**Addition of New Russian Timezones**

The following Russian timezones have been added to the list of those supported for the `clock timezone` command:

- Russia Zone 1 (RTZ 1) = GMT+2:00, Kaliningrad Standard Time, no daylight savings: europe-eastern (Kaliningrad)
- Russia Zone 2 (RTZ 2) = GMT+3:00, Russian Standard Time, no daylight savings: europe-moscow (Moscow, St. Petersburg, Volgograd)
- Russia Zone 3 (RTZ 3) = GMT+4:00, no daylight savings: europe-samara (Izhevsk, Samara)
- Russia Zone 4 (RTZ 4) = GMT+5:00, Ekaterinburg Standard Time, no daylight savings: asia-yekaterinburg (Ekateringburg)
- Russia Zone 5 (RTZ 5) = GMT+6:00, N. Central Asia Standard Time, no daylight savings: asia-omsk (Novosibirsk)
- Russia Zone 6 (RTZ 6) = GMT+7:00, North Asia Standard Time, no daylight savings: asia-krasnoyarsk (Krasnoyarsk)
- Russia Zone 7 (RTZ 7) = GMT+8:00, North Asia East Standard Time, no daylight savings: asia-irkutsk (Irkutsk)
- Russia Zone 8 (RTZ 8) = GMT+9:00, Yakutsk Standard Time, no daylight savings: asia-yakutsk (Yakutsk)
- Russia Zone 9 (RTZ 9) = GMT+10:00, no daylight savings (Vladivostok, Magadan): pacific-guam (Brisbane, Cairns, Sydney, Guam)
- Russia Zone 10 (RTZ 10) = GMT+11:00, no daylight savings (Chokurdakh): asia-magadan (Magadan)
- Russian Zone 11 (RTZ 11) = GMT+12:00, no daylight savings (Anadyr, Petropavlovsk-Kamchatsky): pacific-kwajalein (Kwajalei)

**Command Changes**

clock timezone

The timezone options for this command now include (RT n) indicators that designate Russian timezones.

- asia-irkutsk - (GMT+8:00) Irkutsk (RTZ 7)
- asia-krasnoyarsk - (GMT+7:00) Krasnoyarsk (RTZ 6)
- asia-omsk - (GMT+6:00) Novosibirsk (RTZ 5)
- asia-yakutsk - (GMT+9:00) Yakutsk (RTZ 8)
- asia-yekaterinburg - (GMT+5:00) Ekaterinburg (RTZ 4)
- europe-kaliningrad - (GMT+2:00) Kaliningrad (RTZ 1)
- europe-moscow - (GMT+3:00) Moscow, St. Petersburg, Volgograd (RTZ 2)
- europe-samara - (GMT+4:00) Izhevsk, Samara (RTZ 3)

configure

clock timezones zones

africa-johannesburg - (GMT+2:00) Johannesburg
africa-nairobi - (GMT+3:00) Nairobi
america-buenos-aires - (GMT-3:00) Buenos Aires
america-caracas - (GMT-4:30) Caraca
america-guatemala - (GMT-6:00) Guatemala
america-la_paz - (GMT-4:00) La Paz
america-lima - (GMT-5:00) Lima
america-puerto-rico - (GMT-4:00) Puerto Rico
america-sao-paulo - (GMT-3:00) Sao Paulo
america-tijuana - (GMT-8:00) Tijuua
america-venezuela - (GMT-4:30) Venezuela Standard Tim
asia-almaty - (GMT+6:00) Almaty
asia-azerbaijan - (GMT+4:00) Azerbaijan
asia-baghdad - (GMT+3:00) Baghdad, Kuwait, Nairobi, Riyadh, Moscow, Tehran (RTZ 2)
System Changes in Release 17

System and Platform Enhancements for Release 17.1

Asia:
- Bangkok (GMT+7:00) Bangkok (RTZ 6)
- Calcutta, Mumbai, New Delhi (GMT+5:30)
- Dhaka (GMT+6:00) Dhaka (RTZ 5)
- Hong Kong (GMT+8:00) Hong Kong
- Irkutsk (GMT+8:00) Irkutsk (RTZ 7)
- Kabul (GMT+4:30) Kabul
- Karachi (GMT+5:00) Karachi (RTZ 4)
- Kathmandu (GMT+5:45) Kathmandu
- Krasnoyarsk (GMT+7:00) Krasnoyarsk (RTZ 6)
- Kuwait (GMT+3:00) Kuwait
- Magadan (GMT+11:00) Magadan (RTZ 10)
- Abu Dhabi, UAE, Muscat, Tbilisi, Volgograd, Kabul (GMT+4:00) Muscat
- Novosibirsk (RTZ 5)
- Rango (GMT+6:30) Rango
- Riyadh (GMT+3:00) Riyadh
- Seoul (GMT+9:00) Seoul
- Tehran (GMT+3:30) Tehran
- Tokyo (GMT+9:00) Tokyo
- Yakutsk (GMT+9:00) Yakutsk (RTZ 8)
- Ekaterinburg (GMT+5:00) Ekaterinburg (RTZ)
- Azores (GMT-1:00) Azores
- Cape Verde Islands (GMT-1:00) Cape Verde Islands
- Southern Territory - Adelaide (GMT+9:30)
- Queensland - Brisbane, Cairns, Toowoomba, Townsville (GMT+10:00)
- Northern Territory - Alice Springs, Darwin, Uluru (GMT+9:30)
- Tasmania - Hobart, Launceston (GMT+10:00)
- Lord Howe Island (GMT+10:30)
- Victoria - Ballarat, Melbourne (GMT+10:00)
australia-perth   - (GMT+8:00) Perth
australia-sydney - (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
canada-newfoundland - (GMT-3:30) Newfoundland
canada-saskatchewan - (GMT-6:00) Saskatchewan
europe-central - (GMT+1:00) Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo, Prague
europe-dublin - (GMT+0:00) Dublin, Ireland
europe-eastern - (GMT+2:00) Athens, Helsinki, Istanbul, Jerusalem, Harare (RTZ 1)
europe-kaliningrad - (GMT+2:00) Kaliningrad (RTZ 1)
europe-london - (GMT+0:00) London, England
europe-moscow - (GMT+3:00) Moscow, St. Petersburg, Volgograd (RTZ 2)
europe-samara - (GMT+4:00) Izhevsk, Samara (RTZ 3)
europe-western - (GMT+0:00) Lisbon
mexico-central - (GMT-6:00) Central Mexico, Mexico City
mexico-mountain - (GMT-7:00) Mexico Mountain (S Baja, Nayarit, Sinaloa)
newzealand-auckland - (GMT+12:00) New Zealand - Auckland, Christchurch, Wellington
newzealand-chatham - (GMT+12:45) New Zealand - Chatham Island
nuku - (GMT+13:00) Nuku'alofa
pacific-fiji - (GMT+12:00) Wellington, Fiji, Marshall Islands
pacific-guam - (GMT+10:00) Brisbane, Cairns, Guam (RTZ 9)
pacific-kwajalein - (GMT+12:00) Kwajalei (RTZ 11)
pacific-norfolk - (GMT+11:30) Norfolk Island
pacific-samoa - (GMT+11:00) Samoa
us-alaska - (GMT-9:00) Alaska
us-arizona - (GMT-7:00) Arizona
us-central - (GMT-6:00) Chicago, Saint Louis
us-eastern - (GMT-5:00) Bogota, New York City
us-hawaii - (GMT-10:00) Hawaii
us-indiana - (GMT-6:00) Indiana
<table>
<thead>
<tr>
<th>Timezone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-mountain</td>
<td>(GMT-7:00) Cheyenne, Denver, Las Vegas</td>
</tr>
<tr>
<td>us-pacific</td>
<td>(GMT-8:00) San Francisco, LA, Seattle</td>
</tr>
</tbody>
</table>
System and Platform Enhancements for Release 17.0

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.

CSCtr45924 - root privileges for ftp-user, no restriction to specific ftp-directory

Applicable Products: All

Feature Changes

Restrict User Access to a Specified Root Directory

**Previous Behavior:** An admin user who has ftp/sftp access can access/modify any files under the /mnt/user/ directory. Access is granted on an “all-or-nothing” basis to the following directories: /flash, /cdrom, /hd-raid, /records, /usb1 and /usb2

**New Behavior:** If a customer has a user who needs read-only access to one of these directories or sub-directories, that user can now be assigned with a root directory with read-only or read-write privilege.

An administrator or configuration administrator can create a list of SFTP subsystems with a file directory and access privilege. When a local user is created, the administrator assigns an SFTP subsystem. If the user's authorization level is not security admin or admin, the user can only access the subsystem with read-only privilege. This directory is used as the user's root directory. The information is set as environmental variables passed to the openssh sftp-server.

Command Changes

```
subsystem sftp
```

This command has been modified to allow the assignment of an SFTP root directory and associated access privilege level.

```
configure
  context local
    server sshd
      subsystem sftp  [ name sftp_name root-dir pathname mode { read-only | readwrite } ]
```

Notes:
- `sftp_name` is an alphanumeric string that uniquely identifies this subsystem.
- `pathname` specifies the root directory to which SFTP files can be transferred. Options include:
  - `/hd-raid/records/cdr`
  - `/flash`

`local-user username`

This command has been modified to allow the association of an SFTP root directory for a specified username.

```
configure

  local-user username user_name authorization-level level ftp sftp-server sftp_name password password

exit
```

`administrator`

This command has been modified to allow the association of an SFTP root directory for a specified administrator.

This command has been modified to allow the assignment of an SFTP root directory and associated access privilege level.

```
configure

  context local

  administrator user_name password password ftp sftp-server sftp_name

exit
```

`config-administrator`

This command has been modified to allow the association of an SFTP root directory for a specified configuration administrator.

This command has been modified to allow the assignment of an SFTP root directory and associated access privilege level.

```
configure

  context local

  config-administrator user_name password password ftp sftp-server sftp_name

exit
```

**CSCtr55441 - VoLTE related ICSR optimization**

*Applicable Products: P-GW, S-GW, SAEGW*
Feature Changes

ICSR Framework Changes to Support VoLTE

Additional internal enhancements have been made in this release to support voice-grade redundancy for Voice over LTE (VoLTE) deployments. ICSR components have been internally optimized to ensure that failure recovery is accomplished within acceptable limits for VoLTE. The impact on the data path is high priority.

The table below cross-references the various CDETS IDs that have been addressed as part of this ICSR-VoLTE performance optimization.

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuf30336</td>
<td>fw-and-nat policy ID checkpointing to peer chassis</td>
<td>Supports backward compatibility for inline services.</td>
</tr>
<tr>
<td>CSCuh89843</td>
<td>SM PGW Performance: FC are 50% more in make/break call model</td>
<td>Eliminates redundant second timer for full checkpoint.</td>
</tr>
<tr>
<td>CSCui26809</td>
<td>SR:Stats to check the number of FC and Microcheckpoints</td>
<td>Adds statistics for how many times an archive is being sent or received, as well as checkpoint statistics. This data can be used for session recovery.</td>
</tr>
<tr>
<td>CSCui31912</td>
<td>MemoryOptimization: Move per-session chkpt information to instance level</td>
<td>Create infrastructure for sharing common Diameter peer information. See CSCum57444</td>
</tr>
<tr>
<td>CSCul28844</td>
<td>SR: Optimisation of Prioritisation of calls based on priority</td>
<td>Creates separate lists in aaamgr for VoLTE/Emergency calls. The array for each list points to a particular priority.</td>
</tr>
<tr>
<td>CSCul42657</td>
<td>Memory Fragmentation in Session Recovery code path</td>
<td>Minimizes frequent malloc and release cycles that result in memory fragmentation.</td>
</tr>
<tr>
<td>CSCul46207</td>
<td>VoLTE:Zero billing loss during switchover with &lt; than 3 sec data outage</td>
<td>Internal changes made to minimize zero billing loss during ICSR switchover.</td>
</tr>
<tr>
<td>CSCum17282</td>
<td>[17.0] VoLTE Retainability KPI</td>
<td>Provide counters, KPIs and corresponding bulkstats to measure VoLTE specific performance.</td>
</tr>
<tr>
<td>CSCum50114</td>
<td>Initiate Session Checkpoint upon Session Creation</td>
<td>An ICSR check point is sent immediately after an IMS PDN session is created to avoid checkpoint loss for sessions established within 60 seconds of an ICSR switchover.</td>
</tr>
<tr>
<td>CSCum57323</td>
<td>Messenger Bounce handling for flush complete message</td>
<td>Implements a callback mechanism to handle message bounces from vpnmgr.</td>
</tr>
<tr>
<td>CSCum57428</td>
<td>ICSR:Handling MC when FC is queued</td>
<td>When a full checkpoint is queued, a pending micro checkpoint is discarded.</td>
</tr>
<tr>
<td>CSCum57444</td>
<td>SR:Instance Level Checkpoint framework for recovery</td>
<td>Reduces the amount of information replicated by the SRP Call Recovery Record task.</td>
</tr>
</tbody>
</table>
System Changes in Release 17

System and Platform Enhancements for Release 17.0

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCum57521</td>
<td>Messenger Bounce handling for post switchover processing</td>
<td>Implements a callback mechanism to handle message bounces from vpnmgr.</td>
</tr>
<tr>
<td>CSCum96879</td>
<td>ICSR: Schedule FC for 1stFC not sent + invalid crf case for critical MC</td>
<td>Improves handling of critical micro checkpoints.</td>
</tr>
</tbody>
</table>

CSCum39930 - Pilot Packet to Multiple Destinations

Applicable Products: NAT

Feature Changes

Assign Pilot Packets to Multiple Destinations

Previous Behavior: Currently the ASR5000/ASR5500 sends Pilot Packet content to only a single IP destination

New Behavior: Make Pilot Packet content available to multiple applications, up to four destinations.

Customer Impact: Maintainability

Command Changes

pilot packet

Up to four destinations can be assigned via this command.

configure

    context context_name

    pilot-packet source-ip-address src-ip destination-ip-address dst-ipl destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

    pilot-packet source-ip-address src-ip destination-ip-address dst-ip2 destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

    pilot-packet source-ip-address src-ip destination-ip-address dst-ip3 destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

    pilot-packet source-ip-address src-ip destination-ip-address dst-ip4 destination-udp-port dst-udp-port [ dscp-marking dscp_value ]

    end

CSCum39932 - Pilot Packet Statistics Enhancement

Applicable Products: All products supporting the Pilot Packet feature
Feature Changes

Pilot Packet Statistics

Pilot Packet statistics are now available via new and modified CLI `show` commands, and system schema `bulkstats`.

Performance Indicator Changes

system Schema

The following statistics have been added to the system schema:

- nat-alloc-pilot-packet-sent
- nat-de-alloc-pilot-packet-sent
- non-nat-alloc-pilot-packet-sent
- non-nat-de-alloc-pilot-packet-sent

**show apn statistics**

The output of the `show apn statistics` command has been modified to include the following Pilot Packet statistics:

- APN Name
- NAT Alloc
- Nat De Alloc
- Non NAT Alloc
- Non NAT De Alloc
- Total Alloc
- Total De Alloc

**show pilot-packet statistics**

A new Exec mode `show pilot-packet statistics` command is available to display the following Pilot Packet statistics:

- VPN Name
- Server name
- NAT Alloc
- Nat De Alloc
- Non NAT Alloc
- Non NAT De Alloc
- Total Alloc
- Total De Alloc

**show session subsystem facility sessmgr**
The output of the `show session subsystem facility sessmgr` command has been modified to include the following Pilot Packet statistics:

- VPN Name
- Server name
- Total NAT Alloc Pilot-Packets Sent
- Total NAT De-alloc Pilot-Packets Sent
- Total Non NAT Alloc Pilot-Packets Sent
- 0 Total Non NAT De-alloc Pilot-Packets Sent
- Total Alloc Pilot-Packets Sent
- Total De-alloc Pilot-Packets Sent

**CSCum50058 - ICSR Stats Reporting through BulkStats**

**Applicable Products:** All products supporting ICSR

**Performance Indicator Changes**

**ICSR Schema**

The following statistics now appear in the `icsr` schema:

- switchover-number
- switchover-time
- switchover-reason
- switchover-duration
- total-num-act-calls-swo-time
- total-num-lost-calls-swo-time
- checkpoints-never-sent
- checkpoints-send-failed
- audit_number
- audit_chassis_state
- audit_start_time
- audit_duration
- audit_reason
- total_audit_active_sessions
- total_audit_new_sessions
- total_audit_stale_sessions
- total_audit_inactive_sessions
- total_sessmgr
- total_sessmgr_active_connected
- total_sessmgr_standby_connected
- total_sessmgr_pending_connected
- total_sess_crr_count
- total_sess_crr_pre_installed
- total_first_fc_during_critical_flush
- total-num-act-sessions-swo-time
- total-num-lost-sessions-swo-time
- volte-data-outage-start-time
- volte-data-outage-end-time
- non-volte-data-outage-start-time
- non-volte-data-outage-end-time
- critical-flush-duration
- volte-flush-duration
- non-volte-flush-duration
- total-num-checkpoint-fc-flush
- total-num-checkpoint-critical-mc-flush
- total-num-checkpoint-mc-flush
- total-num-checkpoint-volte-accounting-stat-flush
- total-num-checkpoint-non-volte-accounting-stat-flush
- total-num-first-fc-never-sent
- total-num-critical-fc-not-sent
- total-num-volte-accounting-stat-not-sent
- total-num-nonvolte-accounting-stat-not-sent
- internal-audit-duration
- total-num-fc-encode-failure
- total-num-mc-encode-failure

For detailed descriptions of these statistics, see the Statistics and Counters Reference.

**CSCum50087 - Configurable Subscriber State Management Audit Process-Phase2**

**Applicable Products:** All products that support ICSR
Feature Changes

Audit Scheduler

A new keyword has been added to the SRP Configuration mode audit command to allow an operator to schedule SRP statistical audits. The scheduler emulates cron job functionality.

Command Changes

**audit**

A cron keyword has been added to this command.

```
configure

context context_name

service-redundancy-protocol variable

audit cron [ daily hour hour_number minute minute_number ] [ day-of-month day_number ] [ month month_number ] [ week-of-day day_name ]

end
```

Notes:

- **daily hour hour_number minute minute_number** – configures the hour and minute of the day when the job will run. Specify hour_number as an integer from 0 to 23 and minute_number as an integer from 0 to 59.
- **day-of-month day_number** – configures the day of the month when the job will run. Specify day_number as an integer from 1 to 31.
- **month month_number** – configures the month of the year when the job will run. Specify month_number as an integer from 1 to 12.
- **week-of-day day_name** – configures the week day on which the job will run. Specify day_name as one of the following names: friday, monday, saturday, sunday, thursday, tuesday, or wednesday.

CSCum87749 - Configurable SRP Redundancy/AAA/Diameter Guard Time(r)

**Applicable Products:** All products that support ICSR

**Related CDETS ID:** CSCuj54855

Feature Changes

Configurable Guard Timers

**Previous Behavior:** SRP Redundancy Guard Time and SRP Redundancy Guard Timer are hard coded to 60 seconds.

**New Behavior:** Configurable timers have been introduced for AAA, Diameter and SRP redundancy.

**Customer Impact:** Interoperability
Command Changes

**guard-timer**

This new SRP Configuration mode command configures the redundancy-guard-period and monitor-damping-period for SRP service monitoring.

Use these guard timers to ensure that local failures, such as card reboots and task restarts, do not result in ICSR events which can be disruptive.

```conf
configure
  context context_name
    service-redundancy-protocol variable
      guard-timer { aaa-switchover-timers { damping-period seconds | guard-period seconds } | diameter-switchover-timers { damping-period seconds | guard-period seconds } | srp-redundancy-timers { aaa { damping-period seconds | guard-period seconds } | bgp { damping-period seconds | guard-period seconds } | diam { damping-period seconds | guard-period seconds } } }
end
```

Notes:

- **aaa-switchover-timers** – sets timers that prevent back-to-back ICSR switchovers due to an AAA failure (post ICSR switchover) while the network is still converging.
  - **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
  - **guard-period** – configures the local-failure-recovery network-convergence timer.

- **diameter-switchover-timers** – sets timers that prevent a back-to-back ICSR switchover due to a Diameter failure (post ICSR switchover) while the network is still converging.
  - **damping-period** – configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period.
  - **guard-period** – configures the local-failure-recovery network-convergence timer.

- **srp-redundancy-timers** – sets timers that prevent an ICSR switchover while the system is recovering from a local card-reboot/critical-task-restart failure.
  - **aaa** – local failure followed by AAA monitoring failure
  - **bgp** – local failure followed by BGP monitoring failure
  - **diam** – local failure followed by Diameter monitoring failure

### CSCum87759 - Configurable MinRtAdvInterval

**Applicable Products:** All products that support ICSR

**Related CDETS ID:** CSCum80398
Feature Changes

Configurable BGP Route Advertisement Interval for ICSR

**Previous Behavior:** By default, the MinRtAdvInterval was set for each peer with a value of 5 seconds for an iBGP peer and 30 seconds for an eBGP peer. An operator can use the `neighbor identifier advertisement-interval` command to globally change the default interval.

**New Behavior:** The BGP advertisement-interval can now be separately set for each address family. If configured, this value over-rides the peer's default advertisement-interval for that address-family only. BGP will send route update-message for each AFI/SAFI based on the advertisement-interval configured for that AFI/SAFI. If no AFI/SAFI advertisement-interval is configured, the peer-based default advertisement-interval is used.

**Customer Impact:** In ICSR configurations, this feature can be used to speed route advertisements and improve network convergence times.

Command Changes

```
timers bgp icsr-aggr-advertisement-interval
```

This new command is available in both the BGP Address-Family (VPNv4/VPNv6) Configuration and BGP Address-Family (VRF) Configuration modes

```
configure

    context context_name

    router bgp as_number

    address-family { ipv4 | ipv6 | vpnv4 | vpnv6 }

    timers bgp icsr-aggr-advertisement-interval seconds
```

Notes:
- `seconds` – sets the number of seconds as an integer from 0 to 30. Default: 0.

**CSCum87764 - Announcing Routes from Standby Chassis**

**Applicable Products:** All products supporting ICSR

**Related CDETS ID:** CSCuj54862

Feature Changes

Announcing BGP Routes from a Standby ICSR Chassis

A new SRP Configuration mode command enables advertising BGP routes from an ICSR chassis in standby state. This command and its keywords allow an operator to take advantage of faster network convergence accrued from deploying BGP Prefix Independent Convergence (PIC) in the Optical Transport Network Generation Next (OTNGN).

BGP PIC is intended to improve network convergence which will safely allow for setting aggressive ICSR failure detection timers.
Command Changes

advertise-routes-in-standby-state

This is new command that enables advertising of BGP routes form a standby ICSR chassis.

configure

context context_name

service-redundancy-protocol

   advertise-routes-in-standby-state [ hold-off-time hold-off-time ] [ reset-bfd-nbrs bfd-down-time ]

end

Notes:

- **hold-off-time** *hold-off-time* delays advertising the BGP routes until the timer expires. Specify *hold-off-time* in seconds as an integer from 1 to 300.
- After resetting BFD, **reset-bfd-nbrs** *bfd-down-time* keeps the BFD sessions down for the configured number of milliseconds to improve network convergence. Specify *bfd-down-time* as an integer from 50 to 120000.

CSCum87769 - Chassis to Chassis BFD Monitoring

**Applicable Products:** All products supporting ICSR

Feature Changes

Chassis-to-Chassis BFD Monitoring

This feature supports the use of BFD as a ICSR chassis failure mechanism that permits more aggressive detection time than Service Redundancy Protocol (SRP). This feature also adds the ability to configure static multihop BFD routes.

Command Changes

bfd-mon-ignore-dead-interval

This new SRP Configuration mode command causes the standby ICSR chassis to ignore the dead interval and remain in the standby state until all the BFD chassis-to-chassis monitors fail.

Enable this feature in association with BFD chassis-to-chassis monitoring to support more aggressive ICSR failure detection times.

configure

context context_name

   service-redundancy-protocol variable
bfd-mon-ignore-dead-interval

guard-timer

For a complete description of this command, see CSCum87749 - MFL 2451: Configurable SRP Redundancy/AAA/Diameter Guard Timer.

ip route

A **fall-over bfd multihop mhsess_name** keyword has been added to this Context Configuration mode command. This keyword enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure.

configure

    context context_name

    ip route { ip_address/ip_mask | ip_address ip_mask } { gateway_ip_address | next-hop next_hop_ip_address | point-to-point | tunnel } egress_intrfc_name [ cost cost ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] [ vrf vrf_name [ cost value ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] ] +

eend

The **ip route** command now also allows you to add a static multihop BFD route.

    ip route static multihop bfd mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr

Notes:

- **mhbfd_sess_name** specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.
- **local_endpt_ipaddr** specifies the local endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **remote_endpt_ipaddr** specifies the remote endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** SNMP traps are generated when BFD sessions go up and down (BFDsUp and BFDsDown).

ipv6 route

A **fall-over bfd multihop mhsess_name** keyword has been added to this Context Configuration mode command. This keyword enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure.

configure

    context context_name
ipv6 route ipv6_address/prefix_length { interface name | next-hop ipv6_address interface name } [ cost cost ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] [ vrf vrf_name [ cost value ] [ fall-over bfd multihop mhsess_name ] [ precedence precedence ] ]

end

The ipv6 route command now also allows you to add a static multihop BFD route.

ipv6 route static multihop bfd mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr

Notes:
• mhbfd_sess_name specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.
• local_endpt_ipv6addr specifies the local endpoint address in IPv6 colon-separated-hexadecimal notation.
• remote_endpt_ipv6addr specifies the remote endpoint address in IPv6 colon-separated-hexadecimal notation.

Important: SNMP traps are generated when BFD sessions go up and down (BFDSessUp and BFDSessDown).

bfd interval

The range of accepted values for two keywords have been extended for this Ethernet Interface Configuration mode command.

configure

context context_name

interface interface_name broadcast

bfd interval interval_num min_rx milliseconds multiplier value

end

Notes:
• For release 17.0 onwards, interval_num is an integer from 50 through 10000. (Default 50)
• For release 17.0 onwards, milliseconds is an integer from 50 through 10000. (Default 50)

CSCum87774 - MFL 1858: KPI to Increase the 32K BGP routes per context to 64K (MPN)

Applicable Products: All
Related CDETS ID: CSCup90954
Feature Changes

BGP Routes per Context KPI Limit Increased to 64000

**Previous Behavior:** The BGP Routes per Context KPI supported 32000 routes. This KPI applies to the total number of routes that can be supported in a given context. A BGP route can be:

- A pool route
- A static route
- An interface or loopback IP route (for example, a VLAN interface IP address or a HA service Loopback IP)
- A learned or imported route from a BGP peer (primary and secondary where the same route is learned from two different peers)
- A NEMO route learned from Mobile Routers

The maximum number of supported routes per system is dictated by KPIs (max # routes in forwarding table and max # NEMO prefixes or routes per system).

**New Behavior:** The BGP Routes per Context KPI is increased to 64000 routes.

CSCum87782 - Increase the number of configurable SSH hosts and keys in ctxt

**Applicable Products:** All

Feature Changes

Increase Number of Configurable SSH Hosts and Keys to 50

**Previous Behavior:** The maximum number of configurable SSH hosts and keys via the Context Configuration mode `ssh` command was 10.

**New Behavior:** The maximum number of configurable SSH hosts and keys via the Context Configuration mode `ssh` command is now 50.

**Customer Impact:** Interoperability

CSCum87789 - Trap for failed Diameter or Radius peer success

**Applicable Products:** XGW, P-GW, HA and ePDG

Feature Changes

Generate SNMP Trap for Failed Diameter or RADIUS Peer Success

**Previous Behavior:** There is no indication provided by the system when a Diameter or RADIUS peer fails to connect with endpoints upon ICSR failover.

**New Behavior:** An SRP trap (SRPSwitchoverOccured) is now generated with the following possible Switchover Reasons:

- AAA failure
- BFD Failure
- BGP Failure
- Diameter Failure
- Manual switchover
- Unknown event
- Active - SRP connectivity loss

**Customer Impact:** Interoperability

**CSCum98092 - MS-to-MS traffic for Ipsec**

*Applicable Products:* PGW, GGSN

**Feature Changes**

**Local Routing of IPSec Packets**

**Previous Behavior:** When IPSec is used for corporate customers and the ACL includes a destination “any”, all packets are sent to the remote IPSec peer via the tunnel, even when a subscriber tries to reach another subscriber in the same IP pool.

**New Behavior:** When packets are sent from one MS to another MS in the same pool or a different pool in the same group, the packets are not sent into the IPSec tunnel and reach the other MS by routing inside the system.

**Customer Impact:** Capability/Functionality

This enhancement supports the following functionality:

- This feature is only supported with a Match Address ACL.
- Cut through is an Always On feature at chassis level.
- MS-to-MS communication can be blocked by a Match Address ACL.
- UEs connected to the same APN can reach each other on the IP level.
- UEs from the same subnet connected to that APN are seen as directly connected network.
- UEs from different subnets, subnet ranges or pools but belonging to the same APN have local IP connectivity.
- MS-to-MS communication is possible regardless of IP allocation type (static, dynamic, AAA, DHCP).
- Traffic from one UE to another is subject to ACL (firewall) and ECSv2 DPI.
- MS-to-MS traffic can be steered out of the GGSN towards the Internet side to allow the corporate side/endpoint to control UE-to-UE traffic.
- All of the above functionality is applicable to APNs with VRF, as well as non-VRF APNs.
- Billing accurately reports volumes/time for such subscribers.
- Gx, Gy functionality is not affected by local MS-to-MS communication.
- NAT is not be performed for MS-to-MS communication within the same system.
- Session recovery is supported.
- ICSR is supported.

**CSCun88666 - [ePDG] require ipsec-large support**

**Applicable Products:** ePDG, PDIF  
**Related CDETS IDs:** CSCug87420, CSCun65041

**Feature Changes**

**Boost Crypto Performance**

A new command boosts IPSec crypto performance by enabling the resource manager (RM) task to assign additional IPSec managers to packet processing cards that have sufficient processing capacity.

**Command Changes**

`require ipsec-large`

This new Global Configuration mode command enables a boost in crypto performance.

```
configure
    require ipsec-large
end
```

**Performance Indicator Changes**

**show configuration**

The output of this command will include “require ipsec-large” when this feature is enabled.

**CSCuo55792 - new switchover reason as dual active + dual standby and bulkstat support**

**Applicable Products:** All products that support ICSR

**Feature Changes**

**New Switchover Reasons**

The `show srp call-loss statistics` command has been enhanced to include new switchover reasons. Switchover reason “Unknown” has been replaced with “Not Defined”. Corresponding changes have also been incorporated in the ICSR bulkstats schema.
Performance Indicator Changes

ICSR Schema

For the complete list of ICSR statistics, Refer to Ref - CSCum50058

show srp call-loss statistics

The following switchover reasons may now appear in the output of this command:

- Manual Switchover
- AAA failure
- BFD failure
- BGP failure
- Chassis-Chassis BFD failure
- Dead Timer Expiry
- Diameter failure
- Dual Active
- Dual Standby
- HSRP switchover (WSG/SecGW service only)
- Not Defined (replaces “Unknown”)

CSCuo84001 - [ares] Need User configurable command to monitor FAP Egress drops

Applicable Products: All (ASR 5500 only)

Feature Changes

Event Log Entry Generation for Dropped Egress FAP Traffic Packets

A new command enables or disables the generation of a syslog event message when the number of egress Fabric Access Processor (FAP) packet drops exceeds a set threshold within a window of time on an ASR 5500.

Command Changes

fabric egress drop-threshold

This new Global Configuration mode command specifies the maximum number of egress FAP traffic packets that can be dropped within a window of time before a syslog event message is generated.

configure

    fabric egress drop-threshold enable count number interval-secs seconds
end

Notes:

- **count number** specifies the maximum number of egress traffic packets that can be dropped before a syslog event message is generated. The count is specified as an integer from 10 through 5000.
- **interval-secs seconds** specifies the time interval (window) within which the maximum egress packet drop count can be exceeded. The interval is specified in seconds as an integer from 30 through 600.
- When the threshold is exceeded, the syslog event message is generated once, until the condition clears. Only then will it be generated again.
- By default, this feature is disabled.

**CSCuo84086 - IPv6 support for NTP**

Applicable Products: All
Related CDETS ID: CSCuq49149

**Feature Changes**

IPv6 Support for NTP Servers

**Previous Behavior:** An NTP server at an IPv6 address could not be reached.
**New Behavior:** An NTP server at an IPv6 address can now be reached.

**CSCuo84096 - IPv6 support for SNMP**

Applicable Products: All

**Feature Changes**

SNMP Support for IPv6

**Previous Behavior:** SNMP did not support IPv6 addressing.
**New Behavior:** SNMP now supports IPv6 addressing.

**CSCuo90200 - Show configuration do not display Checkpoint Session duration**

Applicable Products: All products that support ICSR

**Feature Changes**

Handling of IMS and non-IMS Checkpoint Durations
**Previous Behavior:** Checkpoint durations were not properly handled for IMS and non-IMS sessions. This caused the output of the `show configuration` command not to display the correct checkpoint session durations for IMS and non-IMS sessions.

**New Behavior:** Two new keywords have been added to the `checkpoint session duration` command in an SRP context. The keywords specify separate checkpoint durations for IMS and non-IMS sessions.

**Customer Impact:** Reliability

### Command Changes

`checkpoint session duration`

Two new mandatory keywords – `ims-session` and `non-ims-session` – have been added to the SRP configuration mode `checkpoint session duration` command.

```configure
context context_name
  service-redundancy-protocol
    checkpoint session duration { ims-session | non-ims-session } duration
end
```

Notes:
- `context_name` is the name of the SRP context.

### CSCup90954 - BGP: VRF CLI 'ip maximum-routes' threshold of 32K should be 64K (NEMO)

**Applicable Products:** Any product using VRFs  
**Related CDETS ID:** CSCum87774

### Feature Changes

**Raise IP Maximum Routes Threshold in a VRF to 64K**

**Previous Behavior:** The maximum number of routes in a VRF that could be set via the `ip maximum-routes` command was 32768.

**New Behavior:** The maximum number of routes in a VRF that can be set via the `ip maximum-routes` command has been increased to 65536.

### Command Changes

`ip maximum-routes`

This IP VRF Configuration mode command has been modified to increase its `max_routes` value to 65536.
configure

    context  context_name
    ip  vrf  vrf_name
    ip  maximum-routes  max_routes
end

CSCup91637 - FTP server with ipv6 is not working

Applicable Products: All

Feature Changes

Support for IPv6 FTP

Previous Behavior: FTP was supported for IPv4 only.
New Behavior: FTP is now supported for IPv4 and IPv6.
Customer Impact: Interoperability

CSCuq49149 - NTP service does not work without ipv4 address for SPIO int

Applicable Products: All (ASR 5000)

Feature Changes

NTP Service No Longer Needs IPv4 Address for Any SPIO Interface

Previous Behavior: The show ntp command did not work when only an IPv6 address was present on the SPIO interface.
New Behavior: During startup the localhost IP address is now added as both 127.0.0.1 and ::1. Based on the configured IP address localhost will be treated as IPv4 or IPv6.

CSCzn41068 - ICSR support for L2TP on GGSN/PGW

Applicable Products: All products that support ICSR
Related CDETS IDs: CSCuj82077, CSCuo45472

Feature Changes

L2TP Support for L2TP

L2TP Access Concentrator (LAC) functionality for ICSR is supported by the following services:
• eGTP – enhanced GPRS Tunneling Protocol
• GGSN – Gateway GPRS Support Node
• SAEGW – System Architecture Evolution Gateway

L2TP Access Concentrator (LAC) functionality for ICSR is not supported by the following services:
• HA – Home Agent
• PMIP - P-GW – Proxy Mobile IP - Packet Data Network Gateway

L2TP Network Server (LNS) functionality for ICSR is not supported by any services.

Important: There are no behavior changes associated with ICSR support for L2TP functionality.

Important: ICSR support for LAC requires a separate LAC license, as well as an Inter-Chassis Session Recovery license.
Chapter 25
VPC-DI Changes in Release 17

This chapter identifies features and functionality added to, modified for, or deprecated from VPC-DI in StarOS 17 software releases.
VPC-DI Feature Changes for 17.1

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.

---

**CSCup50172 - DI: SF cards with ports - should be able to migrate from fewer ports**

*Applicable Products:* VPC-DI

**Feature Changes**

**Port Migrations Between SFs**

**Previous Behavior:** Migration between SF VMs with different port configurations was not allowed.

**New Behavior:** Migration between SF VMs with different port configurations is now allowed.

**CSCup57478 - DI should use hypervisor provided MAC addresses for DI network**

*Applicable Products:* VPC-DI

**Feature Changes**

**QvPC-DI to use Hypervisor MAC Addresses for DI Network**

VPC-DI now uses MAC addresses obtained from the hypervisor for the VPC-DI network.

**CSCuq12270 - Add support for multiple IP interfaces in the same IP subnet**

*Applicable Products:* VPC-DI
Feature Changes

Multiple IP Interfaces in the Same IP Subnet

**Previous Behavior:** IP interfaces must belong to different subnets.

**New Behavior:** IP interfaces can now belong to the same subnet.

**Important:** OSPF is not supported for multiple interfaces on the same subnet.

CSCuq13578 - Support for Intel 82599 VF (SRIOV)

**Applicable Products:** VPC-DI

Feature Changes

Starting QvPC-DI VMs with Insufficient Memory

vzulkows

**Previous Behavior:** All VPC-DI VMs were treated the same.

**New Behavior:** VPC-DI VMs with memory less than 48GB are treated as reduced capacity (Medium Model) systems.

CSCuq13618 - Support for up to 32 ECMP members

**Applicable Products:** VPC-DI

Feature Changes

Support for 32 ECMP Paths

Up to 32 ECMP paths are supported in this release.

CSCuq13710 - openstack cfgdisk metadata for DI Slot number

**Applicable Products:** VPC-DI

Feature Changes

OpenStack Configuration Metadata

OpenStack cfgdisk metadata now includes a param.cfg file to include anything that is in the param.cfg on the vHDD. This would include slot number, card type (if needed), etc.
CSCuq95642 - [QvPC-DI] unable to start GTPUMgr, insufficient unserved memory

Applicable Products: VPC-DI

Feature Changes

Starting QvPC-DI VMs with Insufficient Memory

vzulkows

Previous Behavior: All VPC-DI VMs were treated the same.

New Behavior: VPC-DI VMs with memory less than 48GB are treated as reduced capacity (Medium Model) systems.

CSCuq97176 - QvPC-DI Network mapping and A-B bonding support

Applicable Products: VPC-DI

Feature Changes

Network Mapping of NICs for non-UCS Hardware

VPC-DI now supports a way to specify network topology in a param.cfg file that specifies NIC operating parameters including:

- Designation of DI-Network or service ports
- VLAN for DI-Network
- Configuration applies to single NIC or a pair of NICs in A-B redundancy mode

A-B network redundancy (bonding driver) is supported for non-UCS hardware. This feature allows for setup of redundant connections to the physical L2 switch.

The following are sample bonding configurations:

qvpc-di:card3-cpu0# cat /cdrom1/staros_param.cfg

CARDSLOT=3

ETH0_MAC=00:05:47:00:02:01
ETH1_MAC=00:50:56:87:d7:1d
ETH2_MAC=00:50:56:87:a2:52

BOND0_MAP=ETH0
BOND0_PRIMARY=ETH0
BOND0_REVERSION_POLICY=0
BOND0_LINK_DETECT=0
BOND0_MII_POLL=100

BOND1_MAP=ETH1,ETH2
BOND1_PRIMARY=ETH1
BOND1_REVERSION_POLICY=0
BOND1_LINK_DETECT=0
BOND1_MII_POLL=100

**CSCuq97178 - Should be able to boot SF locally even with passthrough NICs**

*Applicable Products: VPC-DI*

**Feature Changes**

**Passthrough Booting Locally**

For a CF, if the network interface is configured and a slot number is available, the CF will try to boot from the other CF first. It tries boots based on its boot.sys if the CF fails to boot from the other CF (current behavior).

If the network interface is not configured or a slot number is not available, the CF will boot based on its boot.sys without trying to boot from the other CF. This is the scenario for passthrough NIC.

For an SF, if the network interface is configured and a slot number is available, the SF will boot from either of the CFs (current behavior)

If the network interface is not configured or a slot number is unavailable, the SF will boot from its local partition 1 to load “/boot1/staros.bin”. This is the scenario for passthrough NIC.

**CSCur44411 - DI: rc should reboot if masterslot can't be determined**

*Applicable Products: VPC-DI*

**Feature Changes**

**SF Reboot Timeout When CF Cannot Be Detected**

An SF will reboot itself after a 3-minute timeout period if it cannot detect a CF in the master slot.
VPC-DI Feature Changes for 17.0

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.

---

**CSCui20002 - SSI knpusim**

**Feature Changes**

**knpusim Packet Handler**

**Previous Behavior:** All packets on the VPC-SI virtual platform flowed through the npusim task which simulates hardware-based NPU functionality.

**New Behavior:** To improve packet handling performance, the npusim code has been moved into the StarOS-kernel. The knpusim task is used for all ingress and egress packets except for IPSec and IP fragments which will still be routed to the slower npusim path.

**Customer Impact:** Improved performance

**CSCui20092 - SSI support for virtio/vmxnet3 vNIC types**

**Feature Changes**

**Support for virtio and vmxnet3 vNICs**

In this release the supported vNIC options include:

- VMware – para-virtualized vmxnet3
- KVM – para-virtualized virtio
  - Multiqueue virtio-net is supported.
CSCup57481 - CFE support for passthrough NIC types

Feature Changes

Support for Passthrough vNICs

Changes to VPC-DI CFE (Common Firmware Environment) now support the following vNIC types on Cisco UCS servers/blade running SF (Service Function) vital machines:

- VMware – ESX eNIC
- VMware – ixgbe (Linux base driver for 10 Gigabit Ethernet controllers)

The above passthrough vNICs are supported on Cisco UCS platforms equipped with Cisco Virtual Interface Card (VIC) 1225/1240/1280.

CSCuq13550 - ‘show hardware’ should show NIC multi-q support, hugepage, etc...

Feature Changes

Enhancements to show hardware Command

The output of the `show hardware` command now displays additional information for vNIC interfaces.

Performance Indicator Changes

`show hardware`

The output of this command now displays additional information about vNIC interfaces obtained from the hypervisor, including:

- MAC addresses, vNIC types
- Rx and Tx queues
- NODE-ID

CSCuq13580 - SI/DI installer should have option to leave VMs running

Feature Changes

Leave VMs Running After Hypervisor Installation

VPC-SI installer now includes -R option to leave virtual machine (VM) running after installation.
CSCuq13684 - SI/DI install script should have option to package disk images

Feature Changes

Package Disk Images for Installation

VPC-SI installer now includes -q option to package disk images.
This chapter identifies features and functionality added to, modified for, or deprecated from VPC-SI StarOS 17 software releases.
VPC-SI Feature Changes for 17.0

This section identifies all of the VPC-SI enhancements included in this release:

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

---

**CSCui20002 - SSI knpusim**

**Feature Changes**

**knpusim Packet Handler**

**Previous Behavior:** All packets on the VPC-SI virtual platform flowed through the npusim task which simulates hardware-based NPU functionality.

**New Behavior:** To improve packet handling performance, the npusim code has been moved into the StarOS-kernel. The knpusim task is used for all ingress and egress packets except for IPSec and IP fragments which will still be routed to the slower npusim path.

**Customer Impact:** Improved performance

---

**CSCui20092 - SSI support for virtio/vmxnet3 vNIC types**

**Feature Changes**

**Support for virtio and vmxnet3 vNICs**

In this release the supported vNIC options include:

- VMware – para-virtualized vmxnet3
- KVM – para-virtualized virtio
  - Multiqueue virtio-net is supported.
CSCuq13550 - ‘show hardware’ should show NIC multi-q support, hugepage, etc...

Feature Changes

Enhancements to show hardware Command

The output of the `show hardware` command now displays additional information for vNIC interfaces.

Performance Indicator Changes

show hardware

The output of this command now displays additional information about vNIC interfaces obtained from the hypervisor, including:

- MAC addresses, vNIC types
- Rx and Tx queues
- NODE-ID

CSCuq13580 - SI/DI installer should have option to leave VMs running

Feature Changes

Leave VMs Running After Hypervisor Installation

VPC-SI installer now includes -R option to leave virtual machine (VM) running after installation.

CSCuq13684 - SI/DI install script should have option to package disk images

Feature Changes

Package Disk Images for Installation

VPC-SI installer now includes -q option to package disk images.