Release Change Reference, StarOS Release 16
Last Updated June 23, 2015

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

About this Guide ................................................................................................................. xxxiii
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 16 ................................................................................................. 39
AAA Enhancements for 16.4 ................................................................................................. 40
CSCus24059 - New dynamic dict for Customer ................................................................. 40
  Feature Changes .................................................................................................................. 40
CSCus33524 - New S6b Dict for Customer to support GTPv2_SUPPORTED in MIP6-Feature-Vector
  Feature Changes .................................................................................................................. 40
CSCus59440 - Diameter : S6b Origin-Host AVP truncation ................................................. 41
  Feature Changes .................................................................................................................. 41
  Command Changes ............................................................................................................. 41
AAA Enhancements for 16.3 ................................................................................................. 42
CSCup75566 - Add CC-Group AVP in Gx Dictionary for Customer ........................................ 42
  Feature Changes .................................................................................................................. 42
CSCuq06614 - Radius AVP SN-Rad-APN-Name to be added in custom67 ......................... 42
  Feature Changes .................................................................................................................. 42
AAA Enhancements for 16.2 ................................................................................................. 43
CSCui47290 - Display issue in 15.0 for cli show ims-authorization service name gx ............ 43
  Feature Changes .................................................................................................................. 43
CSCui07715 - ASR5000 sends CCR-T before CCA-U arrived for CCR-U ....................... 43
  Feature Changes .................................................................................................................. 43
CSCup09827 - Bulkstats counter not present for CCR-Event Retry .................................... 44
  Performance Indicator Changes ......................................................................................... 44
CSCup22833 - [GGSN] SM not sending updated GBR to IMSA after QoS negotiation ....... 44
  Feature Changes .................................................................................................................. 44
CSCup49621 - Rf-Gy Synchronization Enhancements .......................................................... 44
  Feature Changes .................................................................................................................. 44
CSCup77319 - PGW: missing Framed-IPv6-Prefix/Interface-Id in RADIUS-acct custom15 45
  Feature Changes .................................................................................................................. 45
CSCuo3247 - update-dictionary-avps: Event Triggers by default w/o PCRF installation .... 45
  Feature Changes .................................................................................................................. 45
  Command Changes ............................................................................................................. 45
CSCuo08909 - Charging QoS MBR values when QCI not included in QoS-Info from PCRF 46
  Feature Changes .................................................................................................................. 46
AAA Enhancements for 16.1 ................................................................................................. 47
CSCug72343 - Assumed Positive Stats in Bulkstats for the DIAMETER Interfaces ............... 47
  Performance Indicator Changes ......................................................................................... 47
CSCuh11035 - PDSN/PCEF Supports CCR format on Gx interface .................................... 47
  Feature Changes .................................................................................................................. 47
CSCuh51213 - Always send Charging-Rule-Report AVP in RAA on Gx ............................. 47

Release Change Reference, StarOS Release 16
<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCui47290 - Display issue in 15.0 for cli show ims-authorization service name gx</td>
<td>48</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>48</td>
</tr>
<tr>
<td>CSCui59026 - Enhancements in ASR5x00 Timer Implementation - Gy Changes</td>
<td>48</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>48</td>
</tr>
<tr>
<td>Command Changes</td>
<td>49</td>
</tr>
<tr>
<td>CSCui10006 - PGW not sending CCR-E to the OCS on receiving Trigger Type Grouped AVP</td>
<td>49</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>49</td>
</tr>
<tr>
<td>CSCui53306 - Adding a new AVP on Gx interface - Service group QoS</td>
<td>50</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>50</td>
</tr>
<tr>
<td>CSCui61923 - Extra CCR-E message being sent to the OCS</td>
<td>50</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>50</td>
</tr>
<tr>
<td>CSCui07715 - ASR5000 sends CCR-T before CCA-U arrived for CCR-U</td>
<td>50</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>50</td>
</tr>
<tr>
<td>CSCum96361 - No CCR-T when diameter failover from primary to secondary diameter host</td>
<td>51</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>51</td>
</tr>
<tr>
<td>CSCun52379 - Redirection when RC4012 or RC4010 at MSCC level with FUI redirect</td>
<td>51</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>51</td>
</tr>
<tr>
<td>CSCun85201 - Request new Vendor-Id for Race Condition</td>
<td>51</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>51</td>
</tr>
<tr>
<td>CSCuo97456 - CC-Service-Specific-Units Avp getting update for a dynamic rule</td>
<td>51</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>51</td>
</tr>
<tr>
<td>CSCup09827 - Bulkstats counter not present for CCR-Event Retry</td>
<td>52</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>52</td>
</tr>
<tr>
<td>CSCup49621 - Rf-Gy Synchronization Enhancements</td>
<td>52</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>52</td>
</tr>
<tr>
<td>CSCup9675 - gtp-cp push-to-active feature password shown in plain text</td>
<td>52</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>53</td>
</tr>
<tr>
<td>Command Changes</td>
<td>53</td>
</tr>
<tr>
<td>CSCup77319 - PGW: missing Framed-IPv6-Prefix/Interface-Id in RADIUS-acct custom15</td>
<td>53</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>53</td>
</tr>
<tr>
<td>AAA Enhancements for 16.0</td>
<td>54</td>
</tr>
<tr>
<td>CSCty15753 - Suppress USU from CCR for FUI/REDIRECT</td>
<td>54</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>54</td>
</tr>
<tr>
<td>Command Changes</td>
<td>54</td>
</tr>
<tr>
<td>CSCty34193, CSCtz85672, CSCun86025 - Rf-Gy Synchronization Enhancements</td>
<td>55</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>55</td>
</tr>
<tr>
<td>Command Changes</td>
<td>55</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>56</td>
</tr>
<tr>
<td>CSCty98259 - OCS selection using field name Charging Characteristic</td>
<td>57</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>57</td>
</tr>
<tr>
<td>Command Changes</td>
<td>57</td>
</tr>
<tr>
<td>CSCtz62801, CSCtw75856, CSCty34184 - Processing Diameter Gx Messages in the order in which they were received</td>
<td>58</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>58</td>
</tr>
<tr>
<td>Command Changes</td>
<td>59</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>59</td>
</tr>
<tr>
<td>CSCua25104 - Segmentation fault PC: [094f04e8/X] sn_diam_abort_message()</td>
<td>60</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>60</td>
</tr>
<tr>
<td>CSCuc16278 - DPCA PCRF too busy counter getting incremented with wrong vendor id</td>
<td>60</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>61</td>
</tr>
<tr>
<td>CSCud06768 - OCS/CCF address not displayed in show ims-authorization sessions full all</td>
<td>61</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>61</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>61</td>
</tr>
</tbody>
</table>
CSCud32573 - All Diameter Result Code 2xxx to be interpreted as success .................................................. 62
Feature Changes .................................................................................................................................................. 62
Performance Indicator Changes ...................................................................................................................... 62
CSCud42899, CSCui44116 - PCEF supervision/maintenance bulkstats .............................................................. 63
Feature Changes .................................................................................................................................................. 63
Performance Indicator Changes ...................................................................................................................... 63
CSCue51208, CSCue68221, CSCue68228, CSCue68231, CSCui08926 - support for SN-Transparent-Data on
Gx, Gy and CDRs - IPSG .................................................................................................................................. 64
Feature Changes .................................................................................................................................................. 64
CSCue68677 - include Framed-IPv6-Prefix AVP in custom43 Radius dictionary ................................................ 64
Feature Changes .................................................................................................................................................. 64
CSCuf56984 - Gx-Support for Flow-Direction AVP - Bidirectional(3) required ................................................ 64
Feature Changes .................................................................................................................................................. 64
CSCuf81120, CSCug02124 - RADIUS AAA and CoA/DM Requirements for PGW/LMA ................................. 65
Feature Changes .................................................................................................................................................. 65
CSCug38375 - Backpressure CLI needs to be made non-hidden ..................................................................... 65
Feature Changes .................................................................................................................................................. 65
Command Changes .............................................................................................................................................. 65
Performance Indicator Changes ....................................................................................................................... 66
CSCug38387, CSCug72334 - New GX DIAMETER KPIs in CLI ........................................................................ 66
Feature Changes .................................................................................................................................................. 66
Performance Indicator Changes ....................................................................................................................... 67
CSCug38399 - Assumed Positive Stats for the DIAMETER Interfaces ............................................................... 68
Feature Changes .................................................................................................................................................. 68
show diameter aaa-statistics .......................................................................................................................... 68
CSCug41175 - Gy & Gx - Length of the Redirect URL increase to 512 .............................................................. 68
Feature Changes .................................................................................................................................................. 68
CSCug70326, CSCun27457 - Gy Backpressure Enhancements .................................................................... 69
Feature Changes .................................................................................................................................................. 69
Performance Indicator Changes ....................................................................................................................... 69
CSCug75153, CSCug86476 - Additional set of KPIs for Gy assume positive ................................................... 70
Feature Changes .................................................................................................................................................. 70
Command Changes .............................................................................................................................................. 71
Performance Indicator Changes ....................................................................................................................... 71
CSCug78671, CSCui08938, CSCui08968 - support for SN-Transparent-Data on Gx, Gy and CDRs - GGSN 72
Feature Changes .................................................................................................................................................. 72
CSCuh24827 - Support new Interfaces for Tracing: Gy : GGSN/PGW/SAEGW ........................................... 72
Feature Changes .................................................................................................................................................. 72
Command Changes .............................................................................................................................................. 72
CSCuh41778, CSCul85477 - Gx, T(Potentially re-transmitted message) Flag not sent on retrans ... 73
Feature Changes .................................................................................................................................................. 73
Command Changes .............................................................................................................................................. 73
CSCuh43130 - Server unreachable condition is hit without behavior trigger configured ............................... 74
Feature Changes .................................................................................................................................................. 74
CSCuh53213 - PGW should not generate Rf records if UE is IDLE & not tx any data ................................. 74
Feature Changes .................................................................................................................................................. 74
Command Changes .............................................................................................................................................. 74
CSCuh75147 - LP support for APN AMBR failure/Default EPS bearer failure .............................................. 75
Feature Changes .................................................................................................................................................. 75
Command Changes .............................................................................................................................................. 75
Performance Indicator Changes ....................................................................................................................... 76
CSCuh75212 - Clean up of unused clis in Local Policy .................................................................................. 76
Feature Changes .................................................................................................................................................. 76
Performance Indicator Changes ....................................................................................................................... 76
<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>Command Changes</th>
<th>Performance Indicator Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuh75223 - Support for Local policy and PCRF together</td>
<td>77</td>
<td>77</td>
</tr>
<tr>
<td>CSCuh86452 - Gx support for Assumed Positive Stats in CLI</td>
<td>79</td>
<td>79</td>
</tr>
<tr>
<td>CSCuh86548 - Gx: Backpressure CLI needs to be made non-hidden</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>CSCuh86555 - Gy: Backpressure CLI needs to be made non-hidden</td>
<td>82</td>
<td>82</td>
</tr>
<tr>
<td>CSCui79823 - local issue for iRat from 4G to S4</td>
<td>82</td>
<td>82</td>
</tr>
<tr>
<td>CSCui38626 - [Paging] Reservation for radius &amp; AAA attr for HNBGW Gridld paging</td>
<td>83</td>
<td>83</td>
</tr>
<tr>
<td>CSCui70597, CSCui42608, CSCui63683 - Homogenous Support of IMS Voice over PS Sessions indication in ULR msg</td>
<td>83</td>
<td>83</td>
</tr>
<tr>
<td>CSCui70624 - Support T-ADS Data Retrieval</td>
<td>84</td>
<td>84</td>
</tr>
<tr>
<td>CSCui34346 - Need Statistics to display the reason for fallback to local-policy</td>
<td>84</td>
<td>84</td>
</tr>
<tr>
<td>CSCui39668 - [samog] DER Flags and DEA Flags AVP support for STa interface</td>
<td>84</td>
<td>84</td>
</tr>
<tr>
<td>CSCui39695 - [samog] 3GPP-GPRS-Negotiated-QoSProfile addition in DEA and AAA message</td>
<td>85</td>
<td>85</td>
</tr>
<tr>
<td>CSCui68013 - IPSG:No ULI towards Gx in CCR-I with diameter dictionary r8-gx-standard</td>
<td>85</td>
<td>85</td>
</tr>
<tr>
<td>CSCui96681 - pcfr_received qos is not recovering correctly</td>
<td>85</td>
<td>85</td>
</tr>
<tr>
<td>CSCum06052 - Degraded RAID failed after unexpected switchover as dirty degraded array</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>CSCum44960 - Call gets established on receiving error result code from Gx server</td>
<td>87</td>
<td>87</td>
</tr>
<tr>
<td>CSCum64825 - Segmentation Fault: acsmgr_dcca_message_cb</td>
<td>87</td>
<td>87</td>
</tr>
<tr>
<td>CSCum72921 - Redirect-Host AVP support for Rf Interface</td>
<td>87</td>
<td>87</td>
</tr>
<tr>
<td>CSCum75843 - Experimental Result code 5142 is populated in Result Code AVP</td>
<td>88</td>
<td>88</td>
</tr>
<tr>
<td>CSCum88821 - Sig11: PC: [~/is73944/X] libc.so.6/strnncmp_sse4_2()</td>
<td>88</td>
<td>88</td>
</tr>
<tr>
<td>CSCum97722 - Unexpected resultcode value in RAA when invalid QoS is installed in RAR</td>
<td>88</td>
<td>88</td>
</tr>
<tr>
<td>CSCun18463 - Gx: CCR-U for Revalidation_timeout sent even after disabling the trigger</td>
<td>89</td>
<td>89</td>
</tr>
<tr>
<td>CSCun34690 - IPSG sessions cleared with REAUTH_ADD_FAILURE upon CCA-u arrival on Gx</td>
<td>89</td>
<td>89</td>
</tr>
<tr>
<td>CSCun51012 - Bulkstat variables to be added for Switches-Tx timeout, Switches-RAR ch</td>
<td>89</td>
<td>89</td>
</tr>
</tbody>
</table>
### CF Changes in Release 16

- **CSCun62685** - CCR-U is retried even if server-retries configured as zero
- **Feature Changes**
- **CSUn89716** - Can’t find time at which Gy assume positive was triggered for a session
- **Feature Changes**
- **Performance Indicator Changes**

### ADC Changes in Release 16

- **ADC Enhancements for 16.2**
- **CSCue79102** - skypeout detection required
- **Feature Changes**
- **Command Changes**
- **Performance Indicator Changes**
- **CSCuo80798** - [P2P] CLI required for Audio/Video Duration Counter in p2p analyser
- **Feature Changes**
- **Command Changes**

### ECS Changes in Release 16

- **ECS Enhancements for 16.2**
- **CSCuq49998** - PGW (Gp) rejecting dynamic rule with Unknown Bearer ID cause
- **Feature Changes**
CSCup67356 - Rule failure counters not incremented .................................................. 110
Feature Changes ........................................................................................................ 110
Performance Indicator Changes ............................................................................. 111
CSCup86339 - Assert sessmgr_ipv4.c:10235 : sessmgr_ipv4_process_user_pkt_part2() .... 111
Feature Changes ........................................................................................................ 111
CSCug23706 - Removal of dynamic Rule is not working in UE only mode .................. 111
Feature Changes ........................................................................................................ 111
ECS Enhancements for 16.1 ....................................................................................... 112
CSCuc90721 - CCR-T not triggered when mandatory avp rating-grp wrong in rule install .... 112
Feature Changes ........................................................................................................ 112
Performance Indicator Changes ............................................................................. 112
CSCud411033 - flow idle timeout + flow limit for udp does not work ..................... 112
Feature Changes ........................................................................................................ 112
Command Changes .................................................................................................... 113
CSCui26390, CSCUm92182 - PDSN/PCEF upgrades/downgrades users’ Qos, depending on service start/stop .................................................................................................................. 113
Feature Changes ........................................................................................................ 113
Command Changes .................................................................................................... 113
CSCui55484, CSCuj96529 - Support of ULI as X-header field in HE feature .............. 114
Feature Changes ........................................................................................................ 114
CSCui16626 - ECS Support Always send Charging-Rule-Report AVP in RAA on Gx .... 114
Feature Changes ........................................................................................................ 114
CSCuo63589 - TRM Fastpath CLI needs change .......................................................... 115
Feature Changes ........................................................................................................ 115
Command Changes .................................................................................................... 115
ECS Enhancements for 16.0 ....................................................................................... 116
CSCue69163 - I-RAT handover - change in Rating Group to utilize CCR-U on Gy interface .... 116
Feature Changes ........................................................................................................ 116
CSCug70309 - S5 Signaling minimization for MBR change of non-GBR flows ............. 116
Feature Changes ........................................................................................................ 116
CSCug71725, CSCuh65672 - ECS Normal Path Performance Improvements ............. 117
Feature Changes ........................................................................................................ 117
CSCug86838, CSCub86414, CSCui19930, CSCui19941, CSCug86780, CSCug87258, CSCug87234 - [ICSR-Volte] Removing usage of pacing queue for critical MC-ECS new frmk .... 117
Feature Changes ........................................................................................................ 117
CSCug87349 - Gy Assume Positive - HA Usage Reporting .......................................... 118
Feature Changes ........................................................................................................ 118
Command Changes .................................................................................................... 118
CSCuh63073 - Charging for retransmissions to be controlled by svc/rbase level CLI .... 122
Feature Changes ........................................................................................................ 122
Command Changes .................................................................................................... 122
CSCui06831 - Lean Path for Rf .................................................................................. 122
Feature Changes ........................................................................................................ 122
CSCuij78410 - Cannot enable/configure TRM feature on SSI UCS/blade platform .... 123
Feature Changes ........................................................................................................ 123
CSCum39392 - Incorrect readdressed stats shown in ‘charging-action statistics’. ......... 123
Feature Changes ........................................................................................................ 123
Command Changes .................................................................................................... 124
CSCum45087 - ACR-I is generated with Zero usage with CC SERVICE_DATA_TIME_LIMIT... 125
Feature Changes ................................................................. 125
CSCum95153 - Sig11:PC: [08425115/X] acsmgr_handle_frag_reassembly()........... 126
Feature Changes ................................................................. 126
CSCun35089 - Printing the warnings for retransmissions elated CLIs to be deprecated... 126
Feature Changes ................................................................. 126
Command Changes .................................................................. 127

**ePDG Changes in Release 16** ........................................... 129

ePDG Enhancements for 16.2 .................................................................. 130
CSCum84987 - [ePDG] - P-CSCF addr over GTP S2b via the APCO parameter in the CSR... 130
Feature Changes .................................................................. 130
CSCuo74940 - [ePDG] - Non-UICC device support using certificate based authentication... 131
Feature Changes .................................................................. 131
CSCuo74943 - [ePDG] - IPsec subsystem enhancement to trigger AUTH req post OCSP comm... 131
Feature Changes .................................................................. 131
CSCuo94733 - [ePDG] - Bulkstats support for non UICC devices .................................. 131
Feature Changes .................................................................. 131
ePDG Enhancements for 16.1 .................................................................. 132
CSCtz75077 - ASR5500 Support for ePDG ................................................................. 132
Feature Changes .................................................................. 132
ePDG Enhancements for 16.0 .................................................................. 133
CSCua99299 - [ePDG] no show epdg-svc session peer-addr <IP> .................................. 133
Feature Changes .................................................................. 133
CSCug87380 - Narrowing of Traffic Selectors ............................................................... 133
Feature Changes .................................................................. 133
CSCuh32223 - [ICSR-VoLTE] Need a CLP level distinction for VoLTE and non VoLTE calls... 134
Feature Changes .................................................................. 134
CSCuh32234, CSCuh32245 - [ICSR-VoLTE] Changes to allow control and data traffic in pending_standby... 134
Feature Changes .................................................................. 134
CSCuh33073 - Static IP address allocation for the UE ......................................................... 134
Feature Changes .................................................................. 134
CSCuh33133 - New Bulkstats for the number of UEs present in system ......................... 135
Feature Changes .................................................................. 135
CSCuh46483 - Support .................................................................. 136
Feature Changes .................................................................. 136
Command Changes .................................................................. 136
CSCui21701 - Enhance ePDG service stats for the qci based bearer stats...................... 136
Feature Changes .................................................................. 136
Performance Indicator Changes .................................................................................. 137
CSCug83335 - IPV6 IPsec Swu interface .................................................................. 138
Feature Changes .................................................................. 138
CSCui42954 - ePDG and HeNBGW combo ................................................................. 138
Feature Changes .................................................................. 138
CSCui21726 - Sessmgr changes for SWu over IPv6 transport support ......................... 140
Feature Changes .................................................................. 140
CSCul15285 - Local PGW resolution required for ePDG .............................................. 140
Feature Changes .................................................................. 140
CSCul88963 - VoLTE enhancement License for 16.0 ..................................................... 141
Feature Changes .................................................................. 141

**GGSN Changes in Release 16** ........................................... 143

GGSN Enhancements for 16.2 .................................................................. 144
CSCun84742 - S6b Assume +ve counter is missing for the Current Subs in system ........ 144
Feature Changes .................................................................. 144
### GTPP Enhancements for 16.2

- CSCu040814 - [gn-gp]: 2 Bearers with same QCI/ARP combination - QCI Downgrade Case
- Feature Changes

### GTPP Enhancements for 16.5

- CSCun84742
- CSCuo40814
- CSCun71456
- CSCu12720
- CSCuh28410
- CSCug70293
- CSCty95123
- CSCum15133
- CSCug41145
- CSCul59203
- CSCuh35139
- CSCua99366
- CSCui04214
- CSCuo40814

### GGSN Enhancements for 16.0

- CSCua97985 - Graceful Shutdown of PDN with inactive VoLTE calls
- Feature Changes
- Command Changes
- CSCu99366, CSCu04214 - Dedicated bearer timeout action
- Feature Changes
- CSCug38359 - QCI Based Stats for CLI and Bulkstats
- Feature Changes
- Performance Indicator Changes
- CSCuh35139 - PGW SM sync up with driver [Phase 1]
- Feature Changes
- CSCui59203 - GGSN Rf Record populated with SGSN MCC-MNC AVP as ????
- Feature Changes
- Command Changes
- CSCug41145 - QoS eARP - H & M configuration on GGSN/PGW
- Feature Changes
- Command Changes
- Performance Indicator Changes
- CSCug95856 - GGSN - Common flags control through CLI
- Feature Changes
- Command Changes
- Performance Indicator Changes
- CSCum15133 - Def Bearer Rejected stats under APN level is inconsistent for HO cases
- Feature Changes
- CSCum85474 - Wrong data type for Bearer reject bulkstat variable (rejbearer)
- Performance Indicator Changes
- CSCun51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change
- Feature Changes
- CSCty95123 - Always-ON license for GGSN
- Feature Changes
- Performance Indicator Changes
- CSCug70293 - PCO for UE Notification - GGSN Support
- Feature Changes
- CSCuh28410 - GTP-U UDP Bundle
- Feature Changes
- Command Changes
- Performance Indicator Changes

### GTPP Changes in Release 16

- GTPP Enhancements for 16.5
- CSCuu12720 - Wrong timeOfFirstUsage value in LOSDV for Service idle out condition
- Feature Changes
- GTPP Enhancements for 16.2
- CSCun71456 - Diff order of supportzone config causes stranded CDR stuck
- Feature Changes
- CSCup59675 - gtpn push-to-active feature password shown in plain text
Feature Changes ........................................................................................................................................ 165
Command Changes .................................................................................................................................. 165
GTPP Enhancements for 16.1 .................................................................................................................. 166
CSCuo33140 - SGWRECORD EPCQoSInformation UL/DL GBR/MBR showing negative values. 166
Feature Changes ...................................................................................................................................... 166
GTPP Enhancements for 16.0 .................................................................................................................. 167
CSCua75528 - GGSN/PGW/SGW multiple sessmgr-crashes occurred-due to dictionary change. 167
Feature Changes ...................................................................................................................................... 167
CSCue50610, CSCui11709 - PGW CDR for session from S4SGSN (with CGI,RAI) has only CGI in ULI field 168
Feature Changes ...................................................................................................................................... 168
CSCue68228 - IPSG: Support SN-Transparent-Data and SN-Assigned-VLAN-ID in eGCDRs. 169
Feature Changes ...................................................................................................................................... 169
CSCug95458 - CDRs on CGW and SaMOG GW .................................................................................... 169
Feature Changes ...................................................................................................................................... 169
CSCuh31699 - CDR LIFO ....................................................................................................................... 170
Feature Changes ...................................................................................................................................... 170
CSCuh30721 - Stranded CDR on ICSR automated solution .................................................................. 171
Feature Changes ...................................................................................................................................... 171
Command Changes ................................................................................................................................ 171
Performance Indicator Changes ............................................................................................................. 172
CSCui95971, CSCui3956 - Rel10 Compliance for SGW-CDRs.............................................................. 172
Feature Changes ...................................................................................................................................... 172
Command Changes ................................................................................................................................ 172
CSCui99515 - Disabling the triggers for closing CDR service containers. ............................................. 173
Feature Changes ...................................................................................................................................... 173
Command Changes ................................................................................................................................ 173
CSCui23630 - Change the max outstanding configuration for GTPP .................................................. 174
Feature Changes ...................................................................................................................................... 174
Command Changes ................................................................................................................................ 174
CSCui77461 - aaaproxy in warn state during call model run ............................................................... 175
Feature Changes ...................................................................................................................................... 175
CSCui88752 - Std GTPP dictionaries should support multiple data record format version .................. 175
Feature Changes ...................................................................................................................................... 175
Command Changes ................................................................................................................................ 175
Performance Indicator Changes ............................................................................................................. 176
CSCum14682 - The tag values of ambr uplink and downlink should be made 3gpp compliant. ............ 176
Feature Changes ...................................................................................................................................... 176
CSCum55255 - behavior change in PGW-CDR .................................................................................... 176
Feature Changes ...................................................................................................................................... 177
CSCum72801 - custom24 dictionary not supporting qos req/neg length >15 in CDRs ......................... 177
Feature Changes ...................................................................................................................................... 177
CSCum76702 - CDR File transfer of Stranded CDR at new standby is very slow .............................. 178
Feature Changes ...................................................................................................................................... 178
CSCum99631 - To add ps fci related fields to custom43 ...................................................................... 178
Feature Changes ...................................................................................................................................... 178
HeNBGW Changes in Release 16 ........................................................................................................... 179
HeNBGW Enhancements for 16.1 ............................................................................................................ 180
CSCtx74503 - HENBGW: Access side SCTP params configuration template support. ...................... 180
Feature Changes ...................................................................................................................................... 180
Command Changes ................................................................................................................................ 181
Performance Indicator Changes ............................................................................................................. 181
HNBGW Changes in Release 16

HNBGW Enhancements for 16.0

CSCtx74512 - HENBGW: Network side SCTP params configuration template support

Command Changes

Feature Changes

Performance Indicator Changes

CSCtx94825 - HeNBGW IPSec: Need to support Certificate based IKEv2 authentication

Feature Changes

CScu51912 - HENBGW: Need support for displaying secgw detail under henbgw access svc

Feature Changes

Performance Indicator Changes

CSCub79833 - HENBGW: Support for IPv6 PDNs

Feature Changes

CSCub79840 - HENBGW: Support for IPv4V6 PDN

Feature Changes

CSCuh88668 - HeNBGW: 3GPP release 10 S1AP support

Feature Changes

CSCuh90407 - HeNBGW: X2 Handover support

Feature Changes

CSCuh92913 - HENBGW: AP trace using HeNB ID or IP

Feature Changes

CSCuh95440 - HENBGW Session recovery enhancements

Feature Changes

CSCum08997 - KT HeNBGW: Trap support for Congestion control

Feature Changes

Performance Indicator Changes

CSCui94489 - KT HeNBGW: HeNBGW does not send HB REQ after primary path recovery

Feature Changes

CSCui62727 - HeNBGW-nsvc: Cli to reflect multihomed log enb - mme assoc paths

Feature Changes

HNBGW Changes in Release 16
HSGW Changes in Release 16...................................................................................................................... 199
HSGW Enhancements for 16.0.................................................................................................................................... 200
CSCCu34742 - [HSGW]: Incorrect DSCP marking done on A11 ................................................................. 200
Feature Changes ........................................................................................................................................... 200
CSCu87231 - HSGW, PGW support Pmipv6 control protocol over ipv4 ...................................................... 201
Feature Changes ........................................................................................................................................... 201
HSGW and P-GW support for Pmipv6 control protocol over ipv4 ........................................................... 201
Command Changes ....................................................................................................................................... 201
CSCud56103 - HSGW Support MSISDN in PBU to PGW through S2a interface ........................................ 201
Feature Changes ........................................................................................................................................... 201

InTracer Changes in Release 16.......................................................................................................................... 203
InTracer Enhancements for 16.3.......................................................................................................................... 204
CSCu46241 - SGSN v 1.1 Header Support ......................................................................................................... 204
Feature Changes ........................................................................................................................................... 204

IPSG Changes in Release 16 ............................................................................................................................... 205
IPSG Enhancements for 16.0.............................................................................................................................. 206
CSCt43130 - Support to check lawful-intercept statistics per context level ...................................................... 206
Feature Changes ........................................................................................................................................... 206
CSCuc58900 - Combo IPSG+GGSN required .................................................................................................... 207
Feature Changes ........................................................................................................................................... 207
CSCui90453 - IPSG+GGSN qualification on ASR5500 ...................................................................................... 207
Feature Changes ........................................................................................................................................... 207
CSCui90463 - IPSG qualification on SSI .......................................................................................................... 207
Feature Changes ........................................................................................................................................... 207

MME Changes in Release 16.............................................................................................................................. 209
MME Enhancements for 16.5............................................................................................................................. 210
CSCur19886, CSCus74843 - Sessmgr crash sess/mme/mme-app/app/mme_egtp_fw.c:1014 ........................................ 210
Feature Changes ........................................................................................................................................... 210
CSCus18004 - MME rounds down max bitrate in VoLTE leading to packet loss ........................................ 211
Feature Changes ........................................................................................................................................... 211
CSCus82793 - MME Re-locate UE command to expand range from 0-65536 ............................................. 211
Feature Changes ........................................................................................................................................... 211
Command Changes ....................................................................................................................................... 211
MME Enhancements for 16.4............................................................................................................................. 213
CSCup36013 - Missing TAI bulkstats variable: tai-emm-msgtx-csg-not-subscribed ........................................ 213
Feature Changes ........................................................................................................................................... 213
Performance Indicator Changes .................................................................................................................. 214
CSCuq57243 - MME does E-RAB release at the end of CS HO ..................................................................... 214
Feature Changes ........................................................................................................................................... 214
Performance Indicator Changes .................................................................................................................. 214
CSCuq88194 - New Reject cause needs to be added under Bearer Alloc Reject ESM message ...................... 214
Feature Changes ........................................................................................................................................... 214
Performance Indicator Changes .................................................................................................................. 215
CSCur27407 - NewConnectionsDisallowed SNMP trap firing a lot ............................................................. 215
Feature Changes ........................................................................................................................................... 215
CSCur38243 - MME discards EGTP_CREATE INDIRECT_DATA_FORWARDING_TUNNEL_RSP215 Feature Changes .......................................................................................................................... 215
CSCur52162 - Parser error for initial-ue msgs with nas-pdu length from than 127 bytes .............................. 216
Feature Changes ........................................................................................................................................... 216
CSCur73766 - TAU Reject Cause 0 after Auth Req Timeout .......................................................................... 216
Feature Changes ........................................................................................................................................... 216
CSCur89996 - MME releases UE context with Category NAS : Unspecified for Radio issues ...................... 216
Feature Changes ........................................................................................................................................... 216
Command Changes ................................................................. 217
CSCur97596, CSCun97512 - paging event causing failures (PSC3 only, DPC is not) ... 218
Feature Changes ..................................................................... 218
Command Changes .................................................................. 218
CSUs14148 - Dynamic Paging cache size allocation through CLI ...................... 218
Feature Changes ..................................................................... 218
Command Changes .................................................................. 219
MME Enhancements for 16.3 ..................................................... 221
CSCu52247 - SIM-less emergency attach failure when UE does not support EIA0&EEA0 ... 221
Feature Changes ..................................................................... 221
CSCu57477 - Card Busy-out CLI on PSC card in the MME causes loss of Service ... 222
Feature Changes ..................................................................... 222
MME Enhancements for 16.2 ..................................................... 223
CSCum50504 - MME doesn’t release resources after receiving DDN from SGW .... 223
Feature Changes ..................................................................... 223
CSCu13234 - MME behavior when receiving NAPTR response with empty flag ... 224
Feature Changes ..................................................................... 224
CSCu17932 - MME sending old QoS values to UE after HO from 2G>4G>2G .... 224
Feature Changes ..................................................................... 224
Command Changes .................................................................. 224
Performance Indicator Changes ................................................... 225
CSCu24135 - SLs: show sl-service peers all CLI output can display mmemgr ID too ... 225
Performance Indicator Changes ................................................... 225
CSCu29345 - Need MMEmgr CPU and Memory bulkstat counter for MME capacity monitoring ... 225
Feature Changes ..................................................................... 225
Performance Indicator Changes ................................................... 226
CSCu44359 - [CMAS]: Need to restructure few SBC counters for better clarity ... 226
Performance Indicator Changes ................................................... 226
CSCu54025 - S1 and SGs associations not equally distributed across mmemgr tasks ... 227
Feature Changes ..................................................................... 227
Performance Indicator Changes ................................................... 227
CSCu58544 - sessmgr Fatal Signal 6 __kernel_vsyscall() - show mme-service db record ... 228
Feature Changes ..................................................................... 228
CSCu70412 - mmemgr resources not used when eSMCC peers are UP ... 228
Performance Indicator Changes ................................................... 228
MME Enhancements for 16.1 ..................................................... 229
CSCh68156 - Demux failover with 32k eNBs, Assert=mmemgr_add_flow_aggregate() ... 229
Feature Changes ..................................................................... 229
CSCh92041 - MME is not sending Destination-Host AVP in LRR .......................... 230
Feature Changes ..................................................................... 230
Command Changes .................................................................. 230
Performance Indicator Changes ................................................... 230
CSCh56247, CSCh80306, CSCh80313, CSCh80317 - MME: SLs interface support .... 231
Feature Changes ..................................................................... 231
Command Changes .................................................................. 231
Performance Indicator Changes ................................................... 236
CSCh68851 - MME TAC level EMM procedure counter support .......................... 241
Feature Changes ..................................................................... 241
Command Changes .................................................................. 242
Performance Indicator Changes ................................................... 243
CSCh59961, CSCh59952 - SLg Interface - Include MSISDN AVP in procedures ...... 252
Feature Changes ..................................................................... 252
CSCh68522 - PDN_Connect by UE rejected during IM exit procedure ................. 253
Feature Changes

CSCuo21484 - Enhance show session subsystem mmemgr CLI for sbc stats ........................................... 253
Performance Indicator Changes ........................................... 253
CSCuo56093 - 'qos ue-ambr max-ul 0 max-dl 0' added automatically in configuration ..................... 255
Feature Changes ........................................... 255
Command Changes ........................................... 255
CSCup23821 - NPUMGR Restart causing MME enB SCTP failures and impact to SGs/S1AP ....... 256
Feature Changes ........................................... 256
Performance Indicator Changes ........................................... 256
CSCup32019 - SLs: MME needs to handle S10 TAU (AF not set) for NI-LR lcs procedure .......... 257
Feature Changes ........................................... 257
CSCzn11186 - MME support for Sbc interface (Sbc-AP) to Cell broadcast center (CBC) ........ 257
Feature Changes ........................................... 257
Command Changes ........................................... 258
Performance Indicator Changes ........................................... 261

MME Enhancements for 16.0 ........................................................................................................................................... 269
CSCtr43130 - Support to check lawful-intercept statistics per context level ........................................... 269
Feature Changes ........................................... 269
CSCtt33631 - session disconnect-reason - mme-regional-zone-code needs to be removed ...... 270
Performance Indicator Changes ........................................... 270
CSCtt40129 - MME(LI)-Support for Request Type TLV in TYPE x14 IRI event .......... 270
Feature Changes ........................................... 270
CSCtt61742 - MME should support configuration to distinguish between HENBGW and eNBs ........ 270
Feature Changes ........................................... 270
Command Changes ........................................... 270
Performance Indicator Changes ........................................... 272
CSCty04851 - Standards-based tracing enhancements ................................................................................. 272
Feature Changes ........................................... 272
Command Changes ........................................... 273
Performance Indicator Changes ........................................... 273
CSCua84681 - LI : LI Provisioning doest support IPv6 address subscriber provisioning ........ 274
Feature Changes ........................................... 274
Command Changes ........................................... 274
CSCub06145 - MME:SGS VLR re-selection in case of loss of VLR association ........................................... 275
Feature Changes ........................................... 275
Command Changes ........................................... 275
Performance Indicator Changes ........................................... 275
CSCub06763 - Paging Load Control .................................................................................................................. 276
Feature Changes ........................................... 276
Command Changes ........................................... 276
Performance Indicator Changes ........................................... 277
CSCub29503 - MME: Sv Improvements - MSC selection using DNS ......................................................... 278
Feature Changes ........................................... 278
Command Changes ........................................... 279
Performance Indicator Changes ........................................... 279
CSCub29525 - MME: Sv Improvements: MSC fallback on failure ......................................................... 280
Feature Changes ........................................... 280
CSCuc96756, CSCuh04626, CSCun73028 - MME: Extend paging-map for PS to include QCI ........................................... 280
Feature Changes ........................................... 280
Command Changes ........................................... 281
Performance Indicator Changes ........................................... 281
CSCug50843 - Improved UX for status commands ......................................................................................... 285
Feature Changes ........................................... 285
Command Changes ........................................... 286
Performance Indicator Changes ................................................................. 286
CSCuh31666 - Authentication vector management in MME and S4 SGSN ............... 286
Feature Changes .................................................................................. 286
Command Changes .............................................................................. 287
CSCuh35890 - MME Optimization of S1 reset handling in MME ......................... 287
Feature Changes .................................................................................. 287
Performance Indicator Changes ............................................................. 288
CSCuh38256 - LCS : LR Answer Dropped stat not pegged ............................. 288
Performance Indicator Changes ............................................................. 288
CSCuh47311 - Need CLI visibility into id database in S1AP stack ..................... 288
Command Changes .............................................................................. 288
Performance Indicator Changes ............................................................. 288
CSCuj16369 - MME is not sending S1-Setup response when 33 PLMNs are configured ................................................................. 289
Feature Changes .................................................................................. 289
CSCuj42591 - Setting ‘IMS voice over PS session indicator’ per TAI list .............. 290
Feature Changes .................................................................................. 290
Command Changes .............................................................................. 290
Performance Indicator Changes ............................................................. 290
CSCuj42608, CSCuj63683 - Setting ‘Homogenous Support of IMS Voice over PS Sessions’ indication in Update Location Request message ........................................ 291
Feature Changes .................................................................................. 291
Command Changes .............................................................................. 291
CSCuj42615 - Purge requirement for PS -> CS handoff after SGSN Context Transfer ........................................................................... 292
Feature Changes .................................................................................. 292
Command Changes .............................................................................. 292
CSCui54893 - Support on MME for Tracing s13 interface ............................... 293
Feature Changes .................................................................................. 293
Command Changes .............................................................................. 293
CSCui61714 - Support for statistics to distinguish between CLI or HSS initiated Trace ....................................................................... 294
Performance Indicator Changes ............................................................. 294
CSCun28592 - S6a Feature List AVP is hardcoded in MME ............................. 294
Feature Changes .................................................................................. 294
CSCzn16621, CSCzn16622 - MME needs to support non-3gpp-to-LTE handover ......................................................................... 294
Feature Changes .................................................................................. 294
Performance Indicator Changes ............................................................. 295
CSCzn59071 - Improve logging and debug stats in MME/MEMGR ....................... 296
Performance Indicator Changes ............................................................. 296

MVG Changes in Release 16 ..................................................................... 297
MVG Enhancements for 16.0 .................................................................... 298
CSCug89455 - Video detection using HTTP payload contents ......................... 298
Feature Changes .................................................................................. 298
Command Changes .............................................................................. 298
CSCug89478 - Adding support for content-range HTTP header ....................... 299
Feature Changes .................................................................................. 299
Command Changes .............................................................................. 299

NAT Changes in Release 16 ..................................................................... 301
NAT Enhancements for 16.0 ..................................................................... 302
CSCud50942 - Need stats for packets that were bypass nated .......................... 302
Feature Changes .................................................................................. 302
Performance Indicator Changes ............................................................. 302
CSCuh25763 - NAT Realm per FW/NAT policy ............................................ 303
Feature Changes .................................................................................. 303
CSCuh97978 - [ICS-Volte] Removing the usage of pacing queue for critical MCs ................................................................. 303
PDSN Changes in Release 16

PDSN Changes in Release 16

PDSN Enhancements for 16.0

CSCull83326, CSCzm98044 - CLI to filter the subscribers based on on-demand NAT IP usage time

Feature Changes

Command Changes

PDSN Enhancements for 16.1

CSCtu38298 - AMBR/MBR/QCI parameter support in PDSN/PCEF

Feature Changes

Command Changes

CSCuh03636 - Need PDSN to support combined ipv4/v6 accounting for dual stack session

Feature Changes

Command Changes

PDSN Enhancements for 16.0

CSCum82051 - Call not up when 802.P is set to odd value in l2-mapping-table

Feature Changes

CSCun65435 - Assertion at sessmgr_imsa.c:453 Function: sessmgr_authorize_with IMSA

Feature Changes

CSCzn10122 - After configuring no max-login failures local user is not granted access

Feature Changes

Command Changes

PSF Changes in Release 16

PSF Changes in Release 16

PSF Enhancements for 16.0

CSCI88372 - SFW: feature parity of the PSFW between uplink and downlink

Feature Changes

Command Changes

Performance Indicator Changes

CSCub35955 - ICSR Support for Dynamic Firewall Access Rules

Feature Changes

CSCud50947 - Stats needed for traffic allowed thru default sfw rules/pin-holes

Feature Changes

Performance Indicator Changes

CSCue70886 - src-ip based flood attack detection

Feature Changes

Command Changes

Performance Indicator Changes

CSCue95313 - ASR5k port-scan request timeout should range from 1 to 30 secs

Feature Changes

P-GW Changes in Release 16

P-GW Changes in Release 16

P-GW Enhancements for 16.4

CSCup32052, CSCup08125 - Congestion is cleared on performing unplanned demux DPC migration

Feature Changes

CSCur72239 - Access point MAC address not displayed in show command

Feature Changes

P-GW Enhancements for 16.3

CSCuq88332 - Need EDR records from different rulebases to goto single EDR file

Feature Changes

CSCur26723 - MAPCON with Wifi and 3G

Feature Changes

P-GW Enhancements for 16.2

CSCuo06912 - PGW call fails if Framed-Pool enforced from radius

Feature Changes

CSCuo95038 - TMOPZ: PGW forces lower AMBR values than received
Feature Changes .................................................................................................................. 325
CSCup44058 - Acct msg shows both v4 and v6 addr even if v4 is denied for static alloc ........ 325
Feature Changes .................................................................................................................. 325
CSCup51117 - Difference in behaviour for eHRPD and LTE for fragmented output packets ... 325
Feature Changes .................................................................................................................. 325
CSCzn58818 - [gn-gp]: Anomaly in the display of 'IP allocation type' in the o/p of c .......... 326
Feature Changes .................................................................................................................. 326
P-GW Enhancements for 16.1 .............................................................................................. 327
CSCug23975 - VoLTE: Prioritized handling of for VoLTE/Emergency calls ....................... 327
Feature Changes .................................................................................................................. 327
Command Changes ............................................................................................................. 328
Performance Indicator Changes .......................................................................................... 328
CSCuh06375 - [PGW-S2a] Session creation after RADIUS Accounting-Response .............. 329
Feature Changes .................................................................................................................. 329
Command Changes ............................................................................................................. 329
CSCuh45717 - [PGW/S2a] Need support to Reject PBU (Type LE) ..................................... 330
Feature Changes .................................................................................................................. 330
CSCuh74228 - Unwanted UBRreq/UBResp for apn-ambr/QCI modification ...................... 330
Feature Changes .................................................................................................................. 330
CSCuh75147 - LP support for APN AMBR failure/Default EPS bearer failure .................. 331
Feature Changes .................................................................................................................. 331
Command Changes ............................................................................................................. 331
Performance Indicator Changes .......................................................................................... 332
CSCui11722 - Xheader inserted bytes included in Radius Accounting .............................. 332
Feature Changes .................................................................................................................. 332
CSCuj73225 - IPv4 Downlink Data packet forwarding/redirection support ......................... 332
Feature Changes .................................................................................................................. 332
CSCuj73344 - PGW: IPv6 Network Reachability Server for IPv6 Pools ......................... 333
Feature Changes .................................................................................................................. 333
Command Changes ............................................................................................................. 333
CSCuj73352 - PGW: ICSR support for customer enterprise PGW ....................................... 334
Feature Changes .................................................................................................................. 334
CSCuj73381 - PGW: PGW capability improvements ............................................................ 334
Feature Changes .................................................................................................................. 334
CSCuj88821 - Clab: gtpc overload-protection ingress CLIs cause misleading .................... 334
Feature Changes .................................................................................................................. 334
CSCuj89567 - show sub subsystem stats incorrect ............................................................. 334
Feature Changes .................................................................................................................. 334
Performance Indicator Changes .......................................................................................... 335
CSCun12922 - Dedicated bearer timeout Min value to be 5 min ...................................... 339
Command Changes ............................................................................................................. 339
CSCun84742 - S6b Assume +ve counter is missing for the Current Subs in system ............ 339
Feature Changes .................................................................................................................. 339
Performance Indicator Changes .......................................................................................... 340
CSCuo11336 - Update bearer Request not triggered on FUA action from Gy .................. 340
Feature Changes .................................................................................................................. 340
CSCuo16591 - Radius Acct Interim Update for Qos Change generated for all bearers .......... 341
Feature Changes .................................................................................................................. 341
CSCup03974 - No syslog generated for nw-reachability server status change Down -> Up ... 341
Feature Changes .................................................................................................................. 341
CSCup08125 - congestion state is not retained after egtpinmkr kill and recovery ............. 341
Feature Changes .................................................................................................................. 341
P-GW Enhancements for 16.0 .............................................................................................. 342
CSCsts49711 - [GTP-S5] Rad-Acct: No Interim for ULI-chng using ChngNotificationTrigger ... 342
Feature Changes .................................................................................................................. 342
CSCua47367, CSCuh30602 - Enhance PGW to report exact failure resulting in CC 73 .......... 343
Feature Changes .................................................................................................................. 343
CSCua97985 - Graceful Shutdown of PDN with inactive VoLTE calls .................................. 345
Feature Changes .................................................................................................................. 345
Command Changes ............................................................................................................. 346
CSCua99366 - Dedicated bearer timeout action ................................................................. 346
Feature Changes .................................................................................................................. 346
Command Changes ............................................................................................................. 346
Performance Indicator Changes .......................................................................................... 347
CSCub27300 - ASR5500 - Newcall support for rejecting calls on PGW .............................. 348
Feature Changes .................................................................................................................. 348
Command Changes ............................................................................................................. 348
CSCuc14962 - LI keep alive sent per sessmgr not per tcp connection ............................... 348
Feature Changes .................................................................................................................. 348
CSCuc87231 - HSGW, PGW support Pmipv6 control protocol over ipv4 ......................... 349
Feature Changes .................................................................................................................. 349
HSGW and P-GW support for Pmipv6 control protocol over ipv4 ..................................... 349
Command Changes ............................................................................................................. 349
CSCud60395 - Local Break Out support for VoLTE roaming ............................................ 349
Feature Changes .................................................................................................................. 349
Command Changes ............................................................................................................. 350
Performance Indicator Changes ......................................................................................... 351
CSCue00897 - PGW - support GTPv2 S2a interface and inter-access mobility ................. 351
Feature Changes .................................................................................................................. 351
CSCue15246 - PGW support - S2a PMIPv6 over IPv4 transport ....................................... 351
Feature Changes .................................................................................................................. 351
CSCug24179 - VoLTE related optimization- Fetching of VoLTE needs to be prioritized .... 352
Performance Indicator Changes ......................................................................................... 352
CSCug38359, CSCug72349 - QCI Based Stats for CLI and Bulkstats ............................... 352
Feature Changes .................................................................................................................. 352
Performance Indicator Changes ......................................................................................... 352
CSCug41145 - QoS eARP - H & M configuration configuration on GGSN/PGW ............... 356
Feature Changes .................................................................................................................. 356
CSCug75135 - PGW LORC mechanism for subscriber billing ........................................... 356
Feature Changes .................................................................................................................. 356
Command Changes ............................................................................................................. 356
Performance Indicator Changes ......................................................................................... 357
CSCug95856 - GGSN - Common flags control through CLI ............................................. 357
Feature Changes .................................................................................................................. 357
CSCuh28006, CSCui24601, CSCui24817 - Additional application support with DSCP-802.1p Marking per Interface ........................................................... 357
Feature Changes .................................................................................................................. 357
Command Changes ............................................................................................................. 358
Performance Indicator Changes ......................................................................................... 361
CSCuh28410 - GTP-U UDP Bundle .................................................................................... 362
Feature Changes .................................................................................................................. 362
Command Changes ............................................................................................................. 362
Performance Indicator Changes ......................................................................................... 362
CSCuh35139 - PGW SM sync up with driver [Phase 1] ....................................................... 363
Feature Changes .................................................................................................................. 363
CSCuh85489, CSCui06202 - SR Performance: Periodic FC interval needs to be increased . 363
Feature Changes .................................................................................................................. 363
CSCui97899 - When CBResp times out CCR-U is not sent from PGW ............................... 364
SAEGW Enhancements for Release 16.4 .................................................. 385
SAEGW Enhancements for Release 16.5 .................................................. 384
CSCur61470 - S2B Support on SAE-GW .................................................. 385
Feature Changes .................................................................................................................. 385
Command Changes ............................................................................................................... 386
Performance Indicator Changes .............................................................................................. 386
SAEGW Enhancements for 16.3 .............................................................................................. 388
CSCuo82399 - Collision counter support in GTP layer .......................................................... 388
Feature Changes ..................................................................................................................... 388
Performance Indicator Changes .............................................................................................. 388
SAEGW Enhancements for 16.2 .............................................................................................. 391
CSCun86828 - CBR - MBR collision causing MME to delete dedicated bearer ...................... 391
Feature Changes ..................................................................................................................... 391
CSCup67356 - Rule failure counters not incremented ............................................................... 392
Feature Changes ..................................................................................................................... 392
CSCuq10038 - NEMO support on SAEGW license request ..................................................... 392
Feature Changes ..................................................................................................................... 392
CSCuq25059 - Assertion failure at sess/smgr(sessmgr_ggsn.c:25058) ................................. 392
Feature Changes ..................................................................................................................... 392
SAEGW Enhancements for 16.1 .............................................................................................. 394
CSCuj89567 - show sub subsystem stats incorrect ................................................................. 394
Feature Changes ..................................................................................................................... 394
Performance Indicator Changes ............................................................................................. 394
CSCun35216 - S4 to Gn SGSN HO, CCR-u shows RAT type event for UTRAN ................ 399
Feature Changes ..................................................................................................................... 399
CSCun84742 - S6b Assume positive counter is missing for the Current Subs in system ... 399
Feature Changes ..................................................................................................................... 399
Performance Indicator Changes ............................................................................................. 399
CSCun86828 - CBR - MBR collision causing MME to delete dedicated bearer ...................... 400
Feature Changes ..................................................................................................................... 400
SAEGW Enhancements for 16.0 .............................................................................................. 401
CSCua99366, CSCui04214 - Dedicated bearer timeout action .............................................. 401
Feature Changes ..................................................................................................................... 401
Performance Indicator Changes ............................................................................................. 402
CSCuh13691 - R11 compliance on standard interfaces ........................................................... 403
Feature Changes ..................................................................................................................... 403
CSCuh13694 - ECS Cookie Match support for Websockets ............................................... 404
Feature Changes ..................................................................................................................... 404
CSCuh13699 - CDR LIFO ........................................................................................................ 404
Feature Changes ..................................................................................................................... 404
CSCuh25810 - SGW Session Idle Timer .............................................................................. 404
Feature Changes ..................................................................................................................... 404
Command Changes ................................................................................................................ 405
CSCuj01136 - SAEGW : pdn-count is not working for multi APN scenario ......................... 406
Command Changes ................................................................................................................ 406
CSCui21603 - SGW Honor ingress & egress DSCP & Support DSCP marking @ APN profile 406
Feature Changes ..................................................................................................................... 406
Command Changes ................................................................................................................ 406
Performance Indicator Changes ............................................................................................. 407
CSCui21610 - Dropped call counters granularity ................................................................... 408
Feature Changes ..................................................................................................................... 408
Performance Indicator Changes ............................................................................................. 408
CSCui04167 - PGW LORC mechanism for subscriber billing ................................................. 417
Feature Changes ..................................................................................................................... 417
Performance Indicator Changes ............................................................................................. 418
CSCui42572 - Error response handling at SGW ................................................................. 418
Feature Changes ..................................................................................................................... 418
Command Changes ........................................................................................................... 418
CSCui95971, CSCuj13956 - Rel10 Compliance for SGW-CDRs ........................................... 419
Feature Changes ............................................................................................................. 419

SaMOG Changes in Release 16 ....................................................................................... 421
SaMOG Enhancements for 16.0 ...................................................................................... 422
CSCue39756, CSCuh83489, CSCue00861, CSCug95521, CSCue39761 - Ethernet over GRE Support on
SaMOG Gateway ............................................................................................................ 422
Feature Changes ............................................................................................................. 422
Command Changes ........................................................................................................ 423
Performance Indicator Changes ..................................................................................... 425
show sub all ..................................................................................................................... 425
show sub samog-only-full ............................................................................................... 425
show sub full ................................................................................................................... 426
show dhcp statistics ....................................................................................................... 426
show apn-profile full ....................................................................................................... 429
show configuration errors .............................................................................................. 429
CSCug95440, CSCuj24323, CSCui95688, CSCui94593 - Local Breakout on SaMOG GW .......... 429
Feature Changes ............................................................................................................. 429
Command Changes ........................................................................................................ 430
Performance Indicator Changes ..................................................................................... 431
CSCug95458 - CDRs on CGW and SaMOG GW ................................................................. 432
Feature Changes ............................................................................................................. 432
Command Changes ........................................................................................................ 432
Performance Indicator Changes ..................................................................................... 434
CSCug95483, CSCui80861 - SaMOG support for 3G subscribers ....................................... 435
Feature Changes ............................................................................................................. 435
Command Changes ........................................................................................................ 436
Performance Indicator Changes ..................................................................................... 438
CSCuh75537 - Congestion Control Threshold and TCA Alerts ...................................... 442
Feature Changes ............................................................................................................. 442
Command Changes ........................................................................................................ 442
Performance Indicator Changes ..................................................................................... 443
CSCuh83409, CSCuh945616, CSCui94628 - Session Recovery support on SaMOG443
Feature Changes ............................................................................................................. 443
CSCun71453 - [SaMOG-3G] 3gpp2 attributes needs to be removed from radius server dict .... 444
Feature Changes ............................................................................................................. 444
CSCuo29010 - [SaMOG-GW] Support for Sequence Number Bit unset default with PMIP GRE .. 444
Feature Changes ............................................................................................................. 444
Command Changes ........................................................................................................ 444
Performance Indicator Changes ..................................................................................... 445

SecGW Changes in Release 16 ....................................................................................... 447
SecGW Enhancements for 16.1 ....................................................................................... 448
CSCtt22271 - RFC 4303 ESN ....................................................................................... 448
Feature Changes ............................................................................................................. 448
Command Changes ........................................................................................................ 449
Performance Indicator Changes ..................................................................................... 449
CSCum19793 - WSG as IKEv2 Initiator .......................................................................... 450
Feature Changes ............................................................................................................. 450
Command Changes ........................................................................................................ 450
Performance Indicator Changes ..................................................................................... 452
CSCum81454 - CLI to support Allow one tunnel per remote IKE_ID feature ..................... 452
Feature Changes ............................................................................................................. 452
Command Changes ........................................................................................................ 452
SGSN Changes in Release 16

SGSN Enhancements for 16.5
CSCus06673 - RAB Setup Fails with cause invalid-rab-parameters-combination
Feature Changes
Command Changes
Performance Indicator Changes

SGSN Enhancements for 16.4
CSCur07639 - Multiple SESSMGR crash of same kind after upgrade to 16.2.0
Feature Changes
Command Changes
Performance Indicator Changes

SGSN Enhancements for 16.3
CSCup77395 - Assert - sn_dp_utran_process_purge_req_evt()
Feature Changes
Command Changes

SGSN Enhancements for 16.2
CSCty13075 - PGW & SGW local address fallback-for-dns not working
Feature Changes
Command Changes

SGSN Enhancements for 16.1

Feature Changes
Command Changes

Security Gateway Enhancements for 16.0
CSCuo62141, CSCuo79732, CSCuo56933 - Remove SGSN Application code for Fast Path
Feature Changes
Command Changes

Command Changes

Feature Changes

Performance Indicator Changes
Contents

SGSN Enhancements for 16.0

Feature Changes

Command Changes

SGSN Enhancements for 16.1

Feature Changes

Performance Indicator Changes

Command Changes

CSCnu87321 - Notify PGW of modified QoS after negotiation with RNC

Feature Changes

Command Changes

CSCUp49664 - [Intracer] Require 1-to-1 mapping for ipms-suppress and no ipms-suppress

Feature Changes

Command Changes

CSCUp94785, CSCqu34454 - QOS management for uplink data messages in 2G

Feature Changes

Command Changes

CSCuo28628 - sm radio-priority

Feature Changes

Performance Indicator Changes

Command Changes

CSCtn15437, CSCuo37725 - InTracer Support of SGSN - New requirement

Feature Changes

Performance Indicator Changes

Command Changes

CSCuq62285 - IP tcp mss settings on sgsn

Feature Changes

Command Changes

CSCu989398 - [16.0] Discrepancy in modify bearer req in rau from pre r7 and r7 rnc

Feature Changes

Command Changes

CSCuo62754 - Assertion failure at sess/sgsn/sgsn-app/db/sgsn_db_pmm.c:1880

Feature Changes

Command Changes

SGSN Enhancements for 16.0

CSCtr31994 - [S4-SGSN] RIM message should be supported over S16 and S3 interface

Feature Changes

Command Changes

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

Feature Changes

Command Changes

CSCts57950, CSCud49814, CSCuj06828 - Configurable Cause code mapping

Feature Changes

Command Changes

Performance Indicator Changes

CSCtx38089 - [S4-SGSN] UE-AMBR over RANAP messages shall be supported

Feature Changes

Command Changes

Performance Indicator Changes

CSCtx38779 - RFSP from subscription or local policy to be supported

Feature Changes

Command Changes

Performance Indicator Changes

CSCty34288, CSCuh28109 - Need enhancement on map statistics as to why SAI / UGL fails

Command Changes

Performance Indicator Changes

CSCty42425 - [S4-SGSN] APN-AMBR override from local config shall be supported in 3G

Feature Changes

Command Changes

CSCty42433 - [S4-SGSN] APN-AMBR override from local config shall be supported in 2G

Feature Changes
Command Changes ........................................................................................................ 496
CSCut44479 - APN Restriction on S4-SGSN ................................................................. 497
Feature Changes ........................................................................................................ 497
CSCz55422 - SGSN should start dns query for default SGSN when nri based query fails / Fallback to RAI based query when NRI based query fails ......................................................... 498
Feature Changes ........................................................................................................ 498
Command Changes ..................................................................................................... 498
Performance Indicator Changes .................................................................................... 498
CSCz55455 - SGSN Disable GTPv0 for specific set of APNs ........................................ 499
Feature Changes ........................................................................................................ 499
Command Changes ..................................................................................................... 499
Performance Indicator Changes .................................................................................... 499
CSCz83032 - NRI Based DNS Query for Inter Pool 2G requests ............................... 499
Feature Changes ........................................................................................................ 499
Command Changes ..................................................................................................... 500
CSCub16134 - Paging Load throttling ........................................................................ 501
Feature Changes ........................................................................................................ 501
Command Changes ..................................................................................................... 501
Performance Indicator Changes .................................................................................... 501
CSCub16201, CSCub48329 - Support for QoS Upgrade from GGSN/PCRF .................. 504
Feature Changes ........................................................................................................ 504
Command Changes ..................................................................................................... 504
Performance Indicator Changes .................................................................................... 504
CSCub16578 - SNAPTR Queries for GGSN selection ................................................... 506
Feature Changes ........................................................................................................ 506
Command Changes ..................................................................................................... 506
CSCub34940 - Bypass APN remap functionality .......................................................... 506
Feature Changes ........................................................................................................ 506
CSCub46992, CSCub47023 - 3G-SGSN and 2G-SGSN on ASR5500 ............................. 508
Feature Changes ........................................................................................................ 508
Command Changes ..................................................................................................... 508
CSCub48101 - QoS based on PLMN and RAT .............................................................. 509
Feature Changes ........................................................................................................ 509
Command Changes ..................................................................................................... 509
Performance Indicator Changes .................................................................................... 509
CSCub48124 - EIR Selection for roaming subscribers ................................................... 511
Feature Changes ........................................................................................................ 511
Command Changes ..................................................................................................... 511
CSCuc21648, CSCuc69746, CSCud12642 - Support higher than 16 Mbps bit rate flag in 3G S4-SGSN 513
Feature Changes ........................................................................................................ 513
Command Changes ..................................................................................................... 513
Performance Indicator Changes .................................................................................... 513
CSCuc90461 - Support DSCP marking on SGSN Diameter interfaces (S6d & S13) .... 514
Feature Changes ........................................................................................................ 514
CSCud12642 - [15.0] Support per RNC level bit rate capping at S4-SGSN .................... 515
Feature Changes ........................................................................................................ 515
CSCud64147 - SGSN shall provide bulk statistics support for LCS-MAP counters ....... 515
Performance Indicator Changes .................................................................................... 515
CSCud69746 - Support S4 interface for non EPC devices ............................................ 516
Feature Changes ........................................................................................................ 516
Command Changes ..................................................................................................... 516
Performance Indicator Changes .................................................................................... 516
CSCue32234 - [S4-SGSN] UE-AMBR override from local config shall be supported ... 518
Feature Changes ........................................................................................................ 518
Command Changes ..................................................................................................... 518
CSCue97071 - CLI to choose MCC, MNC coding in hex or dec for DNS FQDN .................................. 519
  Feature Changes .............................................................................................................. 519
  Command Changes ........................................................................................................... 519
  Performance Indicator Changes ....................................................................................... 520
CSCug56288, CSCun89857, CSCun41909 - EIR IMSI Field in IMEI Check .............................. 521
  Feature Changes .............................................................................................................. 521
  Command Changes .......................................................................................................... 521
  Performance Indicator Changes ....................................................................................... 522
CSCug97812 - Lock Peer-Server Point/Process (PSP) ............................................................. 522
  Feature Changes .............................................................................................................. 522
  Command Changes .......................................................................................................... 522
CSCuh31686 - Authentication vector management in S4 SGSN ............................................ 523
  Feature Changes .............................................................................................................. 523
  Command Changes .......................................................................................................... 523
CSCuh57775 - Common Routing Area for 2G and 3G ............................................................ 524
  Feature Changes .............................................................................................................. 524
  Command Changes .......................................................................................................... 525
  Performance Indicator Changes ....................................................................................... 525
CSCui71700 - Inclusion of CC17 and CC25 for RANAP redirection ........................................ 527
  Feature Changes .............................................................................................................. 527
  Command Changes .......................................................................................................... 528
  Performance Indicator Changes ....................................................................................... 528
CSCui70597 - Support ‘Homogenous Support of IMS Voice over PS Sessions’ indication in ULR message .................................................. 530
  Feature Changes .............................................................................................................. 530
CSCui70624 - Support Terminating-Access Domain Selection (T-ADS) data retrieval .......... 530
  Feature Changes .............................................................................................................. 530
CSCui76698 - Message aggregation between linkmgr/gbmgr to sessmgr should be automated .................................................. 531
  Feature Changes .............................................................................................................. 531
  Command Changes .......................................................................................................... 531
CSCui04175 - S4-SGSN to support R11 agreed CR to avoid SRVCC race condition ............... 531
  Command Changes .......................................................................................................... 531
CSCui66952 - 2G/3G new counter to measure failure for IMSI identity request .................... 532
  Feature Changes .............................................................................................................. 532
  Performance Indicator Changes ....................................................................................... 532
CSCum52817 - Do Not establish RAB even if ASI bit is set .................................................... 533
  Feature Changes .............................................................................................................. 533
  Command Changes .......................................................................................................... 534
  Performance Indicator Changes ....................................................................................... 534
CSCum53036 - SGW/PGW host names can be displayed in show sub sgsn-only full o/p ........ 534
  Performance Indicator Changes ....................................................................................... 534
CSCum56947 - Configuration to enable sending extended MBR for UL/DL ......................... 535
  Feature Changes .............................................................................................................. 535
  Command Changes .......................................................................................................... 535
CSCum56967 - Security Issue - Encryption on SGSN level .................................................... 536
  Feature Changes .............................................................................................................. 536
  Command Changes .......................................................................................................... 536
  Performance Indicator Changes ....................................................................................... 537
CSCum69971 - Modify pdp context reject cause different in 2g and 3g for same scenario ...... 537
  Feature Changes .............................................................................................................. 537
CSCum69981 - change in ‘prefer subscription-interface’ in cc profile is not working .............. 537
  Feature Changes .............................................................................................................. 537
CSCum94531 - Handle negative scenarios in MAP ................................................................ 538
  Feature Changes .............................................................................................................. 538
CSCun09183 - SGSN should not cleanup the subscriber when XID exchange times out ......... 538
Feature Changes ........................................................................................................ 538
CSCun13035 - Detach request is not triggered in following scenario ................... 539
Feature Changes ........................................................................................................ 539
CSCun22801 - In GPRS-Service 'No GMM IMPLICITE-DETACH-INDICATION' should be Added 540
Feature Changes ........................................................................................................ 540
CSCun69966 - Need support to clear RLF context level statistics by RLF framework 540
Feature Changes ........................................................................................................ 540
Command Changes ..................................................................................................... 540
CSCzn60387 - [S4-SGSN] S4-SGSN shall support topology based SGW selection 541
Feature Changes ........................................................................................................ 541
Command Changes ..................................................................................................... 542
CSCzn80731 - Ignoring PDP Inactivity configuration for one or more IMEIs .......... 543
Feature Changes ........................................................................................................ 543
Command Changes ..................................................................................................... 543
Performance Indicator Changes .................................................................................. 543

S-GW Changes in Release 16 ....................................................................................... 545
S-GW Enhancements for 16.5 ..................................................................................... 546
S-GW Enhancements for 16.4 ..................................................................................... 547
CSCup48554, CSCuq10884 - SGW should allow partial context Replacement 547
Feature Changes ........................................................................................................ 547
Performance Indicator Changes .................................................................................. 548
S-GW Enhancements for 16.3 ..................................................................................... 549
S-GW Enhancements for 16.2 ..................................................................................... 550
CSCuo09385 - S-GW session recovery not working post unplanned Demux MIO swover 550
Feature Changes ........................................................................................................ 550
S-GW Enhancements for 16.1 ..................................................................................... 552
CSCui86237 - Inaccurate SGW session stats on standby ASR 552
Feature Changes ........................................................................................................ 552
CSCul24516 - show sub subsystem stats incorrect.................................................. 553
Feature Changes ........................................................................................................ 553
Performance Indicator Changes .................................................................................. 553
CSCuo09385 - SGW session recovery not working post unplanned Demux MIO swover 554
Feature Changes ........................................................................................................ 554
S-GW Enhancements for 16.0 ..................................................................................... 555
CSCug83805 - InTracer Support: Auto and more simultaneous traces - S-GW 555
Feature Changes ........................................................................................................ 555
CSCuh25810 - SGW Session Idle Timer ................................................................ 556
Feature Changes ........................................................................................................ 556
Command Changes ..................................................................................................... 557
CSCuh35193 - SGW ASSERT removal .................................................................... 558
Feature Changes ........................................................................................................ 558
S-GW Schema ............................................................................................................. 558
Performance Indicator Changes .................................................................................. 558
CSCuh71727, CSCui42572 - Error response handling at SGW 559
Feature Changes ........................................................................................................ 559
Command Changes ..................................................................................................... 559
CSCui04167 - PGW LORC mechanism for subscriber billing .................................... 560
Feature Changes ........................................................................................................ 560
Performance Indicator Changes .................................................................................. 561
CSCui04214 - Dedicated bearer timeout action ....................................................... 561
Feature Changes ........................................................................................................ 561
S-GW Schema ............................................................................................................. 563
CSCui21603 - SGW Honor ingress & egress DSCP & Support DSCP marking @ APN profile 563
Feature Changes ........................................................................................................ 563
## Contents

- Command Changes ................................................................. 564
- Performance Indicator Changes ............................................. 564
- CSCui21610 - Dropped call counters granularity .......................... 565
- Feature Changes .................................................................. 565
- Performance Indicator Changes ............................................. 565
- CSCui37794, CSCui47671 - ULI inclusion cond during Service Request procedure when ISR is active Feature Changes ............................................. 574
- CSCui37806 - Suspend Notification/Acknowledge message in SGSN pool Feature Changes ............................................. 574
- CSCui37810, CSCui47711 - PGW restoration upon PGW failure w/o restart Feature Changes ............................................. 574
- CSCui47671 - ULI inclusion cond during Service Request procedure when ISR is active Feature Changes ............................................. 575
- CSCui37800, CSCui47691 - Adding a Cause Value in Delete Session Request message Feature Changes ............................................. 576
- CSCui70609 - [15.0]multi-access keyword under apn-profile to be concealed/removed Feature Changes ............................................. 576
- CSCui92670 - VOLTE: GTPU service to reserve bind addresses for VOLTE data bearers Feature Changes ............................................. 576
- CSCui95971, CSCuj13956 - Rel10 Compliance for SGW-CDRs Feature Changes ............................................. 577

### SNMP MIB Changes in Release 16 ........................................ 579

- SNMP MIB Object Changes for 16.5 ........................................ 580
- New SNMP MIB Objects .......................................................... 580
- Modified SNMP MIB Objects .................................................... 580
- Deprecated SNMP MIB Objects .............................................. 580
- SNMP MIB Alarm Changes for 16.5 ........................................ 581
- New SNMP MIB Alarms .......................................................... 581
- Modified SNMP MIB Alarms .................................................... 581
- Deprecated SNMP MIB Alarms .............................................. 581
- SNMP MIB Conformance Changes for 16.5 ............................ 582
- New SNMP MIB Conformance ................................................ 582
- Modified SNMP MIB Conformance ........................................ 582
- Deprecated SNMP MIB Conformance .................................... 582
- SNMP MIB Object Changes for 16.4 ........................................ 583
- New SNMP MIB Objects .......................................................... 583
- Modified SNMP MIB Objects .................................................... 583
- Deprecated SNMP MIB Objects .............................................. 583
- SNMP MIB Alarm Changes for 16.4 ........................................ 584
- New SNMP MIB Alarms .......................................................... 584
- Modified SNMP MIB Alarms .................................................... 584
- Deprecated SNMP MIB Alarms .............................................. 584
- SNMP MIB Conformance Changes for 16.4 ............................ 585
- New SNMP MIB Conformance ................................................ 585
- Modified SNMP MIB Conformance ........................................ 585
- Deprecated SNMP MIB Conformance .................................... 585
- SNMP MIB Object Changes for 16.3 ........................................ 586
- New SNMP MIB Objects .......................................................... 586
- Modified SNMP MIB Objects .................................................... 586
- Deprecated SNMP MIB Objects .............................................. 586
- SNMP MIB Alarm Changes for 16.3 ........................................ 587
- New SNMP MIB Alarms .......................................................... 587
- Modified SNMP MIB Alarms .................................................... 587
- Deprecated SNMP MIB Alarms .............................................. 587
System Changes in Release 16

System Changes in Release 16

SNMP MIB Conformance Changes for 16.3
  New SNMP MIB Conformance
  Modified SNMP MIB Conformance
  Deprecated SNMP MIB Conformance

SNMP MIB Object Changes for 16.2
  New SNMP MIB Objects
  Modified SNMP MIB Objects
  Deprecated SNMP MIB Objects

SNMP MIB Alarm Changes for 16.2
  New SNMP MIB Alarms
  Modified SNMP MIB Alarms
  Deprecated SNMP MIB Alarms

SNMP MIB Conformance Changes for 16.2
  New SNMP MIB Conformance
  Modified SNMP MIB Conformance
  Deprecated SNMP MIB Conformance

SNMP MIB Object Changes for 16.1
  New SNMP MIB Objects
  Modified SNMP MIB Objects
  Deprecated SNMP MIB Objects

SNMP MIB Alarm Changes for 16.1
  New SNMP MIB Alarms
  Modified SNMP MIB Alarms
  Deprecated SNMP MIB Alarms

SNMP MIB Conformance Changes for 16.1
  New SNMP MIB Conformance
  Modified SNMP MIB Conformance
  Deprecated SNMP MIB Conformance

SNMP MIB Object Changes for 16.0
  New SNMP MIB Objects
  Modified SNMP MIB Objects
  Deprecated SNMP MIB Objects

SNMP MIB Alarm Changes for 16.0
  New SNMP MIB Alarms
  Modified SNMP MIB Alarms
  Deprecated SNMP MIB Alarms

SNMP MIB Conformance Changes for 16.0
  New SNMP MIB Conformance
  Modified SNMP MIB Conformance
  Deprecated SNMP MIB Conformance

System Changes in Release 16

CSCuh81020 - [Ares] 'Boost' EM (Exact Match) Flow enhancements: NPUMGR
  Feature Changes

CSCuo50178 - Need IPv6 support in crashd to send a full core file to crashlog server
  Feature Changes

CSCuo50183 - Need IPv6 support in syslog/evlogd for logging events in syslogd server
  Feature Changes

CSCuo84086 - IPv6 support for NTP
  Feature Changes

CSCuo84268 - show egtpc peers needs to be added to the SSD
  Feature Changes

CSCup68502 - Software version data should be consistent across prime network

Release Change Reference, StarOS Release 16
Feature Changes ........................................................................... 608
CSCug91637 - FTP server with ipv6 is not working.......................... 608
Feature Changes ........................................................................... 608
CSCug28805 - ICSR failover resulted in loss of PCRF binding........... 608
Feature Changes ........................................................................... 608
Command Changes ........................................................................ 608
System and Platform Enhancements for 16.1.................................. 610
CSCug23975 - VoLTE: Prioritized handling of VoLTE/Emergency calls 610
Feature Changes ........................................................................... 610
CSCuh25721 - LAG CLI Enhancements........................................... 610
Feature Changes ........................................................................... 610
Performance Indicator Changes .................................................... 610
CSCul69462 - Need a way to configure no-password user account ... 612
Feature Changes ........................................................................... 612
Command Changes ........................................................................ 612
CSCun71100 - show version changes needed for new version numbering scheme for 16.0 614
Feature Changes ........................................................................... 614
Performance Indicator Changes .................................................... 615
CSCuo70354 - Unable to set more than one BGP extended community using route-map 615
Feature Changes ........................................................................... 615
Command Changes ........................................................................ 616
CSCuo84001 - [ares] Need User configurable command to monitor FAP Egress drops .... 617
Feature Changes ........................................................................... 617
Command Changes ........................................................................ 617
CSCuo91363 - Non-Redundant MIO Failure recovery action upon initialization failure 618
Feature Changes ........................................................................... 618
System and Platform Enhancements for 16.0.................................. 619
CSCtr55441 - VoLTE related ICSR optimization............................... 619
Feature Changes ........................................................................... 619
CSCug23975 - VoLTE: Prioritized handling of VoLTE/Emergency calls 621
Feature Changes ........................................................................... 621
CSCuh25721 - LAG CLI Enhancements........................................... 622
Feature Changes ........................................................................... 622
Performance Indicator Changes .................................................... 622
CSCul69462 - Need a way to configure no-password user account ... 624
Feature Changes ........................................................................... 624
Command Changes ........................................................................ 624
CSCtr67709 - Configurable Subscriber State Management Audit Process 625
Feature Changes ........................................................................... 625
Command Changes ........................................................................ 625
CSCtw93119 - show rct stats should show cause of event................. 626
Performance Indicator Changes .................................................... 626
CSCua66992 - IKEv1/v2 ACL & Subscriber mode combo support .... 626
Feature Changes ........................................................................... 626
CSCua86606 - eXGW full support on ASR5500............................... 627
Feature Changes ........................................................................... 627
CSCuf60462 - Activity to Remove mallocs in IPsec code ............... 627
Feature Changes ........................................................................... 627
CSCug70348 - Allow comments in the configuration files ............... 627
Command Changes ........................................................................ 627
CSCug96855 - Multiple Traffic Selectors ....................................... 628
Feature Changes ........................................................................... 628
Command Changes ........................................................................ 628
Performance Indicator Changes .................................................... 629
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 16. 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>🔄</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>

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

Related Common Documentation

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and 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 *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 Software 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
- SCM 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 16

This chapter identifies accounting management features and functionality added to, modified for, or deprecated from AAA in StarOS 16 software releases.
AAA Enhancements for 16.4

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

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

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

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

---

**CSCus24059 - New dynamic dict for Customer**

**Applicable Products:** PDSN

**Feature Changes**

**New Dynamic Dictionary to Meet Customer’s Requirements**

New dynamic Diameter dictionary has been created without USER-EQUIPMENT-INFO AVP in CCR messages to meet customer’s requirements.

---

**CSCus33524 - New S6b Dict for Customer to support GTPv2_SUPPORTED in MIP6-Feature-Vector**

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

**Feature Changes**

**New Diameter Dictionary for S6b**

Customer-specific Diameter dictionary “aaa-custom20” has been defined to support GTPv2_SUPPORTED flag in MIP6-Feature-Vector AVP on S6b interface for SAE-GW. This support has been provided in order to be in compliance with 3GPP 29.273 v10.5.0.

**Previous Behavior:** S6b Diameter dictionary was configured with the CLI command “diameter authentication dictionary aaa-custom14”. The MIP6-Feature-Vector AVP parsed in this dictionary included only PMIP6_SUPPORTED flag.

**New Behavior:** S6b Diameter dictionary should be configured as “diameter authentication dictionary aaa-custom20” to support GTPv2_SUPPORTED flag in MIP6-Feature-Vector AVP.

**Important:** This behavior change is customer-specific.
CSCus59440 - Diameter : S6b Origin-Host AVP truncation

Applicable Products: P-GW, SAE-GW

Feature Changes

Change in Origin Host Configuration

**Previous Behavior:** Origin-Host AVP was capped at 63 characters in all application messages even though it was allowed to configure up to 255 characters through CLI.

**New Behavior:** Origin-Host AVP will now include the entire value configured through CLI, which is up to a maximum of 255 characters.

**Customer Impact:** Diameter messages may be received with longer Origin-Host AVP value by Diameter servers if configured.

Command Changes

`origin host`

This command allows the user to configure the host name up to a maximum of 255 characters.

`configure`

```
context context_name

diameter endpoint endpoint_name

    origin host host_name address ipv4/ipv6_address [ port port_number ] [ accept-incoming-connections ] [ address ipv4/ipv6_address_secondary ]

no origin host host_name address ipv4/ipv6_address [ port port_number ]
```

`end`
AAA Enhancements for 16.3

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

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

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

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

**CSCup75566 - Add CC-Group AVP in Gx Dictionary for Customer**

*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.

**CSCuq06614 - Radius AVP SN-Rad-APN-Name to be added in custom67**

*Applicable Products:* GGSN, P-GW

**Feature Changes**

**SN1-RAD-APN-Name AVP in custom67 for Access Accept Management**

The RADIUS AVP “SN1-RAD-APN-Name” is added as an optional AVP in RADIUS access accept message for custom67 dictionary. This AVP specifies the RADIUS returned APN name. SN1-RAD-APN-Name if present in RADIUS access accept message, will be used to configure the virtual APN.

If this AVP is not present in the Access Accept message or if the AVP value is invalid, the SGSN supplied APN value in create PDP context will be used for the session.

If the RADIUS returned APN Name is invalid, the call will be dropped. Also, SN1-VIRTUAL-APN-NAME is not sent in accounting message even if SN1-RAD-APN-Name is sent in access accept.
AAA Enhancements for 16.2

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

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

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

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

CSCui47290 - Display issue in 15.0 for cli show ims-authorization service name gx

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

**Feature Changes**

**Cosmetic Changes to the Display of** `show ims-authorization service name` and `show ims-authorization sessions full all` **Commands**

For a default configuration, the “`show ims-authorization service name <name>`” displays “Supported Features” as NA, “Reauth Trigger” as All/Not Enabled/None and “Custom Reauth Trigger” as None. These values will be displayed in single heading line. For a valid configuration, this show CLI command displays “Supported Features”, “Reauth Trigger” and “Custom Reauth Trigger” values in sub heading with multiple lines based on configuration.

Similarly, for a default configuration or when no events are received from messages, the “`show ims-authorization sessions full all`” CLI displays “Negotiated Supported Features” as NA, “Event Triggers”, “Event Report Indication” and “Local Policy Enabled Event Triggers” as None. These values will be displayed in single heading line.

For a valid configuration, this show CLI command displays “Negotiated Supported Features”, “Event Triggers”, “Event Report Indication” and “Local Policy Enabled Event Triggers” values in sub heading with multiple lines based on configuration/events received from messages.

CSCul07715 - ASR5000 sends CCR-T before CCA-U arrived for CCR-U

**Applicable Products:** P-GW

**Feature Changes**

**CCR-T Sent Before CCA-U Arrived for CCR-U**

**Previous Behavior:** CCR-T sent without waiting for CCA-U to come if the call was cleared and there was a pending CCA-U.
New Behavior: If call is cleared when there is a pending update, P-GW will wait for CCA-U to arrive or timeout to happen (whichever happens first).

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

CSCup22833 - [GGSN] SM not sending updated GBR to IMSA after QoS negotiation

Applicable Products: GGSN

Feature Changes

Display changes for APN AMBR and GBR

In this release, the “show ims-authorization sessions full” command displays “NA” for GBR values for non-GBR bearers and APN AMBR keyword has been added to the CLI display before printing the AMBR values.

CSCup49621 - Rf-Gy Synchronization Enhancements

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

Feature Changes

Rf-Gy Synchronization Enhancements

Previous Behavior: Once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U.
New Behavior: As part of this enhancement, containers are closed only after CCA-U is received successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

CSCup77319 - PGW: missing Framed-IPv6-Prefix/Interface-Id in RADIUS-acct

custom15

Applicable Products: P-GW

Feature Changes

New custom15 RADIUS Dictionary Attributes

The RADIUS AVPs “Framed-IPv6-Prefix” and “Framed-Interface-Id” are supported in custom15 RADIUS dictionary.

CSCuo03247 - update-dictionary-avps: Event Triggers by default w/o PCRF installation

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

Feature Changes

Support for Configurable Custom Reauth Event Triggers

The custom-reauth-trigger CLI command has been extended to support enabling or disabling the PCEF’s implicit event triggers. This CLI overwrites the previously configured triggers with the new event triggers. For example, if you have configured the following triggers – QoS change, UE IP address allocation, UE IP address release, preservation-changed, reactivation-changed, then the APN-AMBR modification failure and Resource modification request triggers should be configured. This operation will overwrite all previously configured triggers and will configure only new APN-AMBR modification failure and Resource modification request triggers. IMS Authorization service will send the implicit event trigger in CCR-U only when the trigger is enabled.

Command Changes

custom-reauth-trigger

This command has been extended to support additional keywords to selectively enable/disable the PCEF’s implicit event triggers.

configure

context context_name

ims-auth-service service_name

policy control

default custom-reauth-trigger


default custom-reauth-trigger


default custom-reauth-trigger

Notes:

- The keywords added to this command enable/disable these implicit event triggers — QoS change, UE IP address allocation, UE IP address release, Default EPS bearer QoS change, Resource modification request, APN-AMBR modification failure, Default EPS bearer QoS modification failure respectively. By default, all these implicit event triggers are enabled.

**CSCuo08909 - Charging QoS MBR values when QCI not included in QoS-Info from PCRF**

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

**Feature Changes**

**Updating Session QoS Information in Session Manager**

As part of this enhancement, the gateway nodes take into account the changed QoS values MBR UL and DL for the non-GBR bearer indicated by Bearer-Id value even if QCI AVP is not present inside QoS-Information AVP.
AAA Enhancements for 16.1

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

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

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

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

### CSCug72343 - Assumed Positive Stats in Bulkstats for the DIAMETER Interfaces

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

**Performance Indicator Changes**

**IMSA Schema**

To support assume positive statistics in Bulkstats for Gx interface, the following new bulk statistic variables are added to this schema.

- active-fallback – Current assume positive sessions on Gx interface
- total-fallback – Cumulative assume positive sessions on Gx

### CSCuh11035 - PDSN/PCEF Supports CCR format on Gx interface

**Applicable Products:** PDSN

**Feature Changes**

**Dictionary Changes to Support CCR Format on Gx**

To support accepting CCR messages on Gx interface, customer should configure the Diameter dictionary “dpcacustom28” in IMS Authorization Service configuration mode.

### CSCuh51213 - Always send Charging-Rule-Report AVP in RAA on Gx

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

**Dictionary Specific Changes to Allow Sending Charging-Rule-Report AVP in RAA**

- **Previous Behavior:** Earlier, Charging-Rule-Report AVP was not sent in RAA messages.
- **New Behavior:** The Charging-Rule-Report AVP will be sent in RAA messages for all the rules which were previously installed and the rules which were received in RAR messages for custom dictionary “dpca-custom24”.
- **Customer Impact:** This feature implementation impacts only dpca-custom24 dictionary.

**CSCui47290 - Display issue in 15.0 for cli show ims-authorization service name gx**

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

**Feature Changes**

**Cosmetic Changes to the Display of show ims-authorization service name and show ims-authorization sessions full all Commands**

For a default configuration, the “show ims-authorization service name <name>” displays “Supported Features” as NA, “Reauth Trigger” as All/Not Enabled/None and “Custom Reauth Trigger” as None. These values will be displayed in single heading line. For a valid configuration, this show CLI command displays “Supported Features”, “Reauth Trigger” and “Custom Reauth Trigger” values in sub heading with multiple lines based on configuration.

Similarly, for a default configuration or when no events are received from messages, the “show ims-authorization sessions full all” CLI displays “Negotiated Supported Features” as NA, “Event Triggers”, “Event Report Indication” and “Local Policy Enabled Event Triggers” as None. These values will be displayed in single heading line. For a valid configuration, this show CLI command displays “Negotiated Supported Features”, “Event Triggers”, “Event Report Indication” and “Local Policy Enabled Event Triggers” values in sub heading with multiple lines based on configuration/events received from messages.

**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”.

**CSCuj10006 - PGW not sending CCR-E to the OCS on receiving Trigger Type Grouped AVP**

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

Feature Changes

**Failure Handling for CCR-E Messages**

**Previous Behavior:** Earlier, there was no failure handling support for CCR-E messages (Event based Gy). Any failed CCR-E request was not retried to secondary server.

**New Behavior:** Failure handling for CCR-E is now supported and implemented as follows:
- Diabase Error - For Diabase error, Event-based Gy session will retry sending the CCR-E to configured secondary peer. If CCR-E fails with secondary peer, failure is ignored and the Event-based Gy session will continue to report any further updates.
- Tx timeout/ Response Timeout - On Tx timeout/ Response Timeout (which ever fires first) CCR-E will be retried to secondary peer. If CCR-E fails with secondary peer, failure is ignored and the Event-based Gy session will continue to report any further location updates.
• Result-Code Based Failure Handling - Failure Handling for only result-code 3002, 3004 and 3005 is supported. CCR-E message will be retried to secondary peer. If CCR-E fails with secondary peer, failure is ignored and the Event-based Gy session will continue to report any further location updates.

CSCuj53306 - Adding a new AVP on Gx interface - Service group QoS

Applicable Products: GGSN, P-GW

Feature Changes

Support for Service-Group-QoS AVP in Gx Dictionary

The Diameter dictionary “dpca-custom25” has been created and configured in the Policy Control Configuration mode to support the “Service-Group-QoS” AVP for Gx implementation.

CSCuj61923 - Extra CCR-E message being sent to the OCS

Applicable Products: GGSN, P-GW

Feature Changes

Change in Logic for Sending CCR-E for Event-based Charging

Previous Behavior: When event-based charging is active, CCR-E is generated for all the bearers in the case of initial call setup, location and timezone change triggers.

New Behavior: When event-based charging is active, CCR-E is generated only for default bearer.

CSCuI07715 - ASR5000 sends CCR-T before CCA-U arrived for CCR-U

Applicable Products: P-GW

Feature Changes

CCR-T Sent Before CCA-U Arrived for CCR-U

Previous Behavior: CCR-T sent without waiting for CCA-U to come if the call was cleared and there was a pending CCA-U.

New Behavior: If call is cleared when there is a pending update, P-GW will wait for CCA-U to arrive or timeout to happen (whichever happens first).
CSCum36361 - No CCR-T when diameter failover from primary to secondary diameter host

Applicable Products: P-GW, SAEGW

Feature Changes

Support for Dynamic Route Creation

Previous Behavior: Dynamic route was not added for server-initiated messages.
New Behavior: Dynamic route is now created when server-initiated messages are received in the Diameter failure handling scenario.

CSCun52379 - Redirection when RC4012 or RC4010 at MSCC level with FUI redirect

Applicable Products: GGSN

Feature Changes

Support for FUI Redirection for 4010/4012 Result Codes

In this release, FUI redirection will happen even when 4010/4012 result-codes are received in CCA-I or CCA-U at MSCC level.

CSCun85201 - Request new Vendor-Id for Race Condition

Applicable Products: GGSN, P-GW

Feature Changes

Modifications to Race-Condition Feature Implementation

Previous Behavior: The gateway never advertised support of Pending Transactions (PT) feature in CCR-I as the Race condition feature was customer-specific i.e. applicable only to dpca-custom8 dictionary.
New Behavior: The gateway advertises the support of PT in CCR-I when “encode-supported-features pending-transactions” CLI command is configured.
The gateway will send 4198+ Cisco Vendor Id in RAA if CCR and RAR cross on wire.

CSCuo97456 - CC-Service-Specific-Units Avp getting update for a dynamic rule

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

Change in CC-Service-Specific-Units AVP Value for Dynamic Rules

CC-Service-Specific-Units AVP is applicable only for static and predefined rules. Ideally for a dynamic rule, there is no way to specify the charge-unit value and CC-Service-Specific-Units should not be updated.

Previous Behavior: CC-Service-Specific-Units AVP was updated for all rules irrespective of the charge-units value.

New Behavior: The CC-Service-Specific-Units AVP is not updated for any of the rules when the charge-units is set to a non-zero value. For dynamic rule scenarios, this AVP should be set as 0.

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

CSCup49621 - Rf-Gy Synchronization Enhancements

Applicable Products: P-GW

Feature Changes

Generation of Rf Trigger on CCA-U Arrival

Previous Behavior: Once a CCR-U was sent out over Gy, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U.

New Behavior: Rf trigger will be sent only after receiving CCA-U message.

CSCup59675 - gtpp push-to-active feature password shown in plain text

Applicable Products: GGSN, P-GW, SAEGW, SGSN, S-GW
Feature Changes

Configuration Support for Encrypted URL

**Previous Behavior:** The `show configuration` command will display the `gtpp push-to-active` configuration in clear text.

**New Behavior:** A new keyword option “encrypted” has been added to the `gtpp push-to-active` command to support configuring the peer chassis URL in encrypted format.

The `show configuration` command will display the `gtpp push-to-active` configuration in encrypted format. The `show configuration showsecrets` command will display the `gtpp push-to-active` configuration in clear text.

**Customer Impact:** Additional support is available for configuring push-to-active url.

Command Changes

gtpp push-to-active

`encrypted` is a new keyword in this command to support configuring the peer chassis URL in encrypted format.

`configure`

gtpp push-to-active [ encrypted ] url url via-context context_name

`no gtpp push-to-active`

`end`

**Notes:**

- `[ encrypted ]` - Indicates that the URL is encrypted for security reasons.

**CSCup77319 - PGW: missing Framed-IPv6-Prefix/Interface-Id in RADIUS-acct custom15**

**Applicable Products:** P-GW

Feature Changes

**New custom15 RADIUS Dictionary Attributes**

The RADIUS AVPs “Framed-IPv6-Prefix” and “Framed-Interface-Id” are supported in custom15 RADIUS dictionary.
AAA Enhancements for 16.0

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

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

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

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

---

**CSCty15753 - Suppress USU from CCR for FUI/REDIRECT**

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

**Feature Changes**

**CLI-based Control for Suppressing USU in CCR for FUI Redirect/Restrict-access**

**Previous Behavior:** In Release 12.2, the gateway used to send FINAL in CCR-T even though there is no quota usage to be reported to OCS server when the MSCC is in FUI Redirect/Restrict-access state. But in Release 15.0 this behavior had changed and FINAL reporting was not sent.

**New Behavior:** The current implementation is to control the FINAL reporting by suppressing USU in CCR-T message when the MSCC enters into FUI Redirect/Restrict-access state and when there is no quota usage to be reported to the server.

The default behavior is to not send CCR-T with reporting reason as FINAL even when MSCC is in FUI Redirect/Restrict-access state and USU is zero.

**Important:** This default behavior is applicable to all dictionaries except for dcca-custom12 and dcca-custom13 dictionaries. In the case of dcca-custom12 and dcca-custom13, the FINAL reporting will always be sent in CCR-T even if MSCC is in FUI Redirect/Restrict-access and USU is zero.

**Command Changes**

```
diameter disable-final-reporting-in-ccru
```

This command is now obsolete and supported only for backward compatibility reasons. Release 16.0 and beyond, use `diameter msg-type { ccru|ccrt } suppress-final-reporting` command for this functionality.

```
configure
require active-charging
active-charging service service_name
```
credit-control

diameter disable-final-reporting-in-ccru

{ default | no } diameter disable-final-reporting-in-ccru
end

diameter msg-type

This is a new command introduced in the Credit Control configuration mode to suppress FINAL reporting in CCR messages when there is no quota usage to be reported to the OCS server and when the MSCC is in FUI Redirect/Restrict-access state.

configure

require active-charging

active-charging service service_name

credit-control

diameter msg-type { ccru | ccrt } suppress-final-reporting

[ no ] diameter msg-type ccru suppress-final-reporting
end

Notes:

- **ccru**: This keyword disables Immediate FINAL reporting for result code 4010/4012 in CCR-U message.
- **ccrt**: This keyword disables FINAL reporting in CCR-T for MSCC which are in no-quota and FUI Redirect/Restrict-access state

The default behavior is to not send CCR-T with reporting reason as FINAL even when MSCC is in FUI Redirect/Restrict-access state and USU is zero.

**Important**: This default behavior is applicable to all dictionaries except for deca-custom12 and deca-custom13 dictionaries. In the case of deca-custom12 and deca-custom13, the FINAL reporting will always be sent in CCR-T even if MSCC is in FUI Redirect/Restrict-access and USU is zero.

---

**CSCty34193, CSCtz85672, CSCun86025 - Rf-Gy Synchronization Enhancements**

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

**Feature Changes**

**Rf-Gy Synchronization Enhancements**
In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, older release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers “Service Data Volume Limit” and “Service Data Time Limit”. Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions.

If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

**Previous Behavior:** Earlier whenever the volume/time-limit event triggers are generated, ACR-Interims were sent out immediately.

**New Behavior:** Now, CLI configuration options are provided in policy accounting configuration to control the various RF messages (ACRs) triggered for sync on this feature. This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

**Command Changes**

`trigger-type`

This is a new command used to enable/disable the event triggers for Rf-Gy interaction.

```bash
configure

  context context_name

  policy accounting policy_name

    trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } } +

    { default | no } trigger-type

end
```

Notes:

- This CLI configuration will either enable PCEF to send an ACR-Interim immediately or cache the container records for reporting in a future transaction. If there is no such configuration for that event-trigger, then the ACR-Interims will be dropped.
- When the subscriber disconnects while in Assume Positive mode, then the CLI configuration enables the PCEF to send an ACR-Stop with PS-level change condition “Normal Release” and container level “Service Specific Unit Limit”. The presence of the “Service Specific Unit Limit” change condition at the container level
indicates to the OFCS that data has gone unreported on Gy. The change-condition at container level is only present if the keyword option `gy-sdf-unit-limit` is configured.

**Performance Indicator Changes**

**Diameter Accounting Schema**

This new statistic variable is added to the Diameter accounting schema to track the total number of ACR-STOP messages that are sent with the change-condition “SERVICE-SPECIFIC-UNIT-LIMIT”.

- `acr-stop-serv-sp-unit-limit`

**show diameter aaa-statistics**

These new fields are added to the output of the `show diameter aaa-statistics` command to track the total number of ACR-STOP messages that are sent with the change-condition “SERVICE-SPECIFIC-UNIT-LIMIT”.

- ACR-Stop Event Stats
  - Service-Sp-Unit-Limit

**CSCty98259 - OCS selection using field name Charging Characteristic**

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

**Feature Changes**

**Charging-Characteristic based OCS Selection**

**Previous Behavior:** Only one credit-control-group was allowed to be specified inside an APN.

**New Behavior:** APN configuration is extended to include the Charging-Characteristic (CC) preference for the credit-control-group. This APN configuration is also extended to allow configuring additional credit-control-groups for each of the CC values.

With this enhancement, the OCS selection can be done based on the CC value received via GTP request. The CC 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.

**Important:** A maximum of four credit-control-group charging-profile configurations can be possible inside one APN.

**Customer Impact:** Operator has the added flexibility now to choose different OCS charging servers based on their business logic. This could help multi-national operators to choose correct OCS servers based on countries for roaming subscribers.

**Command Changes**

`credit-control-group`
**AAA Changes in Release 16**

**AAA Enhancements for 16.0**

`cc-profile` is a new keyword in this command to specify the charging-characteristic preference for the credit-control-group.

```
class
    context context_name
    apn apn_name
        credit-control-group cc_group_name [ cc-profile cc_profile_index ]
        no credit-control-group cc_group_name [ cc-profile cc_profile_index ]
    end
```

Notes:
- `cc_profile_index` must be an integer from 0 through 15. Note that one charging-characteristic value can be mapped to only one credit-control-group inside one APN.
- With this enhancement, the OCS selection can be done based on the CC value received via GTP request.

**CSCtz62801, CSCtw75856, CSCty34184 - Processing Diameter Gx Messages in the order in which they were received**

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

**Feature Changes**

**Race Conditions and Parallel Processing**

Gx-based applications are vulnerable to certain race conditions (e.g. concurrent RAR/CCR). Enhancements are done on the Diameter protocol to deterministically handle the race conditions on Gx.

In a scenario wherein RAR is received while waiting for CCA-U, Gx application rejects RAR with Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION (4198). Though the PCRF does not support this functionality, the gateway will send the experimental result code (4198) if the CLI command “diameter encode-supported-features pending-transactions” is configured.

**Previous Behavior:** Currently, if PCEF receives a server initiated message while PCEF initiated message is still pending and no response was received for the message, the PCEF rejects the server initiated message with DIAMETER_UNABLE_TO_DELIVER or DIAMETER_UNABLE_TO_COMPLY. This causes the PCRF to reject/abort the procedure based on configuration.

**New Behavior:** As part of the enhanced behavior a new cause code DIAMETER_PENDING_TRANSACTION (4198) is supported by PCEF to respond to the server when a pending client initiated procedure exists. The out of order RAR message with session release cause is processed now.

Similarly, PCEF handles Experimental Result Code DIAMETER_PENDING_TRANSACTION (4198) whenever it is received from PCRF in CCA-U and will retry.

**Important:** This behavior change is currently applicable only to dpca-custom8 dictionary.
**Customer Impact:** If race conditions are not processed properly, it can lead to unpredictable behavior from each node, resulting in subscriber disconnection. With this feature, the outcome in such situation is deterministic and operator has the ability to influence the node behavior aligned with their policy.

**Command Changes**

`diameter encode-supported-features`

`pending-transactions` is a new keyword in this command to configure `pending-transactions` as part of supported features. This keyword addition is to handle race conditions on Gx i.e. process the Diameter messages in the order they are received.

`configure`

```plaintext`
context context_name
ims-auth-service service_name
policy-control
diameter encode-supported-features pending-transactions
no diameter encode-supported-features
end`
```

Notes:
- Currently only one pending transaction is supported. So, all other transactions (like handoffs, etc) while one is pending will be rejected.

`msg-type`

`max-transmissions` is a new keyword in this command to allow configuring the maximum CCR-U retry attempts when the experimental result code `DIAMETER_PENDING_TRANSACTION` (4198) is received from PCRF in CCA-U.

`configure`

```plaintext`
failure-handling-template FHTemplate_name
msg-type any failure-type diameter exp-result-code expresult_code action retry-and-terminate max-transmissions number-of-retries
end`
```

Notes:
- Maximum number of retries that can be configured is 5 and the default value for retries is 1. When max-retries are exhausted, session termination happens.

**Performance Indicator Changes**

**DPCA Schema**
To support race conditions and parallel processing, the following new bulkstat variables are added to this schema.

- pending-trans-rarsent
- pending-trans-ccarcvd

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

To determine the number of pending transaction indications detected by the PCEF per interface and per server, the following new fields have been added to the output of the `show ims-authorization policy-control statistics` command.

- Pending-Trans-Sent
- Pending-Trans-rcvd
- Retry same server

**show ims-authorization service name**

To determine the number of pending transactions detected by the PCEF per interface and per server, the following new field has been added to the output of the `show ims-authorization service name` command.

- pending-transactions - This field has been added under the category “Supported Features”.

**show ims-authorization servers ims-auth-service**

In support of this feature, the following new fields have been added to the output of this show command.

- Pending-Transactions
  - RAA sent
  - CCA rcvd

**CSCua25104 - Segmentation fault PC: [094f04e8/X] sn_diam_abort_message()**

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

**Feature Changes**

**Dropping off Corrupted Diameter Messages**

*Previous Behavior:* On receiving corrupt mandatory AVP, CCR-T was triggered immediately to terminate the call.

*New Behavior:* The message with corrupted AVP will be dropped completely and if no further message is received within the configured timer, failure handling will take place.

**CSCuc16278 - DPCA PCRF too busy counter getting incremented with wrong vendor id**

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

PCRF Too Busy Counter Incremented for Invalid Vendor ID

When PCRF sends Experimental Result AVP with an invalid Vendor ID, the DPCA statistics field “PCRF Too Busy” is getting incremented in “show ims-authorization policy-control statistics” command. There is no log or error printed by P-GW/HSGW in this scenario.

**Previous Behavior:** Vendor ID of Experimental Result AVP was not parsed and checked before incrementing any of the statistics in the “show ims-authorization policy-control statistics” command.

**New Behavior:** Vendor ID of Experimental Result AVP is now parsed and checked. In case of a Vendor ID mismatch, “Bad Exp Result Code” statistics will be incremented instead of “PCRF Too Busy” field. Corresponding logs are also added.

CSCud06768 - OCS/CCF address not displayed in show ims-authorization sessions full all

Applicable Products: GGSN

Feature Changes

Display Changes to show ims-authorization sessions full all Command

In this release, both primary and secondary OCS and CCF information such as Hostname, Port and Protocol are removed from the output of show ims-authorization sessions full all command. Also when the downgrade occurs it will not be present and will be shown as NA.

Performance Indicator Changes

show ims-authorization sessions full all

The following fields are removed from the output of this show command:

- Primary OCS
  - Hostname
  - Port
  - Protocol
- Secondary OCS
  - Hostname
  - Port
  - Protocol
- Primary CCF
  - Hostname
  - Port
- Protocol
- Secondary CCF
- Hostname
- Port
- Protocol

CSCud32573 - All Diameter Result Code 2xxx to be interpreted as success

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

**Feature Changes**

**Interpreting All Diameter Result Code 2xxx as Success**

Currently, only result codes 2001 and 2002 are interpreted as success result codes by DCCA implementation and any result codes above 2002 would result in invoking CCFH configuration. As per RFC 3588, all 2xxx result codes are to be interpreted as success. DCCA implementation of 2xxx result code interpretation is now compliant to RFC 3588.

**Previous Behavior:** In DCCA only 2001 and 2002 were treated as success result codes. All other Diameter Result Codes in the range of 2000 to 2999 received at command level in CCA message were terminated with cause as “Diameter_Bad_Answer” even if the RFC 3588 defined the Result Code 2xxx as “success” Result Code.

**New Behavior:** As part of this enhancement, all Result Codes in the range of 2000 to 2999 are considered as “success” both at command level and MSCC level. The same behavior is applied for Result-Code AVP sent both at command level and at MSCC level.

To know the CCA success count, a new field “Result Code 2xxx” is added to the `show active-charging credit-control statistics group` command output and the same is added under bulkstats as well.

**Customer Impact:** This helps the operator to implement different charging logic in the OCS server depending on different business logics.

**Performance Indicator Changes**

**DCCA Group Schema**

The following new bulkstats variable has been added to track the total number of CCA Result-Codes that are received in range of 2000 and 2999 at command level.

- cca-2xxx-rc

`show active-charging credit-control statistics group default`

To know the CCA success count, the following new field has been added to the output of this show command under “CCA Result Code 2xxx Stats”:

- Result Code 2xxx
CSCud42899, CSCui44116 - PCEF supervision/maintenance bulkstats

Applicable Products: GGSN, P-GW

Feature Changes

DCCA Supervision/Maintenance Stat Counters

To support some of the customer requested KPIs, new counters have been added for counting the NULL quota and HTTP redirections. These additional KPIs can be used for measuring the performance of the Gy interface.

Performance Indicator Changes

DCCA Group Schema

To support some of the customer requested KPIs, the following new bulkstat variables are added for the Gy interface.

- mscc-gsu-null-grant
- mscc-fui-redirect

IMSA Schema

To support some of the customer requested KPIs, the following new bulkstat variables are added for the Gx interface.

- dpca-total-ims-auth-fh-triggered

show bulkstat variables dcca-group

The following new bulkstat variables are appended to the show command.

- mscc-gsu-null-grant
- mscc-fui-redirect

show active-charging credit-control statistics group default

As part of this enhancement, new statistics which count the total number of null quota granted, and the total number of HTTP redirection (FUI redirect) are added under credit-control group level.

- MSCC GSU Null Grant
- MSCC FUI Redirect

show ims-authorization policy-control statistics

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

- Total FH Triggered
CSCue51208, CSCue68211, CSCue68228, CSCue68231, CSCui08926 - support for SN-Transparent-Data on Gx, Gy and CDRs - IPSG

Applicable Products: GGSN, IPSG

Feature Changes

Support for SN-Transparent-Data AVP on Gy

With this enhancement, the AVPs “SN-Transparent-Data” and “Vlan-Id” will be sent over Gy Interface in the Credit-Control-Request message. Any change in SN-Transparent-Data AVP will not be triggering an update, and the updated values will be reported during the next CCR-Request.

The SN-Transparent-Data and VLAN-Id AVPs will be populated by ECS, and DCCA simply reads these values. These AVPs will be sent in CCR requests, only if these are present in the dictionary used. Since there is no custom dictionary, Dynamic-Dictionary feature is used. So, a Dynamic-Dictionary based on dcca-custom8 is constructed with these AVPs and added to the CCR message.

CSCue68677 - include Framed-IPv6-Prefix AVP in custom43 Radius dictionary

Applicable Products: GGSN, P-GW

Feature Changes

Support for Framed-IPv6-Prefix AVP in custom43 RADIUS Dictionary

With this release, Framed-IPv6-Prefix AVP will be included in Accounting-Start messages in custom43 RADIUS dictionary for P-GW IPv6 calls.

CSCuf56984 - Gx-Support for Flow-Direction AVP - Bidirectional(3) required

Applicable Products: GGSN, P-GW

Feature Changes

Support for BIDIRECTIONAL Flow-Direction

In this release, Flow-Direction AVP with the value set to BIDIRECTIONAL (3) is supported on Gx.

This feature should be enabled only after upgrading the active and standby chassis to the build having this feature. That is, PCRF should install dynamic rule with Flow-Direction “BIDIRECTIONAL (3)” only after active and standby chassis is upgraded to the same build which supports Flow-Direction AVP with the value BIDIRECTIONAL (3).
CSCuf81120, CSCug02124 - RADIUS AAA and CoA/DM Requirements for PGW/LMA

Applicable Products: P-GW

Feature Changes

Changes to RADIUS Dictionary Behavior

In this release, a new RADIUS dictionary “custom69” is defined to fulfill customer’s requirements. This dictionary includes standard and customized set of RADIUS accounting and authentication attributes to provide support for PMIP P-GW.

CSCug38375 - Backpressure CLI needs to be made non-hidden

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

Feature Changes

Support for Diameter Backpressure Stats

Previous Behavior: Currently, there is no way to check the value of maximum backpressure and the time at which the maximum backpressure has occurred for a particular or all AAA manager instance(s).

New Behavior: New show CLI commands are added to display the maximum backpressure at a particular AAA manager instance or at all instances, and the time stamp at which maximum backpressure was seen.

Command Changes

reset diameter aaa-statistics misc-data

This is a new command introduced in the Exec mode to reset the values of maximum backpressure and time for all AAA manager instances.

reset diameter aaa-statistics misc-data

show diameter aaa-statistics misc-data

misc-data is a new keyword in this command to display the highest backpressure statistics and the time at which it was seen for all AAA manager instances.

show diameter aaa-statistics misc-data [ instance instance_number ] [ | { grep grep_options | more } ]

Notes:

- instance instance_number: Displays the maximum backpressure statistics at a specified AAA manager instance.
  The AAA manager instance number must be an integer from 1 through 385 characters.
Performance Indicator Changes

`show diameter aaa-statistics`

To display the backpressure statistics, these new fields are added to the output of the `show diameter aaa-statistics` command.

- Backpressure Stats
  - Peer BP Queue Length
  - Peer BP Queue Insertions
  - Peer BP Queue deletions
  - Global BP Queue Length
  - Global BP Queue Insertions
  - Global BP Queue Deletions

`show diameter aaa-statistics misc-data`

To display the peer backpressure statistics, these new fields are added to the output of the `show diameter aaa-statistics` command.

- Facility
- Instance
- Max Peer BP Queue Length
- Max BP Time

**CSCug38387, CSCug72334 - New GX DIAMETER KPIs in CLI**

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

Feature Changes

**Result-code based Stats Support**

With this release, the following statistics are supported for Diameter Gx interface:

- Result-code based statistics/bulkstatistics for RAR
- New CCA stats/bulkstats when failure_cb is invoked
- New CCA stats/bulkstats if the unexpected CCA message is dropped
- Result Code 5xxx
- Other Result Code

**Customer Impact:** This helps the operator with more KPIs to monitor the performance of the interface.
Performance Indicator Changes

IMSA Schema

The following new bulkstats variables have been added to track the Gx Diameter KPIs.

- dpca-msg-ccainitdrop
- dpca-msg-ccaupddrop
- dpca-msg-ccafindrop
- dpca-msg-ccainitfail
- dpca-msg-ccaupdfail
- dpca-msg-ccafinfail
- dpca-peer-switch-tx
- dpca-peer-switch-rar
- dpca-total-ims-auth-flh-triggered
- dpca-imsa-raa-msg-success
- dpca-imsa-raa-msgerr-3xxx
- dpca-imsa-raa-msgerr-4xxx
- dpca-imsa-raa-msgerr-5xxx
- dpca-imsa-raa-msgerr-otherrescode
- dpca-imsa-bp-ccrimsgs
- dpca-imsa-bp-ccri-msg-failures
- dpca-imsa-bp-ccri-sessid-rcvry-failures
- dpca-imsa-bp-ccru-msgs
- dpca-imsa-bp-ccru-msg-failures
- dpca-imsa-bp-ccru-max-retrymsgs
- dpca-imsa-bp-ccru-dropped-msgs
- dpca-imsa-bp-ccru-sessid-rcvry-failures
- dpca-imsa-bp-cert-msgs
- dpca-imsa-bp-cert-msg-failures

show ims-authorization policy-control statistics

The following new fields have been added to the output of this show command to print the statistics for Diameter Gx interface.

- CCA-Initial Dropped
- CCA-Update Dropped
- CCA-Final Dropped
AAA Changes in Release 16

AAA Enhancements for 16.0

- CCA Parse Failure
- CCA-Initial Failure
- CCA-Update Failure
- CCA-Final Failure
- RAA Result Code Stats
- Result Code 2xxx
- Result Code 3xxx
- Result Code 4xxx
- Result Code 5xxx
- Other Result Code

CSCug38399 - Assumed Positive Stats for the DIAMETER Interfaces

Applicable Products: P-GW

Feature Changes

New Stats for Assume Positive

New bulkstats are introduced under the “show diameter aaa-statistics” command to capture the Assume Positive behavior.

show diameter aaa-statistics

To display the assume positive statistics, these new fields are added to the output of the show diameter aaa-statistics command.

- S6b Stats
  - Total Assume-positive

CSCug41175 - Gy & Gx - Length of the Redirect URL increase to 512

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

Feature Changes

Larger Redirect URL Length

At present each of the MSCCs were consuming 256 bytes of memory, irrespective of whether that has received a Redirect-URL or not. With this feature, this behavior is changed so that a maximum of 512 bytes of memory is allocated from memory pool, only when it is required. This helps reduce the memory usage for each of the MSCCs.
Important: This behavior change is currently applicable only to Gy interface, and not on Gx.

Previous Behavior: Currently, the maximum length of a FUI-Redirect-URL on the Gy interface is 256 characters.
New Behavior: The maximum length of Redirect URL is now increased to support up to 512 bytes.

Important: For a better memory management, a total of 512 bytes is allowed for the Redirect-URL, in which the last character will be used for the '0' char at the end of the string. So, a maximum of 511 characters can be possible in Redirect-URL.

Customer Impact: This helps the operator to have a large URL with additional parameters to be sent to AoC server.

CSCug70326, CSCun27457 - Gy Backpressure Enhancements

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

Feature Changes

Gy Backpressure Enhancement

This feature is extended to maintain a list of DCCA sessions that hit backpressure while creating a message i.e., backpressured list, eliminating the current polling procedure. This will maintain a single queue for all types of messages (CCR-I, CCR-U, CCR-T, CCR-E) that are backpressured. The messages will be sent in FIFO order (i.e., session which got first backpressed hit will be served first) from the queue.

After processing a session from the backpressure queue DCCA will check for the congestion status of the peer and continue only if the peer has empty slots in the outstanding message queue to accommodate further CCRs.

Previous Behavior: Currently, the gateway has a max-outstanding configuration at Diameter endpoint level to manage a number of messages that were waiting for response from OCS. When the max-outstanding was configured to a low value, then the frequency to be in congested state was very high. With polling procedure in DCCA application, CPU utilization was reaching very high.

New Behavior: All DCCA sessions associated with the CCR messages that are triggered BACKPRESSURE (when max-outstanding has been reached) will be queued in backpressure list which is maintained per ACS manager instance (credit-control) level.

This list will not have any specific configurable limits on the number of sessions that will be queued in it. This is because there is an inherent limit that is already present which is dependent on the number of subscriber/DCCA sessions.

With this new separate backpressured list, CPU utilization will come down under high backpressure case.

Performance Indicator Changes

DCCA Group Schema

The following new bulkstats variables have been added to track the total number of times backpressure got hit while creating CCR messages.

- ccri-bp-stats
• ccru-bp-stats
• ccrt-bp-stats
• ccrevent-backpressure

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

The following new fields have been added to the output of this show command to track the total number of times backpressure got hit while creating CCR messages.

- Backpressure Stats
  - CCR-I Messages
  - CCR-U Messages
  - CCR-T Messages
  - CCR-E Messages

**show active-charging credit-control statistics group default debug-info**

The following new bulkstats variables have been added to this show command to track the backpressure statistics.

- ccri_bp_retry_ontimer
- ccrt_bp_retry_ontimer
- ccre_bp_retry_ontimer
- ccri_success
- ccrt_success
- ccre_success
- add_into_bp_list
- remove_from_bp_list

**CSCug75153, CSCuh86476 - Additional set of KPIs for Gy assume positive**

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

**Feature Changes**

**Additional KPIs for Gy Assume Positive**

With Gy Assume Positive feature turned ON, it is difficult to debug what condition triggered Gy Assume Positive. In order to identify the scenarios, the following additional KPIs are supported:

- Number of sessions that have Gy Assume Positive triggered
- Error conditions that triggered Gy Assume Positive
- Time at which Gy Assume Positive was triggered for a session
- IMSI, MSISDN, APN, Session ID and Timestamp associated with the session (if possible without memory impact)
- CCR Message Type triggering Gy Assume Positive (CCR-I vs. CCR-U)

These KPIs are considered for bulkstats as well.

These additional KPIs help determine the reason Gy Assume Positive was triggered at the P-GW and in turn help resolve the problem and restore the network to normal operation. To get the details of sessions currently in OCS-unreachable (Gy assume positive) state, a new filter (credit-control ocs-unreachable) is added under the “show active-charging sessions” command.

**Command Changes**

**show active-charging sessions**

A new filter keyword “credit-control server-unreachable” has been added to this command to get the details of sessions that are currently in OCS-unreachable (Gy assume positive) state.

```
show active-charging sessions credit-control server-unreachable [ filter_keyword + ] [ | { grep grep_options | more } ]
```

Notes:
- This new filter can be used along with other filters like imsi and acsmgr instance to narrow down the results.

**Performance Indicator Changes**

**show active-charging sessions credit-control server-unreachable**

Changes have been made to “show active-charging sessions” CLI command to display the server-unreachable details for the session.

- SESSIONID
- CALLID
- IMSI/MSID
- IP
- USERNAME

**show active-charging sessions full credit-control server-unreachable**

The following new fields have been added to this command to capture the reasons of a session going in server unreachable state.

- Total Server Unreachable States Hit
  - Tx-Expiry
  - Response-TimeOut
  - Connection-Failure
  - Result-Code Based
- Server Unreachable Reason
CSCug78671, CSCui08938, CSCui08968 - support for SN-Transparent-Data on Gx, Gy and CDRs - GGSN

Applicable Products: GGSN, IPSG

Feature Changes

SN-Transparent-Data AVP on Gx, Gy and GGSN CDRs

SN-Transparent-Data AVP carries current PDP session information. Once the session specific information such as operator-id, GPS id, satellite-id, etc are made available to the gateway via RADIUS or PCRF interfaces, the same session information can be carried over to other interfaces such as Gx, Gy and Gz (eGCDR) for billing and charging purposes. Any change in SN-Transparent-Data will not be triggering an update, but the updated values will be reported during the next CCR-Request.

This feature is currently applicable to only GGSN and IPSG products and is available only in custom46 for eGCDR and dynamic-dictionary for Gy.

Previous Behavior: Earlier, r8-gx-standard dictionary was used for this requirement.

New Behavior: Now, the Diameter dictionary “dpca-custom22” is created based out of r8-gx-standard dictionary to support a new AVP “SN-Transparent-Data”. GGSN sends this new AVP along with ULI and Timezone in CCR messages to PCRF.

For this requirement on Gy interface, dynamic dictionary is created based on dcca-custom8 dictionary to support the new AVP “SN-Transparent-Data”. Similarly, for this requirement on Gz interface (for eGCDRs), GTPP dictionary “custom46” is newly added to support the new AVP “SN-Transparent-Data”.

Customer Impact: This feature helps the operator to do subscriber specific billing. By co-relating the same subscriber specific information across various interfaces, billing can be easily reconciled and charged to the subscriber accurately.

CSCuh24827 - Support new Interfaces for Tracing: Gy : GGSN/PGW/SAEGW

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

Feature Changes

Management Tracing for Gy Interface

Previous Behavior: Currently, tracing of subscriber sessions on Gy and Gz interfaces are not supported in GGSN, P-GW and S-GW products.

New Behavior: The “session trace” CLI command has been enhanced to support Gy and Gz interfaces while enabling management trace for GGSN, P-GW and S-GW products.

Command Changes

session trace

gy is a new keyword in this command to enable session tracing capabilities for Gy subscribers.
session trace subscriber network-element { mme | pgw | sgw | ggsn } interface gy imsi
imsi_id trace-ref id collection-entity ip_address

Notes:
- New bit-masks have been added for Gy interface for GGSN, P-GW, and S-GW network elements which will be set for the CLI.

CSCuh41778, CSCul85477 - Gx, T(Potentially re-transmitted message) Flag not sent on retrans

Applicable Products: P-GW

Feature Changes

Setting T Flag for Retransmissions

RFC indicates that the T bit has to be set when the message is retransmitted to an alternate server which is not being done in our chassis currently. To resolve this issue, a new CLI command is introduced at Diameter endpoint level so that the operators have the flexibility to expect the T bit or not based on it. A similar CLI is already present under CC-group.

Previous Behavior: Retry-bit (T-bit) was not set for retried messages.

New Behavior: CLI under Diameter endpoint can be used to set T-bit in a retried message.

Similar CLI is present under CC_group as well which when configured will take effect for Gy messages else endpoint configuration will be used.

With this feature turned on, the server can detect any duplicate/re-transmitted messages sent by Diameter clients or agents. Note that this feature is applicable to Gy and Rf messages as well.

Command Changes

app-level-retransmission

This is a new command added in the Diameter Endpoint Configuration mode to set T-bit in a retried Diameter message.

configure

context context_name
diameter endpoint endpoint_name

[ default | no ] app-level-retransmission { retain-e2e | set-retransmission-bit }

diameter endpoint endpoint_name

end

Notes:
- retain-e2e: Sends the same End-to-End Identifier for a retried Diameter message.
- set-retransmission-bit: Sets the retransmission bit for retried Diameter messages.
**CSCuh43130 - Server unreachable condition is hit without behavior trigger configured**

Applicable Products: GGSN, P-GW

**Feature Changes**

**Servers Unreachable Behavior for CCR-I Retried Message**

Server unreachable state is not hit for all dictionaries other than dcca-custom13 dictionary and the call is terminated when Diameter Result Codes like 3002, 3004, 3005 and 4003 are sent from OCS with server-unreachable configuration having only default behavior triggers. Also, the Assume Positive state is entered only when there is an exact matching behavior trigger for the retried messages.

**Previous Behavior:** When the first CCR message matches the servers unreachable behavior trigger, the server unreachable mode is entered even when the retried message does not meet the behavior trigger. Failures for retried CCR messages were not considered for entering into server unreachable state and the CCFH action was applied for them. Server Unreachable was hit for the above mentioned result codes even without the corresponding behavior trigger for dictionaries other than dcca-custom13.

**New Behavior:** If the retry happens due to server unreachable or normal failure handling or failure handling template, the servers unreachable state is hit only when there is an exact matching behavior trigger applicable for the retried message. Server unreachable is not hit for the above mentioned result codes without the corresponding behavior trigger for dictionaries other than dcca-custom13.

**CSCuh53213 - PGW should not generate Rf records if UE is IDLE & not tx any data**

Applicable Products: P-GW

**Feature Changes**

**Cessation of Rf Records When UE is IDLE**

**Previous Behavior:** When the UE was determined to be in IDLE state and not sending any data, the P-GW generated Rf records. During this scenario, the generated Rf records did not include Service Data Containers (SDCs).

**New Behavior:** With this release, the Rf records are not generated in this scenario. Configuration options are provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and when no data is transferred.

**Command Changes**

`session idle-mode`

This is a new command used to control the behavior of whether to send or suppress the ACR-Interims when the UE is idle.
context context_name

policy accounting policy_name

[ default | no ] session idle-mode suppress-interim
end

CSCuh75147 - LP support for APN AMBR failure/Default EPS bearer failure

Applicable Products: P-GW

Feature Changes

Local Policy Configurations for Handling APN AMBR Failure/Default EPS Bearer Failure

As part of this feature, Local Policy engine now supports two new event triggers “APN AMBR Modification failure” and “Default EPS Bearer Modification failure. These event triggers are hit when MME/ePDG rejects a PCRF/Local Policy authorized QoS and informs the same to P-GW.

In order to support the new event triggers at Local Policy, two new event CLIs are added at Local Policy engine. These CLIs will be used by Local Policy engine to map any incoming event from IMSA module. If IMSA posts a Local Policy event for one of these two new event triggers, Local Policy Engine does a rule match and selects the appropriate rule entry line inside eventbase configuration. After selecting the appropriate rule, Local Policy engine installs the actions configured against the rule entry.

Configuration changes to support the two new events are added. New show CLIs are added which would indicate the number of times Local Policy Engine received the apn ambr modification failure event/Default eps failure indication events.

Previous Behavior: Currently, these triggers are supported on Gx but not on local policy.

New Behavior: With this release, these triggers are extended to local policy as well.

Command Changes

rule

event apn-ambr-mod-failure and def-eps-bearer-qos-mod-failure are new keywords in this command to extend the support for the two event triggers to local policy.

configure

local-policy-service service_name

eventbase eventbase-name

rule priority priority [ event apn-ambr-mod-failure ] ruledef ruledef_name
actiondef actiondef_name

rule priority priority [ def-eps-bearer-qos-mod-failure ] ruledef ruledef_name
actiondef actiondef_name
no rule priority priority
end

Performance Indicator Changes

show local-policy statistics all

To support the new event triggers, these two new fields have been added to the output of this show command.

- APN-AMBR Mod Failure
- Def EPS bearer Qos Mod Failure

CSCuh75212 - Clean up of unused clis in Local Policy.

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

Feature Changes

Removal of Unused CLI Commands in Local Policy

The following unused CLI commands have been removed from the local policy configurations:

- activate-policy-group – activates a policy group
- create-bearer – Perform create bearer option
- deactivate-policy-group – deactivate a policy group
- delete-bearer – delete a bearer

Create an event base within local policy service

- pre-bearer-create
- subscription-profile-updated
- time-change

Adds a rule definition within local policy service

- cgi - Configure CGI
- ecgi - Configure ECGI
- sai - Configure SAI
- tai - Configure TAI
- timer - Configure a named timer variable

Performance Indicator Changes

show local-policy statistics
The following associated local-policy statistics are removed.

- **Action Statistics:**
  - Create Bearer
  - Create Bearer Success
  - Create Bearer failure
  - Delete Bearer
  - Delete Bearer Success
  - Delete Bearer failure
  - Activate Policy Grp
  - Activate PolicyGrp Grp Success
  - Activate PolicyGrp Grp failure
  - Deactivate PolicyGrp
  - Deactivate PolicyGrp Success
  - Deactivate PolicyGrp failure

- **Variable Matching Statistics:**
  - Timer
  - CGI
  - SAI
  - TAI
  - ECGI

### CSCuh75223 - Support for Local policy and PCRF together

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

### Feature Changes

**Support for Co-existence of Local Policy and PCRF**

**Important:** For this release, this feature is Lab/Trial Quality only.

In this approach, list of the event-triggers supported by the local-policy will be provided during the call establishment (New-call event). Whenever the event occurs, if the PCRF cannot handle that event and if the local-policy can handle that event, call will be continued with local-policy for that particular event. Whenever failure happens and local-fallback is configured, then the call will be continued with the local-policy (behavior will be the same as in 15.0 release).

Gateway can be configured to contact Local Policy for events like service flow detection/QoS Change and trigger CCR message to PCRF for events like RAT Change.
**Previous Behavior:** A call was associated with local policy only when the call was of type emergency or when a failure was detected in the PCRF connection and local-fallback was configured as failure-handling action. At a time, the call was associated with either PCRF or local-policy.

**New Behavior:** In this release, the calls can be associated with both PCRF and local-policy simultaneously. If the PCRF does not support an event-trigger, local-policy will be contacted (qos-change and default-eps-bearer-qos are supported).

Local-policy can be used to support dual-mode to provide the load balancing support for PCRF. Local-policy can also be used for providing the failure-handling support when PCRF is down or any failure is detected.

**Customer Impact:** This enhancement helps in reducing the traffic between the P-GW and PCRF and does not compromise on the use case the operator wants to apply. By sharing the load of PCRF with P-GW, PCRF can handle more number of new calls and thus improving the overall performance of the network.

**Command Changes**

```
associate local-policy-service

dual-mode is a new keyword in this command to allow both PCRF and local policy to work together.

configure

context context_name

ims-auth-service service_name

policy-control

associate local-policy-service service_name [ dual-mode ]

no associate local-policy-service end

Notes:
- The dual-mode keyword is configured to provide load balancing support for PCRF, and failure-handling support when PCRF is down or any failure is detected.

action

event-triggers is a new keyword variable in this command to enable the event triggers – Default EPS bearer QoS change event trigger and QoS change event trigger.

configure

local-policy-service service_name

actiondef actiondef_name

action priority priority event-triggers [ default-bearer-qos-change | qos-change ]

no action priority priority end
```
condition

*local-policy-mode* is a new keyword variable in this command to select different actions for different modes like local-policy only, dual-mode, and fallback mode for the same event.

```configure
local-policy-service service_name

ruledef ruledef_name

condition priority priority local-policy-mode [ fallback | dual-mode | lp-only ]

no condition priority priority

end```

Performance Indicator Changes

**show ims-authorization sessions full all**

To support the co-existence of PCRF and local policy, the following new field has been added to the output of the `show ims-authorization sessions full all` command.

- Local Policy Enabled Event Triggers

**show local-policy statistics all**

To support the co-existence of PCRF and local policy, the following new fields have been added to the output of the `show local-policy statistics all` command.

- Enable Event Trigger – This field has been added under the category “Local Policy statistics for Service”.
- Enable Event Trigger Failure – This field has been added under the category “Local Policy statistics for Service”.
- Enable Event Trigger Success – This field has been added under the category “Local Policy statistics for Service”.
- LOCAL POLICY MODE – This field has been added under the category “Variable Matching Statistics”.

**CSCuh86452 - Gx support for Assumed Positive Stats in CLI**

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

**Command Changes**

**show ims-authorization sessions**

Three new keywords `facility`, `local-sessions` and `remote-sessions` are added to this command to display the IMSA session level statistics including current number of local policy sessions and PCRF sessions.
show ims-authorization sessions [ facility sessmgr instance instance_no | local-sessions | remote-sessions ] [ | { grep grep_options | more } ]

Notes:

- **facility sessmgr instance instance_no**: Displays the IMS authorization sessions at the session manager instance level.
- **local-sessions**: Displays the IMS authorization sessions that are associated with local-policy.
- **remote-sessions**: Displays the IMS authorization sessions that are associated with PCRF.

**Performance Indicator Changes**

**show ims-authorization service statistics**

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

- Current Fallback Session
- Current PCRF Session

**CSCuh86548 - Gx: Backpressure CLI needs to be made non-hidden**

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

**Feature Changes**

**Support for Diameter Backpressure Stats**

**Previous Behavior**: Currently, there is no way to check the value of maximum backpressure and the time at which the maximum backpressure has occurred for a particular or all session manager instance(s).

**New Behavior**: New show CLI commands are added to display the maximum backpressure at a particular session manager instance or at all instances, and the time stamp at which maximum backpressure was seen.

**Command Changes**

**reset ims-authorization policy-control misc-info**

This is a new command introduced in the Exec mode to reset the values of maximum backpressure related information.

**reset ims-authorization policy-control misc-info max-backpressure { all | facility sessmgr instance instance_number }**

**show ims-authorization policy-control misc-info**

This is a new command introduced in the Exec mode to display the maximum backpressure message in a queue and the time when it was seen.

**show ims-authorization policy-control misc-info max-backpressure [ all | facility sessmgr instance instance_number ] [ | { grep grep_options | more } ]**
Notes:

- **all**: Displays the max-backpressure count among all active session manager instances.
- **facility sessmgr instance instance_number**: Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance.

The session manager instance number must be an integer from 0 through 10000000 characters.

**Performance Indicator Changes**

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

To display the backpressure statistics, these new fields are added to the output of this show command.

- Backpressure Stats
  - CCR-I Backpressure Stats
    - Messages
    - Failures
    - Sess-Id Recovery Failures
  - CCR-U Backpressure Stats
    - Messages
    - Failures
    - Max Retry
    - Dropped Messages
    - Sess-Id Recovery Failure
  - CCR-T Backpressure Stats
    - Messages
    - Failures
    - Sess-Id Recovery Failures

**show ims-authorization policy-control misc-info max-backpressure all**

To display the backpressure statistics, these new fields are added to the output of this show command.

- inst
- max
- current
- max-time
- start-monitoring-time
CSCuh86555 - Gy: Backpressure CLI needs to be made non-hidden

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

Feature Changes

Support for Backpressure Statistics

New CLI keyword is introduced at Exec mode which will display the maximum backpressure count and the time it was seen. This Exec CLI command will display session manager instance number, maximum backpressure count that happened on a particular session manager instance, current length of the backpressure list and the time at which maximum backpressure happened.

Command Changes

reset active-charging credit-control misc-info max-backpressure

This is a new command introduced in the Exec mode to get or reset the maximum back-pressure hit and the timestamp it reached the maximum value.

reset active-charging credit-control misc-info max-backpressure { all | facility sessmgr instance instance_number }

Notes:
- all: Displays the max-backpressure count from all active session manager instances.
- facility sessmgr instance instance_number: Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance.

The session manager instance number must be specified as a numerical value of 1 through 65535 characters.

show active-charging credit-control misc-info

This is a new command introduced in the Exec mode to display the maximum backpressure hit count for all active session managers.

show active-charging credit-control misc-info max-backpressure [ all | facility sessmgr instance instance_number ] [ | { grep grep_options | more } ]

Notes:
- all: Displays the max-backpressure count from all active session manager instances.
- facility sessmgr instance instance_number: Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance.

The session manager instance number must be specified as a numerical value of 1 through 65535 characters.

CSCui79823 - local issue for iRat from 4G to S4

Applicable Products: SAEGW
Feature Changes

APN AMBR Rule Matching During 4G to S4 SGSN Handoff

**Previous Behavior:** During 4G to 3G S4 SGSN handoff, APN AMBR was not sent. The local policy was not hitting this APN AMBR rule because no AMBR values have been requested in the Modify Bearer Request.

**New Behavior:** For 4G to S4 SGSN handoff, previously used APN AMBR values will be used in local-policy rule matching.

CSCuj38626 - [Paging] Reservation for radius & AAA attr for HNBGW GridId paging

**Applicable Products:** HNBGW

Feature Changes

New RADIUS AVP for Paging Support on HNBGW

In this release, a new RADIUS attribute “Paging-Grid-Id” has been introduced for grid based paging support in HNBGW.

This attribute provides the grid-Id of HNB used for Paging. This attribute will be sent from HMS to HNBGW in the Access-Accept message.

CSCuj70597, CSCuj42608, CSCuj63683 - Homogenous Support of IMS Voice over PS Sessions indication in ULR msg

**Applicable Products:** MME, SGSN

Feature Changes

Support for 'Homogenous Support of IMS Voice over PS Sessions' AVP

**Previous Behavior:** The MME supports the 'IMS Voice Over PS Sessions' indicator on a global basis. This is set as a global configuration under the Call Control Profile as part of the `network-feature-support-iec` command. This indicator allows the MME to indicate that 'IMS Voice Over PS' is supported in all TAs. However, there was no setting to indicate that IMS Voice Over PS was not supported in any TA.

**New Behavior:** The MME now can be configured to include the "Homogenous Support of IMS Voice over PS Sessions" AVP in the S6a Update-Location-Request messages to the HSS. This AVP will be sent with the value set to "Not Supported" or "Supported" based on the configuration. If not configured, the AVP will not be sent.

**Customer Impact:** This provides operators implementing VoLTE services the configurable capability to include these indications in ULR message towards the HSS.
CSCuj70624 - Support T-ADS Data Retrieval

Applicable Products: SGSN

Feature Changes

Support for Terminating-Access Domain Selection (T-ADS) Data Retrieval

Previous Behavior: SGSN does not support indication of T-ADS Data Retrieval in ULR message towards the HSS on S6d interface. Support for T-ADS Data Retrieval via IDR/IDA procedures on S6d interface is required.

New Behavior: SGSN now supports indication of T-ADS Data Retrieval in Supported-Features AVP of ULR message towards the HSS on S6d Interface. T-ADS data retrieval in IDR/IDA is supported.

CSCul34346 - Need Statistics to display the reason for fallback to local-policy

Applicable Products: P-GW

Performance Indicator Changes

show ims-authorization policy-control statistics

The following new fields are added to display the reason for fallback to local-policy.

- Local Fallback Cause Stats
  - Tx-expiry
  - Request-timeout
  - Diabase error
  - Result-code error

show ims-authorization service statistics

The following field is modified to display the reason for fallback to local-policy.

- CCR received - Changed as “CCR sent” under Local Fallback category

CSCul39688 - [samog] DER Flags and DEA Flags AVP support for STa interface.

Applicable Products: SaMOG

Feature Changes

New Diameter AVPs for Local Breakout Feature
In support of the Local Breakout feature for SaMOG, two new Diameter attributes "DER-Flags" and "DEA-Flags" are included in Diameter-EAP-Request (DER) and Diameter-EAP-Answer (DEA) messages. More specifically, these attributes are added under the AAA attribute "LTE_STa_Auth" in the RADIUS dictionary.

CSCul39695 - [samog] 3GPP-GPRS-Negotiated-QoSProfile addition in DEA and AAA message

Applicable Products: SaMOG

Feature Changes

Support for 3GPP-GPRS-Negotiated-QoS-Profile AVP in DEA and AAA

With this release, 3GPP-GPRS-Negotiated-QoS-Profile AVP is newly added and parsed in Diameter-EAP-Answer (DEA) and AA-Answer (AAA) messages.

CSCul68013 - IPSG: No ULI towards Gx in CCR-I with dictionary r8-gx-standard

Applicable Products: IPSG

Feature Changes

Dictionary based Encoding of ULI in CCR for WLAN

Previous Behavior: 3GPP-User-Location-Info (ULI) AVP was not encoded in CCR message for RAT Type WLAN (03).

New Behavior: 3GPP-User-Location-Info (ULI) AVP will be sent in CCR messages for WLAN too. This behavior is applicable to all Gx dictionaries except for r8-gx-standard and dpca-custom4.

CSCul96681 - pcrf_received qos is not recovering correctly

Applicable Products: GGSN, P-GW

Feature Changes

PCI and PVI Validation Checks at IMSA

Previous Behavior: IMSA was passing PCI and PVI values to session manager as sent from PCRF without any validations.

New Behavior: Per the 3GPP spec, Pre-emption-Vulnerability and Pre-emption-Capability values can be 0/1. If the PCI or PVI value is not 0 or 1, then IMSA will assign the default value as follows:

- Pre-emption-Capability = PRE-EMPTION_CAPABILITY_DISABLED (1)
• Pre-emption-Vulnerability = PRE-EMPTION_VULNERABILITY_ENABLED (0)

CSCum06052 - Degraded RAID failed after unexpected switchover as dirty degraded array

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

Feature Changes

RAID Recovery and Quarantine

Dirty degraded RAID can now be optionally recovered using the CLI command “quarantine” newly added in the HD RAID configuration mode.

Note that the Quarantine feature is only effective for platforms using RAID5.

Command Changes

quarantine

This is a new command used to recover and quarantine the dirty-degraded RAID,

configure

hd-raid

    quarantine [ mtime modified-within-minutes ] [ directory file-name ] [ limit limit-of-files ]

    [ default | no ] quarantine

end

Notes:

• modified-within-minutes specifies within how many minutes the file is modified to be considered suspects for quarantine, with range 0-60*24, where 0 means no files would be quarantined, default to 5.

• file-name specifies the directory name quarantined files are moved to, default to "lost+found".

• limit-of-files specifies the maximum number of files to quarantine, where 0 is unlimited and default to 3000 (which is 10 files per second during 5 min).

• “no quarantine” will turn off quarantine and let dirty degraded RAID fail just like before the feature was implemented.

• “default quarantine” will set quarantine options to default of no quarantine.

• Changing quarantine option from OFF to ON would restart RAID if RAID is not currently available, otherwise changes would only affect next restart of RAID.
CSCum44960 - Call gets established on receiving error result code from Gx server

Applicable Products: P-GW

Feature Changes

Result Code based Failure Handling

Previous Behavior: When error result code was received from PCRF and generic CCFH action had been configured like “failure-handling cc-request-type initial-request continue” then “retry and terminate” was not applied as a default action.

New Behavior: Now, Retry and terminate FH action will be taken even if result code based FH is not configured.

CSCum64825 - Segmentation Fault: acsmgr_dcca_message_cb

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

Feature Changes

Handling Corrupted Diameter Messages

Previous Behavior: On receiving corrupt mandatory AVP CCR-T was triggered immediately to terminate the call.

New Behavior: The message with corrupt mandatory AVP will be dropped and failure handling will take place after timeout.

CSCum72921 - Redirect-Host AVP support for Rf Interface

Applicable Products: GGSN, P-GW

Feature Changes

Support for Redirection on Rf Interface

Previous Behavior: Currently, Diabase level Redirection was not supported for Rf interface.

New Behavior: Redirection is enabled for Rf interface. The following AVPs are added in Rf standard and aaa-custom4 dictionaries.

- Redirect-Host
- Redirect-Host-Usage
- Redirect-Max-Cache-Time
CSCum75843 - Experimental Result code 5142 is populated in Result Code AVP

Applicable Products: GGSN, P-GW

Feature Changes

Parsing QCI Error Code in Experimental-Result-Code AVP

Previous Behavior: When QCI value was incorrect, the error code (5142) was reported in Result-Code AVP. This behavior is not in compliance with 3GPP specification.

New Behavior: When an incorrect QCI value is detected, the error code (5142) is now encoded and sent in Experimental-Result-Code AVP instead of Result-Code AVP.

CSCum88821 - Sig11: PC: [f7e37944/X] libc.so.6/__strncmp_sse4_2()

Applicable Products: GGSN, P-GW

Feature Changes

Error Logs in show configuration errors Command

Previous Behavior: No configuration errors or warning messages were displayed in the output of show configuration errors command when the same Diameter endpoint is configured in multiple IMS authorization services.

New Behavior: In this release, error message is displayed in the output of show configuration errors command when the user tries to configure an endpoint which is already configured in other IMSA service.

CSCum97722 - Unexpected resultcode value in RAA when invalid QoS is installed in RAR.

Applicable Products: GGSN, P-GW

Feature Changes

Unexpected Result Code Value in RAA when Invalid QoS is Installed

Previous Behavior: In case of parse error in QOS-Information, the QoS-Information was completely ignored without QCI and AMBR, and the value of Result Code in subsequent RAA was set as “DIAMETER_MISSING_AVP (5005)”. 

New Behavior: When an invalid QoS is installed in RAR, the QoS-Information is still ignored and the value of result code in RAA is not set as “DIAMETER_MISSING_AVP (5005)” but as "DIAMETER_INVALID_AVP_VALUE (5004)". Also, if Diameter result code is already populated with an error result code, then this will not be overwritten.
CSCun18463 - Gx: CCR-U for Revalidation_timeout sent even after disabling the trigger

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

Feature Changes

No CCR-U for Revalidation_timeout When Trigger is Inactive

Previous Behavior: CCR-U is triggered for Revalidation_timeout event trigger even if the trigger is disabled.
New Behavior: Now, CCR-U will not be sent for Revalidation_timeout if the trigger is not active.

CSCun34690 - IPSG sessions cleared with REAUTH_ADD_FAILURE upon CCA-u arrival on Gx

Applicable Products: IPSG

Feature Changes

QoS Validation based on QCI Type

Previous Behavior: IMS Authorization Service validated the guaranteed bit rate for both types of QCI i.e. non-GBR QCI and GBR QCI.
When QoS-Information is included in CCA-I, IMSA module validated the guaranteed bit rate for both non-GBR QCI & GBR QCI. If the validation is successful, then QoS is updated else the operation is rejected and a bad answer is sent to PCRF. Debug log is maintained and the call is dropped.
When QoS-Information is included in CCA-U, IMSA module validated the guaranteed bit rate for both types of QCI. If the validation is successful, then QoS should be updated else the operation is rejected and debug log is written.
New Behavior: Now, IMSA module will validate the guaranteed bit rate only for GBR QCI received from PCRF.
Whenever the IMSA module receives QoS-Information from PCRF and if it is a non-GBR QCI, then IMSA module does not validate the guaranteed bit rate.

CSCun51012 - Bulkstat variables to be added for Switches-Tx timeout, Switches-RAR ch

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

Performance Indicator Changes

IMSA Schema

The following new variables are added to support bulkstatistics for peer switches due to Tx timeout and peer switches due to change in peer after RAR received from a different peer.
• dpca-peer-switch-tx
• dpca-peer-switch-rar

CSCun62685 - CCR-U is retried even if server-retries configured as zero

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

Feature Changes

Behavioral Changes to Server Retry Configuration in OCS Unreachable State

Previous Behavior: When the CLI command “servers-unreachable ...” in the Credit Control Configuration mode was configured with server-retries as 0, CCR-U was retried one last time to confirm that the OCS is indeed unreachable.

But this was only done for the Interim-Volume scenario and it was against the configuration.

New Behavior: If no retries are configured for CCR-U volume-exhausted case, the server-unreachable-action will be taken immediately without any server retry.

CSCun89716 - Can't find time at which Gy assume positive was triggered for a session

Applicable Products: P-GW

Feature Changes

Gy Assume Positive Enhancements

With this release, a new field is introduced in the show active-charging sessions credit-control server-unreachable command to display the latest time at which Gy Assume positive got applied to a particular session on the system. The latest time is calculated across all instances of session manager.

If there is no session entering into Assume Positive mode from the time the chassis is booted, the time will not be displayed.

Performance Indicator Changes

show active-charging sessions credit-control server-unreachable

The following new field has been added to the output of this command to display the timestamp for the last Assume positive entered session.

• Timestamp of last session in server-unreachable state
Chapter 2
ADC Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from ADC in StarOS 16 software releases.
ADC Enhancements for 16.2

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

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

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

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

---

**CSCue79102 - skypeout detection required.**

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

**Feature Changes**

**Support for Voipout Sub-classification**

A new sub-classification “voipout”, for applications/protocols is supported in this release. The other supported sub-classification are audio, file-transfer, im, unclassified, video.

**Previous Behavior:** Skypeout traffic was classified as Skype-audio.

**New Behavior:** Skypeout application traffic detection support is added in this release. Skypeout calls are 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.

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.

```
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
CSCuo80798 - [P2P] CLI required for Audio/Video Duration Counter in p2p analyser

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

Feature Changes

CLI Support for Audio and Video Duration

As part of the Skypeout feature, the `show active-charging analyzer statistics` CLI command is enhanced to include voipout along with audio and video. CLI support is provided to update audio/video duration once the audio/video flow ends in P2P analyser statistics. A new keyword `duration` is added to provide the statistics for list of supported audio and video protocols from ADC plugin.

Previous Behavior: The audio/video duration details are updated in EDR and Bulkstats (Offline Charging). There was no CLI to check the audio/video duration in realtime.

New Behavior: CLI is added for audio/video duration.

Command Changes

`show active-charging analyzer statistics`

A new keyword `duration` is added to the `show active-charging analyzer statistics` CLI command to provide the statistics for list of supported audio and video protocols from ADC plugin.

```
show active-charging analyzer statistics name p2p [ duration [ audio { application p2p-audio-duration-list } | video { application p2p-video-duration-list } ] ]
```
ADC Enhancements for 16.1

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.

CSCuo58183 - [P2P] Bulkstats Counter Type shows Unknown

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

**Feature Changes**

**Counter Type Support for P2P Bulk Statistics**

In this release, statistic types — Counter, Gauge and Information are added for all bulk statistics in P2P Schema.

**Performance Indicator Changes**

**P2P Schema**

In this release, statistic types are added for all bulk statistics in P2P Schema.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Counter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>p2p-protocol</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-protocol-group</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-duration-name</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-duration-value</td>
<td>Counter</td>
</tr>
<tr>
<td>p2p-uplnk-bytes-name</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-uplnk-bytes-value</td>
<td>Counter</td>
</tr>
<tr>
<td>p2p-dwlnk-bytes-name</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-dwlnk-bytes-value</td>
<td>Counter</td>
</tr>
<tr>
<td>p2p-uplnk-pkts-name</td>
<td>Information</td>
</tr>
<tr>
<td>p2p-uplnk-pkts-value</td>
<td>Counter</td>
</tr>
<tr>
<td>p2p-dwlnk-pkts-name</td>
<td>Information</td>
</tr>
<tr>
<td>Variables</td>
<td>Counter Type</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>p2p-dwlnk-pkts-value</td>
<td>Counter</td>
</tr>
</tbody>
</table>
ADC Enhancements for 16.0

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.

**CSCuh13903, CSCul83184, CSCum23788 - P2P Counting License enforcement**

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

**Feature Changes**

**P2P Counting License Enforcement**

In this release, P2P counting license is added to the ECS counting license. This feature uses the framework of resource manager to enforce P2P license counting, and maintain a count of the number of active P2P sessions. When this count exceeds the P2P license limit, resource manager sends a message to each session manager saying no more new P2P sessions can be allowed. Once the count reaches below the license limit, it again sends a message to all session managers saying new P2P calls can now be allowed.

**Previous Behavior:** No enforcement support for P2P license counting.

**New Behavior:** Added support for P2P license counting enforcement. Bulk statistics are also added in the System schema in support of this feature.

**Performance Indicator Changes**

**System Schema**

The following bulk statistics are new and added in support of the P2P Counting License Enforcement feature.

- `sess-maxadc`
- `sess-maxadctime`
- `lic-adc`

**show resources session**

The following fields are added to the output of this command in support of the P2P Counting License Enforcement feature.

- P2P information:
• P2P Service:
  • In Use
  • Max Used
  • Limit
  • License Status

**show task info**

The following field is added to the output of this command in support of the P2P Counting License Enforcement feature.

• P2P sessions

**CSCuh88935 - P2P Ruledef optimization**

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

**Feature Changes**

**P2P Ruledef Optimization**

In this release, ADC rules will be optimized rules to reduce overhead while searching ADC rules during rule match.

**Previous Behavior:** For releases prior to 16.0, in case of ADC (P2P) flows, rule match happens for each and every packet in the flow. Rule match is a major performance overhead if more rules and ruledefs are configured by the operator. In case of ECSv2 ADC flows, the rule match tries to match the flow with the ruledef having the highest priority.

**New Behavior:** With this release, P2P rules are made optimized based on ECSv2 scoreboard approach. This will help in reducing overhead in brute force searching of ADC rule during rule match. If all the lines in a ruledef are marked “optimized” by an optimizer (any ECS optimizer/P2P optimizer), the entire ruledef becomes “optimized”.

**CSCum97670 - [SysTest] AssrtFailure at messenger/memacct.c:430 Function: free_acct()**

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

**Feature Changes**

**Error handling in P2P Plugin**

P2P Flow details will not be displayed if P2P Plugin is not loaded. An error message will be displayed for the `show active-charging subsystem all` command.

**Previous Behavior:** No error message is displayed for all CLIs under `show active-charging subsystem all` command. The output was not clearly displayed for P2P Flows.
New Behavior: If P2P Plugin is not loaded successfully, the message “P2P flows: n/a” will be displayed for P2P Flows when `show active-charging subsystem all` command is issued.

CSCun03902 - separate resolution for config/exec cli's for proto deprecation in 16.0

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

**Feature Changes**

**Deprecated Protocol Visibility in CLI**

If any protocol is deprecated in the plugin, the deprecated protocol will appear in the configuration mode to avoid any configuration related errors. This is done for backward compatibility with P2P configuration.

**Previous Behavior:** If any protocol was deprecated in the plugin, the protocol name will be an unrecognized keyword and the deprecated protocol name will not appear in any existing CLI.

**New Behavior:** For backward compatibility with P2P configuration, the deprecated protocol will appear in the configuration mode to avoid any configuration related errors. This will not show up in Exec mode.

CSCun41402 - P2P flows are not taking TRM / FP

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

**Feature Changes**

**P2P support for TRM**

In this release, P2P support for the Transactional Rule Matching (TRM) feature has been provided. The TRM feature enables the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified. This enables ECS to better utilize CPU resources and accommodate additional throughput for the system, thus improving the overall performance.

A transaction for TRM can be defined as the entire UDP flow, the ACK of the 3-way handshake to the FIN/RST of a TCP flow, or the HTTP request to the next HTTP request, or HTTP request to the FIN/RST for the final request of the flow. The TRM feature can also perform rule matching on IP L4 rules (UDP, TCP), HTTP, and HTTPS.

**Previous Behavior:** P2P flows were not in compliance with the TRM feature. P2P and TRM/FP cannot be enabled together.

**New Behavior:** P2P flows are considered for TRM optimization. P2P and TRM/FP can be enabled together. When TRM/FP is enabled with P2P, P2P supported protocols will not take TRM/FP. Most VoIP applications that require all packets of the flow do not support TRM.
Chapter 3
CF Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from CF in StarOS 16 software releases.
CF Enhancements for 16.0

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *CF 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.

CSCuh09464 - 2 ICAP server groups

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

**Feature Changes**

**Support for Standby Servers**

In this release, standby servers can now be configured under the Content filtering server group. The active and standby servers (primary and secondary servers respectively) under the same server group can now be configured to work in active-standby mode. The primary server group will be used as long as at least one server is up in primary group. If all servers are down in primary group, then it will switch to secondary group. This implementation ensures that there is no response delay from the servers from the first group.

**Previous Behavior:** Only active servers could be configured under ICAP server group.

**New Behavior:** In this release, standby servers can also be configured under ICAP server group (Content Filtering Server Group). A maximum of ten active and standby servers can be configured.

**Command Changes**

`icap server`

In this release, **standby** is a new keyword in this command that configure the ICAP server as standby.

`configure`

```
    context context_name

    content-filtering server-group server_name

    [ no ] icap server ip_address [ standby ]

end
```

Notes:
- A maximum of ten active and standby servers per group can be configured.

**Performance Indicator Changes**

**show content-filtering server-group statistics**

The following field has been added to the output of this command to display the number of requests sent to the standby server.

- Num req to standby server
Chapter 4
ECS Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from ECS in StarOS 16 software releases.
ECS Enhancements for 16.4

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.

---

**CSCuq88332 - Need EDR records from different rulebases to go to single EDR file**

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

**Feature Changes**

**Bundling of CDR Records**

Currently, EDRs are stored in individual files for different rulebase names and EDR formats, resulting in a huge number of smaller EDR files. Due to this, customer might experience a delay in the file transfer process. Hence, in this release, CDR module bundles the CDR records with similar fields/headers into single file.

**Previous Behavior:** EDRs were generated for matching rulebase and EDR format. By default, EDRs generated for different rulebases and formats were stored in different files. If either the rulebase or format name was not added to the filename through the `file` command in EDR configuration, then the customer has to open several files to find out the EDRs in each file.

**New Behavior:** In this release, the EDRs with similar fields/headers are bundled together in a single file by CDRMOD, thereby reducing the chances of accessing too many small files.

**Customer Impact:** There should not be any impact on customer backend record processing due to this change. If the customer has configured to include “rulebase” and “format” then the behavior remains the same even with this fix. If the customer has excluded “rulebase” and/or “format”, then their backend record processing tool should know how to process the records in each file without looking into the filename. So, this behavioral change does not have any effect.

---

**CSCur56899 - ECS rule matching wrong for app “Mon Réseau”**

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

**Feature Changes**

**ECS Rule Matching**

---
**Previous Behavior:** As per RFC, the message body with HTTP HEAD response must not be included, and since this was included, rule matching was incorrect.

**New Behavior:** Any content-length/transfer-encoding in HTTP HEAD response will be ignored, and the next downlink packet as new HTTP HEAD response will be considered in case of pipelined HTTP HEAD request/response scenario.

**Customer Impact:** The customer will be able to see proper rule matching for pipelined HTTP HEAD request/response.
ECS Enhancements for 16.3

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.

CSCup74913 - 17.0:Volume Stat mismatches in case session is in Local Policy

**Applicable Products:** P-GW

**Feature Changes**

**Flows hitting the static discard flow charging action are not accelerated**

**Previous Behavior:** Acceleration eligible flows matching a rule-action whose charging-action had discard flow action configured were accelerated. As a result of this feature, there was a charging issue with some flows where packets were getting discarded due to other reasons (such as bandwidth limiting). Since discarded packets do not go for charging, the charging buckets that need to be updated in the acceleration path, were not getting recorded. So the accelerated packets were not getting charged.

**New Behavior:** Now, acceleration is not enabled when the packet is being discarded. When there is a packet which is not discarded and goes for charging, if the conditions are conducive, the flow is accelerated from that point. As a result, the actions and charging buckets can be recorded.

CSCuq15304 - Out-Of-Order timeout expires unexpectedly leading to misbilling

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

**Feature Changes**

**Change in ‘Out-Of-Order Timeout’ Functionality**

**Previous Behavior:** Earlier, when using active-charging and ruledefs to differentiate billing for different flows, for some flows which contained a lot of out-of-order packets (and retransmitted packets), the OOO timeout might fire unexpectedly; the TCP in-order packets were forwarded and TCP OOO timeout was still being run.

**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.
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.
ECS Enhancements for 16.2

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.

**CSCup08420, CSCup49998 - 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.

**CSCup67356 - Rule failure counters not incremented**

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

**Feature Changes**

**Counter for ACS Reject Reason in No Active Rule Condition**

**Previous Behavior**: The subscriber call was rejected when there was no active rule in the rulebase. In this scenario, there was no counter to indicate the corresponding reason for the call rejection through the CLI command “show active-charging service statistics”.

**New Behavior**: Now, the “show active-charging service statistics” CLI command will indicate the total number of ACS calls rejected due to no active rule.
Performance Indicator Changes

show active-charging service statistics

The following new counter has been added to the output of `show active-charging service statistics` command to report the number of ACS calls that were rejected due to no active rule.

- No active rule in Rulebase/Subs

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.

CSCuq23706 - Removal of dynamic Rule is not working in UE only mode

Applicable Products: GGSN, P-GW

Feature Changes

Processing of Rule Removal

**Previous Behavior:** Removal of PCEF rules failed in the UE-only mode.

**New Behavior:** Rule removal will be accepted in UE-only mode for EPS IP-CAN bearer.

This generic behavior is per the standards and presently customers are using custom based CLIs for GnGp use cases. **Customer Impact:** Some functionalities for GnGp handover which were not working previously will work now. For example, GnGp handover cases having default bearer with charging rules will work seamlessly in both UE-only and mixed modes.
ECS Enhancements for 16.1

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.

**CSCuc90721 - CCR-T not triggered when mandatory avp rating-grp wrong in rule install**

**Applicable Products:** P-GW

**Feature Changes**

**Support for Session Disconnect Reason Statistics**

There was no disconnect reason set when there was a failure on Gx interface. Due to this, there was no disconnect reason seen at the CLI for these failure cases.

**Previous Behavior:** There was no disconnect reason getting set when a default bearer was deleted due to rule install failure during session setup.

**New Behavior:** A new session disconnect reason, “no_rules (457)”, will be set when a default bearer is deleted due to rule install failure during session setup.

**Performance Indicator Changes**

**show session disconnect-reasons**

The following disconnect reason has been added when a default bearer is deleted due to rule install failure during session setup:

- no_rules (457)

**CSCud41033 - flow idle timeout + flow limit for udp does not work**

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

**Feature Changes**

**flow idle timeout and flow limit for UDP**
Previous Behavior: In case of flow limit-for-flow-type and over-limit-action terminate-flow set for udp packets in charging-action, each dropped udp packet was being counted as Terminate Flow in the show active-charging charging-action statistics and ITC Terminated Flows in the show active-charging sessions full all statistics.

New Behavior: In case of flow limit-for-flow-type and over-limit-action terminate-flow set for udp packets in charging-action, now each dropped udp flow is counted as Terminate Flow in the show active-charging action statistics and ITC Terminated Flows in the show active-charging sessions full all statistics.

Command Changes

show active-charging charging-action statistics

Earlier, in case of flow limit-for-flow-type and over-limit-action terminate-flow set for udp packets in charging-action, each dropped udp packet was being counted as Terminate Flow in this command. Now, each dropped udp flow is counted.

show active-charging sessions full all

Earlier, in case of flow limit-for-flow-type and over-limit-action terminate-flow set for udp packets in charging-action, each dropped udp packet was being counted as ITC Terminated Flows in this command. Now, each dropped udp flow is counted.

CSCuf26390, CSCUm92182 - PDSN/PCEF upgrades/downgrades users' Qos, depending on service start/stop

Applicable Products: PDSN

Feature Changes

PDSN/PCEF can Upgrade or Downgrade Users’ QoS

PDSN/PCEF can now upgrade or downgrade users’ QoS depending on the service’s start or stop status.

When a service, which is defined in a pre-defined rule, starts, PDSN/PCEF detects this service and activates the action to upgrade users’ 3GPP2-Inter-User-Priority or Allocation-Retention-Priority > priority level value. It then updates it to PCEF through A11 session update message.

When a service, which is defined in a pre-defined rule, ends, PDSN/PCEF detects this service ending and activates another action to downgrade users’ 3GPP2-Inter-User-Priority or Allocation-Retention-Priority > priority level value. It then updates it to PCEF through A11 session update message.

Important: This is a customer specific feature.

Command Changes

service-detection session-update
A new `service-detection session-update` command has been added at the charging-action level in active-charging service. This command need to be configured to enable the support for users’ QoS updation by PDSN/PCEF based on service start or stop.

```
configure
  active-charging service service-name
    charging-action action-name
      [no] service-detection session-update [qos /...]
  end
```

Notes: This feature will be disabled by default.

**CSCuf55484, CSCuj96529 - 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 fields.

- **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.

**CSCui16626 - ECS Support Always send Charging-Rule-Report AVP in RAA on Gx**

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

**Feature Changes**

**Dictionary Specific Changes to Allow Sending Charging-Rule-Report AVP in RAA**

**Previous Behavior:** When RAR was received for dpca-custom24 dictionary, ECS does not report any rules installed in RAA message.

**New Behavior:** When RAR is received with rule installation message, ECS reports all installed rules for that call and performs validation for rules received in current request. ECS also reports all rules in RAA message via Charging-Rule-Report AVP.
CSCuo63589 - TRM Fastpath CLI needs change

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

Feature Changes

TRM Fastpath CLI Concealed

transactional-rule-matching and fastpath functionalities have been merged, and will be governed by only the transactional-rule-matching keyword alone. The keyword fastpath independently can no longer be used to turn on or turn off this functionality. keyword fastpath for transactional-rule-matching has been deprecated, such that, the keyword fastpath is not visible when tab or ? is entered. However, when this keyword is entered, it is accepted.

Previous Behavior: The keyword fastpath was optional and visible for transactional-rule-matching CLI in rulebase config on ASR5000/ASR5500. Even if it was configured, it did not have any effect.

New Behavior: The keyword fastpath has been deprecated and is not visible when tab or ? is entered.

Command Changes

transactional-rule-matching

transactional-rule-matching and fastpath functionalities have been merged, and will be governed by only the transactional-rule-matching keyword alone. The keyword fastpath independently can no longer be used to turn on or turn off this functionality. The keyword fastpath has been concealed from the transactional-rule-matching command.

configure

active-charging service service_name

rulebase rulebase_name

transactional-rule-matching

end
ECS Enhancements for 16.0

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.

CSCue69163 - I-RAT handover - change in Rating Group to utilize CCR-U on Gy interface

Applicable Products: P-GW

**Feature Changes**

**Optimized S2b Handoff Handling at ECS**

**Previous Behavior:** During an I-RAT handover with dedicated bearers active, when the handover happens between LTE and WLAN, P-GW tears down the dedicated bearer. If Online Charging is enabled at the bearer level, P-GW sends a CCR-T to the OCS and once the dedicated bearers are setup after successful handoff, P-GW sends a CCR-I again to terminate and re-initialize the Gy sessions with OCS during the Rating Group Change.

This behavior of sending extra messages (CCR-T and CCR-I) caused increase in Gy traffic. P-GW should be sending a CCR-U to request for quota from OCS in the I-RAT handover case.

**New Behavior:** During S2b handoff ECS will ignore the delete bearer operation and instead move the dormant bearers to active state after successful handoff. This will make sure that a CCR-T is not sent to Gy upon receiving delete bearer from P-GW. This optimization feature is implemented to intelligently send only a CCR-U for requesting quota for changed rating groups on dedicated bearers after handoff.

The current behavior of P-GW is changed to utilize a CCR-U on the Gy interface during the Rating Group change for I-RAT handover between WLAN and LTE.

**Customer Impact:** Less traffic on Gy is observed since the bearer is not deleted during handoff at ECS.

CSCug70309 - S5 Signaling minimization for MBR change of non-GBR flows

Applicable Products: P-GW

**Feature Changes**

**Suppression of Update Bearer Requests**
**Previous Behavior:** In Release 14.0, the “no policy-control update-default-bearer” command was used to suppress all Update Bearer Requests (UBRs) including those that contain changes to TFT, QCI, ARP, and APN-AMBR. In Release 15.0, the “no tft-notify-ue-def-bearer” command was used to enable the gateway to suppress the UBR received when the TFT is changed on a bearer.

**New Behavior:** With this release, the Update Bearer Requests will not be sent to the UE for any changes in QCI, ARP, or APN-AMBR irrespective of whether or not these commands are configured.

---

### CSCug71725, CSCuh65672 - ECS Normal Path Performance Improvements

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

#### Feature Changes

##### ECS Performance Improvements

To improve data-path performance and reduce CPU utilization for control-path functions, lean paths are introduced in this release. Lean path offers fast and light-weight processing for most common class of traffic. Lean path is introduced at various stages of packet processing in ECS. For each stage of packet processing, a lean path is identified, which captures most typical use case (processing path) in that stage. Logic and code of that stage is optimized for such a lean path. Non-typical processing paths are treated as exceptions, and processed in non-lean path – referred to as normal-path. Lean paths at each packet processing stage are identified and implemented independent of other stages. As a data packet moves through packet processing path, it may take lean-path or normal-path at each stage as appropriate.

**Important:** The criteria for taking lean-path are totally driven by internal design and concerns about traffic being processed in either path should be ignored. All the existing functionality in the data path continues to be supported.

Lean-paths have been implemented in the following packet processing stages:

- Shallow Packet Inspection – IP, TCP inspection
- HTTP Protocol Analyzer
- Packet Actions
- CDR Generation

---

### CSCug86838, CSCub86414, CSCui19930, CSCui19941, CSCug86780, CSCug87258, CSCug87234 - [ICSR-Volte] Removing usage of pacing queue for critical MC-ECS new frmk

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

#### Feature Changes

##### ICSR Enhancements for VoLTE
A significant number of internal enhancements have been made in support of voice-grade redundancy for Voice over LTE (VoLTE) deployments. ICSR components have been optimized to ensure that failure recovery is accomplished within acceptable limits for VoLTE. The impact on the data path is high priority. For data path interruptions, recovery be limited to no more than 50 milliseconds for intra-chassis failures and 3-4 seconds for inter-chassis failures.

For more details on this enhancement, see the System Enhancements for April 30, 2014 chapter in this Release Notes.

**CSCug87349 - Gy Assume Positive - HA Usage Reporting**

**Applicable Products:** HA

**Feature Changes**

**Gy Assume Positive Feature Support for HA Usage Reporting through EDR**

**Previous Behavior:** The current implementation does not provide a way to track and report the actual quota usage through EDR during assume positive scenarios for HA and hence resulted in potential revenue leakage and created inaccuracies in billing.

If Gy session is down when the subscriber session terminates, for 4G, the data gets reported in the Rf records, but since no Rf billing is available in 3G, the records are lost.

**New Behavior:** This feature has been enhanced to support reporting/ recording the appropriate usage in volume and time during regular OCS sessions and during assume positive scenarios separately. In this release, EDRs will be generated with new closure reasons when OCS goes down for HA.

Additional configuration options are supported in the EDR format for capturing the attributes needed for tracking usage.

This release supports a new attribute “sn-ocs-server-reachable” having the following values:

- OCS_SERVER_NOT_APPLICABLE = 0
- OCS_SERVER_UNREACHABLE = 0 + 1
- OCS_SERVER_REACHABLE = 0 + 2

This release additionally supports the following values for the attribute “sn-closure-reason”:

- ACS_EDR_OCS_REACHABLE = 16
- ACS_EDR_OCS_UNREACHABLE = 17
- ACS_EDR_INTERIM_VOLUME_EXHAUST = 18
- ACS_EDR_INTERIM_TIME_EXHAUST = 19
- ACS_EDR_OCS_STATUS_UNKNOWN = 20

**Customer Impact:** The actual allocated quota and usage are reported when Local Policy is applied so that customers can appropriately charge the subscribers and track the usage.

**Command Changes**

```
attribute
```

**sn-ocs-server-reachable** is a new keyword in this command to support the attribute “sn-ocs-server-reachable” when the OCS is in Assume positive mode.
configure
    require active-charging

active-charging service service_name

edr-format format_name

    [ no ] attribute sn-ocs-server-reachable priority priority

end

Notes:
- For this new attribute "sn-ocs-server-reachable", the following values are supported:
  - OCS_SERVER_NOT_APPLICABLE = 0
  - OCS_SERVER_UNREACHABLE = 0 + 1
  - OCS_SERVER_REACHABLE = 0 + 2
- For the attribute "sn-closure-reason", these additional values are supported:
  - ACS_EDR_OCS_REACHABLE = 16
  - ACS_EDR_OCS_UNREACHABLE = 17
  - ACS_EDR_INTERIM_VOLUME_EXHAUST = 18
  - ACS_EDR_INTERIM_TIME_EXHAUST = 19
  - ACS_EDR_OCS_STATUS_UNKNOWN = 20

edr edr-dcca-fh

edr-dcca-fh is a new keyword in this command to enable generation of EDRs when the OCS is in unreachable state.

configure
    require active-charging

active-charging service service_name

rulebase rulebase_name

    edr edr-dcca-fh [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] +

    [ default | no ] edr edr-dcca-fh

end

CSCuh13694 - ECS Cookie Match support for Websockets

Applicable Products: SAE-GW
Feature Changes

ECS Cookie Match support for Websockets

Websocket protocol is an independent TCP based protocol. A connection is identified as websocket through the first HTTP Get Request header after the three way handshake. This packet includes an upgrade header (Upgrade: websocket) and other websocket headers (Sec-Websocket*) to upgrade HTTP to websocket protocol. This helps operators to categorize websocket traffic and apply different policies for such traffic. This could also help to zero-rate websocket connection.

A new CLI “websocket flow-detection” has been implemented at rulebase level to detect the websocket protocol. The websocket protocol identification can be enabled or disabled with the new CLI websocket protocol. If the websocket detection is enabled in the rulebase, the ECS parser ensures that in the HTTP Get header fields Host, Upgrade, Connection, Sec-Websocket-Key, Origin and Sec-Websocket-Version should be present to upgrade HTTP to websocket protocol. A ruledef can be defined to identify the HTTP GET request for the websocket and rate it in a certain way. The subsequent data that is transferred through the websocket is also billed the same way as the first packet.

**Previous Behavior:** Websocket protocol was not detected.

**New Behavior:** A new CLI “websocket flow-detection http” is added at rulebase level. This CLI can detect the websocket protocol, which helps in identifying the initial TCP connection for the websocket and rate it in certain way.

**Customer Impact:** Websocket protocol can be enabled or disabled with the new “websocket flow-detection http” CLI.

Command Changes

`websocket flow-detection`

A new command `websocket flow-detection` has been added to enable/disable websocket flow detection. To enable websocket flow detection feature, use the following configuration:

```
configure

  active-charging service <ecs_service_name>

  rulebase<rulebase name>

  websocket flow-detection <protocol>

end
```

**Notes:**

Use the `no websocket flow-detection` command or `default websocket flow-detection` command to disable retransmission counted feature.

**Important:** Currently, only HTTP protocol is supported.
CSCuh28420 - Enhance URL Redirection Encryption with AES

Applicable Products: GGSN, P-GW

Feature Changes

Implementation of AES Encryption

In the current StarOS implementation, when a URL redirection is provisioned in a charging action, additional dynamic fields such as MSISDN, IMEI, username and so on, can be appended to the redirection URL. StarOS currently supports URL encryption of attributes within the redirection by using Blowfish (64 and 128 bit keys) encryption. However, Blowfish is no longer considered robust and thus operator now has the option to augment the security of these redirection parameters with a more robust encryption based on AES Encryption. AES encryption is available for 128 and 256 bit keys. For AES encryption with CBC mode of operation, a key-phrase is taken as configurable field from the operator. This key phrase is internally converted to a 128/256 bit key. An additional field value ("salt") is also allowed as a configurable field. This configurable field is optional.

Security of the subscriber sensitive attributes is enhanced with a more robust encryption algorithm. This helps protect subscriber specific information sent to different servers, thus helping operators to adhere to regulatory policies.

Previous Behavior: When a URL redirection occurs, dynamic fields such as MSISDN, IMEI, and so on can be appended to the redirection URL. These dynamic fields can be encrypted or inserted as plaintext. Earlier only 64 and 128 bit Blowfish algorithm was supported in ASR5x00 for such an encryption.

New Behavior: AES-CBC encryption algorithm is also added in ASR5x00. The AES-CBC encryption is available for 128 or 256 bit keys.

Command Changes

flow action redirect-url

A new keyword aes128 | aes256 has been introduced in the flow action redirect-url command.

To redirect-URL action on packet and flow for Session Control functionality and use blowfish or aes encryption, use this configuration.

configure

    active-charging service <ecs_service_name>

    flow action redirect-url <redirect_url> [ encryption { blowfish128 | blowfish64 | { aes128 | aes256 } [ salt ] } ] [ encrypted ] key <key> ]

end

Notes:

- aes128: Specifies to use AES-CBC encryption with 128 bit key for encrypting the dynamic fields
- aes256: Specifies to use AES-CBC encryption with 256 bit key for encrypting the dynamic fields.
- salt: Specifies to use salt with AES-CBC encryptions of the dynamic fields
CSCuh63073 - Charging for retransmissions to be controlled by svc/rbase level CLI

Applicable Products: P-GW

Feature Changes

Charging for Retransmissions Under Rulebase or Service Level CLI

Currently, whether retransmission should be charged or not is decided at three distinct places — at the charging action level, at the rulebase level, and at the service level. At the charging action level, the CLI "retransmissions-counted" signifies that retransmitted packet bytes or packet counts are to be considered for charging for whichever charging module the charging action specifies. At the rulebase, the CLI "edr sn-charge-volume count-retransmitted-units" signifies that retransmissions are to be counted in charging edrs. At the service level, the CLI "policy-control retransmissions-counted" controls the charging of retransmitted packets that match a dynamic rule. Due to this, the counts for the flow and the secondary bucket get added and this introduces lot of processing.

A new CLI “retransmissions-counted” is introduced at rulebase. This CLI retransmissions are counted for all the charging modules. Thus, this CLI overrides the CLI at the charging action as well as the CLI affecting the retransmissions. Also, the default mode for the newly added CLI enables charging of the retransmissions in the old manner ensuring backward compatibility.

Command Changes

retransmissions-counted

A new command retransmissions-counted has been added at rulebase level.

To enable retransmissions counted feature under rulebase, use the following configuration:

```
configure

active-charging service <ecs_service_name>

rulebase <rulebase name>

retransmissions-counted

end
```

CSCuj06831 - Lean Path for Rf

Applicable Products: P-GW

Feature Changes

Lean Path for RF

The following AVPs have been removed from the RF records as they were rule specific and not required:
- AF-Correlation-Information
- AF-Charging-Identifier
- Flows
- Media-Component-Number
- *[Flow-Number]

**Previous Behavior:** Dynamic rule related AVPs were shown in RF records.

**New Behavior:** Dynamic rule related AVPs are not shown in RF records.

**CSCuj78410 - Cannot enable/configure TRM feature on SSI UCS/blade platform**

**Applicable Products:** GGSN

**Feature Changes**

**Support for TRM feature on SSI Platform**

**Previous Behavior:** Earlier, the Transactional Rule Matching (TRM) feature was restricted to ASR 5500 platform only.

**New Behavior:** With this release, this feature has been extended to support SSI platform as well.

**CSCum33932 - Incorrect readdressed stats shown in ‘charging-action statistics’**

**Feature Changes**

**Incorrect Readdressed Stats Shown in "charging-action statistics"**

It is just stats issue for cli "show active-charging charging action stats" where incorrect stats are getting populated for readdressed uplink/downlink pkts/bytes.

Incorrect statistics were getting populated for readdressed uplink/downlink packets/bytes for the following CLIs:

- show active-charging charging-action statistics
- show active-charging sessions full all
- show active-charging rulebase statistics name consumer-standard

**Previous Behavior:** The CLI show active-charging charging-action statistics earlier showed the following statistics, along with other statistics:

- Upl/Dnl Pkts Readdressed
- Upl/Dnl Bytes Readdressed
- PP/Dnl Upl Pkts Readdressed
- PP/Dnl Upl Bytes Readdressed
• Readdressing Failure Statistics (Packets)

**New Behavior 1:** The CLI `show active-charging charging-action statistics` does not show the above statistics anymore, however, it shows the following statistics in addition to the other statistics:

- Flows/PP Flows Readdressed

**Previous Behavior 2:** The CLI `show active-charging sessions full all` earlier showed the following statistics:

- Current Readdressed Sessions
- Total Readdressed Uplink Pkts
- Total Readdressed Uplink Bytes
- Total Readdressed Downlink Pkts
- Total Readdressed Downlink Bytes
- Total Readdressing Failure Packets
- Non Syn Flow
- Dropped Pkts

**New Behavior 2:** The CLI `show active-charging sessions full all` does not show these statistics anymore.

**Previous Behavior 3:** The CLI `show active-charging rulebase statistics name consumer-standard` earlier showed the following statistics:

- Readdressed Upl Bytes
- Readdressed Dnl Bytes

**New Behavior 3:** The CLI `show active-charging sessions full all` does not show these statistics anymore.

- Readdressed Upl Pkts
- Readdressed Dnl Pkts
- Total Readdressed Flows
- Total Readdressing Failures
- Non Syn Flow
- Dropped Pkts

**Command Changes**

`show active-charging charging-action statistics`

This command has been modified to display the following output. the following statistics have been deleted from the command output:

- Upl/Dnl Pkts Readdressed
- Upl/Dnl Bytes Readdressed
- PP/Dnl Upl Pkts Readdressed
- PP/Dnl Upl Bytes Readdressed
- Readdressing Failure Statistics (Packets)

The following statistics have been added to the command output:
- Flows/PP Flows Readdressed

**show active-charging sessions full all**

This command has been modified to display the following output. The following statistics have been deleted from the command output:
- Current Readdressed Sessions
- Total Readdressed Uplink Pkts
- Total Readdressed Uplink Bytes
- Total Readdressed Downlink Pkts
- Total Readdressed Downlink Bytes
- Total Readdressing Failure Packets
- Non Syn Flow
- Dropped Pkts

**show active-charging rulebase statistics name consumer-standard**

This command has been modified to display the following output. The following statistics have been deleted from the command output:
- Readdressed Upl Bytes
- Readdressed Dnl Bytes

The following statistics have been added to the command output:
- Readdressed Upl Pkts
- Readdressed Dnl Pkts
- Total Readdressed Flows
- Total Readdressing Failures
- Non Syn Flow
- Dropped Pkts

**CSCum45087 - ACR-I is generated with Zero usage with CC SERVICE_DATA_TIME_LIMIT**

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

**Feature Changes**

**Rf Interim Records Generation and Suppression**
Previous Behavior: Interim records were generated for Tariff time trigger and SDF time limit even if there was no data to report.

New Behavior: If the CLI command "session idle-mode suppress-interim" is configured then Interim records will not be generated if there is no data to report irrespective of the trigger being received. If the CLI is not configured then old behavior will be followed.

For more information on this command, see the Command Line Interface Reference for this release.

Customer Impact: There will be no impact on customer as this change is CLI controlled. Customer can choose any behavior they want.

CSCum95153 - Sig11:PC: [08425115/X] acsmgr_handle_frag_reassembly()

Applicable Products: P-GW

Feature Changes

Call Drops When System Runs Out of Memory

Previous Behavior: ECS used to send a bearer release request to session manager, when session manager created a bearer, informed ECS to create the same and ECS failed to do it.

New Behavior: Now, when session manager creates a bearer, informs ECS to create the same, and ECS fails to do it, ECS returns out_of_memory status to session manager. This causes the call to get dropped immediately.

Customer Impact: Call drops can be seen when the system is running out of memory.

CSCun35089 - Printing the warnings for retransmissions elated CLIs to be deprecated

Feature Changes

Printing the Warnings for retransmission CLI

The following CLIs, which were visible have now been concealed. These CLIs would not be visible, however, would get executed if typed. A warnign messages is displayed to indicate that the CLI would be deprecated.

Previous Behavior: The following CLIs were visible and would get executed when typed:

- 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”

New Behavior: The following CLIs are no longer visible. However, when you type the CLI command, the command gets executed and displays the following warning message. "Warning: This CLI will be deprecated from next release”.

- 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

The CLI command `retransmissions-counted` is not visible at the charging action level, however, would get executed when you type it and you will get the following warning message: "Warning: This CLI will be deprecated from next release".

The CLI command `edr sn-charge-volume count-retransmitted-units` is not visible at the rulebase level, however, would get executed when you type it and you will get the following warning message: "Warning: This CLI will be deprecated from next release".

The CLI command `policy-control retransmissions-counted` is not visible at the service level, however, would get executed when you type it and you will get the following warning message: "Warning: This CLI will be deprecated from next release".
Chapter 5
ePDG Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from ePDG in StarOS 16 software releases.
ePDG Enhancements for 16.2

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

CSCum84987 - [ePDG] - P-CSCF addr over GTP S2b via the APCO parameter in the CSR

**Feature Changes**

**P-CSCF addr over GTP S2b**

Sending P_CSCF server address request in APCO IE in create session request or Private-Extension IE based on the configuration.

**Previous Behavior:** Sends P_CSCF server address request in Private extension IE.

**New Behavior:** Configuration based support to send PCSCF server address request in APCO IE or Private-EXTN IE.

**Customer Impact:** By default Private-extension is used. Customer needs to configure, to use the APCO.
CSCuo74940 - [ePDG] - Non-UICC device support using certificate based authentication

Feature Changes

Certificate based authentication support for Non-UICC devices

The ePDG supports non UICC devices which are authenticated using certificates & OCSP.

CSCuo74943 - [ePDG] - IPsec subsystem enhancement to trigger AUTH req post OCSP comm

Feature Changes

IPsec subsystem enhancement

The ePDG should authenticate the subscriber certificate first with help of OCSP responder at its own end using configured CA-certificate. After authentication the ePDG will send the AAR message to AAA server to authorize the subscriber.

Previous Behavior: The ePDG was authenticating the subscriber after authorization.

New Behavior: The ePDG is authenticating the subscriber before authorization.

Customer Impact: None

CSCuo94733 - [ePDG] - Bulkstats support for non UICC devices

Feature Changes

Bulkstats support for non UICC devices

Bulkstats support added for non UICC devices.

Previous Behavior: Non UICC Stats were not available as support for non UICC devices.

New Behavior: Added bulkstats in ePDG schema for the Active/Setup/Released counters for non UICC devices. Also added new disconnect reason Stats for authorization failed.

Customer Impact: None
ePDG Enhancements for 16.1

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 *ASR 5x00 Command Line Interface Reference* for this release.

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

---

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

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- 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:** Uses NPU SIM in data path & data used to take multiple hop in INGRESS.

**New Behavior:**
- NPU is used in Chassis instead of NPUSIM
- NATT / Migration support is added
- Data INGRESS path is more optimized

**Customer Impact:** None
ePDG Enhancements for 16.0

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.

CSCua99299 - [ePDG] no show epdg-svc session peer-addr <IP>

Feature Changes

**IPV6 for show epdg-svc session peer-addr <IP>**

```
show epdg-svc session peer-addr <IP> accepts IPv6 address also.
```

Previous Behavior: "show epdg-svc session peer-addr <IP>" accepts only IPv4 address.

New Behavior: "show epdg-svc session peer-addr <IP>" accepts both IPv4 and IPv6 addresses.

Customer Impact: No.

CSCug87380 - Narrowing of Traffic Selectors

Feature Changes

**Narrowing of Traffic Selectors**

If TSrs configured, except WSG-RAS all other subscribers GW does traffic-selectors negotiation for TSr.

Previous Behavior: Traffic selector does not negotiate, GW responds back with wild-cards tsel in TSr.

New Behavior: TSr can be configured to negotiate traffic-selection according to RFC5996. If TSr is not configured, GW respects the received tsel and responds back with the same. In either case maximum of 4 tsel for TSr can be sent out from GW.

Customer Impact: No.
CSCuh32223 - [ICSR-VoLTE] Need a CLP level distinction for VoLTE and non VoLTE calls

Feature Changes

Need a CLP level distinction for VoLTE and non VoLTE calls

At the CLP level, VoLTE and non-VoLTE calls should be distinguished at the time of ICSR switchover.

Previous Behavior: ePDG does not distinguish between VoLTE and non-VoLTE and do mark the call as VoLTE/non-VoLTE for optimized ICSR behavior.

New Behavior: ePDG does have support for marking the voLTE calls based on QCI being configured for VoLTE in the associated qci-qos-mapping configuration table and have dedicated bearer associated with the VoLTE QCI.

Customer Impact: No.

CSCuh32234, CSCuh32245 - [ICSR-VoLTE] Changes to allow control and data traffic in pending_standby

Feature Changes

Changes to allow control and data traffic in pending_standby

Allow the VoLTE data traffic in pending standby state to support VoLTE service during ICSR switchover.

Previous Behavior: Data traffic not allowed in pending standby state.

New Behavior: Only data traffic allowed while VOLTE call in pending standby state to VOLTE service during ICSR switch over.

Customer Impact: No.

CSCuh33073 - Static IP address allocation for the UE

Feature Changes

Static IP address allocation for the UE

Previously ePDG does not handle the Static IP address provided by AAA for both GTPv2 and PMIPv6 implementations. In addition when PDN type mismatch happens no unique session disconnect ePDG stats incremented so added "PDN Type Mismatch" Stats in ePDG service Stats.

Previous Behavior: No static IP address handling and no unique ePDG stats for PDN type mismatch case.

New Behavior: Added static IP address handling and also PDN type mismatch stats addition in ePDG service stats for the case when PDP type from UE and AAA mismatches.

Customer Impact: No backward compatibility.
CSCuh33133 - New Bulkstats for the number of UEs present in system

Feature Changes

**New counter for GTP based UEs**

New counter added.

*Previous Behavior:* No count of UEs.

*New Behavior:* A new counter to keep track of GTP based UEs.

*Customer Impact:* No.

Performance Indicator Changes

**ePDG Schema**

New bulkstats for catering the "Number of current UEs".

- num-qci1_bearer_active
- num-qci1_bearer_setup
- num-qci1_bearer_released
- num-qci2_bearer_active
- num-qci2_bearer_setup
- num-qci2_bearer_released
- num-qci3_bearer_active
- num-qci3_bearer_setup
- num-qci3_bearer_released
- num-qci4_bearer_active
- num-qci4_bearer_setup
- num-qci4_bearer_released
- num-qci5_bearer_active
- num-qci5_bearer_setup
- num-qci5_bearer_released
- num-qci6_bearer_active
- num-qci6_bearer_setup
- num-qci6_bearer_released
- num-qci7_bearer_active
- num-qci7_bearer_setup
- num-qci7_bearer_released
- num-qci8_bearer_active
• num-qci8_bearer_setup
• num-qci8_bearer_released
• num-qci9_bearer_active
• num-qci9_bearer_setup
• num-qci9_bearer_released
• totgtp-curr-ue-in-sys
• num-disc-invalid-pdn-type

CSCuh46483 - Support "show subs full pgw-address <>" in ePDG

Feature Changes

show subs full pgw-address

Previous Behavior: No command to find the subscribers to specific PGW address
New Behavior: New command introduced to find and clear the existing subscriber in the system to specific PG
Customer Impact:

Command Changes

show subs full pgw-address

New command show subs full pgw-address is introduced to find subscribers specific to PGW.

show subscribers full pgw-address pgw_address
show subscribers summary pgw-address pgw_address
clear subscribers pgw-address pgw_address

CSCui21701 - Enhance ePDG service stats for the qci based bearer stats

Feature Changes

Enhance ePDG service stats for the QCI

A new section "QCI Stats" to the CLI "show epdg-service statistics".

Previous Behavior: QCI stats section was not present in the CLI "show epdg-service statistics" output.
New Behavior: A new section "QCI Stats" has been added to the bulkstatistics counter cli "show epdg-service statistics".
Customer Impact: Customer can track the statistics of each bearer based on the qci value of the bearer.
Performance Indicator Changes

show epdg-service statistics

Below counters keep track of the number of active, setup and released sessions for each bearer based on the QCI value of the bearer.

QCI Stats:

- QCI 1:
  - Bearers:
    - Active
    - Setup
    - Released

- QCI 2:
  - Bearers:
    - Active
    - Setup
    - Released

- QCI 3:
  - Bearers:
    - Active
    - Setup
    - Released

- QCI 4:
  - Bearers:
    - Active
    - Setup
    - Released

- QCI 5:
  - Bearers:
    - Active
    - Setup
    - Released

- QCI 6:
  - Bearers:
    - Active
    - Setup

- Released
- QCI 7:
  - Bearers:
    - Active
    - Setup
    - Released
- QCI 8:
  - Bearers:
    - Active
    - Setup
    - Released

**CSCug83335 - IPV6 IPSec Swu interface**

**Feature Changes**

**IPV6 IPSec Swu interface**

**Previous Behavior:** Only IPv4 bind address was allowed under ePDG Service  
**New Behavior:** Now both IPv4 and IPv6 address can be bind simultaneously under ePDF Service  
**Customer Impact:** No

**CSCui42954 - ePDG and HeNBGW combo**

**Feature Changes**

**IPV6 IPSec Swu interface**

**Previous Behavior:** show/clear subscribers show/clear Subscriber_name cli were not having "epdg-service service_name" filters to display or clear epdg-service specific sessions  
**New Behavior:** keyword "epdg-service <name >" added to below CLI's, example is added in first cli, applicable for all  
**Customer Impact:** No

**show/clear subscribers**

New command show/clear subscribers is introduced to find subscribers specific to ePDG Service.

**show subscribers active epdg-service epdg_service_name**

**show subscribers activity epdg-service epdg_service_name**
show subscribers card-num  card_number  epdg-service  epdg_service_name
show subscribers connected-time  value  epdg-service  epdg_service_name
show subscribers counters  epdg-service  epdg_service_name
show subscribers data-rate  epdg-service  epdg_service_name
show subscribers ebi  ebi_value  epdg-service  epdg_service_name
show subscribers full  epdg-service  epdg_service_name
show subscribers idle-time  value  epdg-service  epdg_service_name
show subscribers imsi  value  epdg-service  epdg_service_name
show subscribers msid  value  epdg-service  epdg_service_name
show subscribers network-type  value  epdg-service  epdg_service_name
show subscribers qci  value  epdg-service  epdg_service_name
show subscribers rx-data  value  epdg-service  epdg_service_name
show subscribers smgr-instance  value  epdg-service  epdg_service_name
show subscribers subscription full  epdg-service  epdg_service_name
show subscribers summary  epdg-service  epdg_service_name
show subscribers tft  epdg-service  epdg_service_name
show subscribers tx-data  value  epdg-service  epdg_service_name
show subscribers username  value  epdg-service  epdg_service_name
show subscribers wfl  epdg-service  epdg_service_name

clear subscribers active  epdg-service  epdg_service_name

clear subscribers card-num  card_number  epdg-service  epdg_service_name

clear subscribers connected-time  value  epdg-service  epdg_service_name

clear subscribers ebi  ebi_value  epdg-service  epdg_service_name

clear subscribers idle-time  value  epdg-service  epdg_service_name

clear subscribers imsi  value  epdg-service  epdg_service_name

clear subscribers msid  value  epdg-service  epdg_service_name

clear subscribers network-type  value  epdg-service  epdg_service_name

clear subscribers rx-data  value  epdg-service  epdg_service_name

clear subscribers smgr-instance  value  epdg-service  epdg_service_name

CSCuj21726 - Sessmgr changes for SWu over IPv6 transport support

Feature Changes

SWu over IPv6 transport support

With this release, ePDG supports IPv6 from the UEs during the IPsec negotiation. When a UE attaches to a WiFi AP, the WiFi Access Point may assign the UE an IPv6 address. Once the UE is provided an IPv6 address the UE will be directed to establish an IPsec connection to the ePDG.

Previous Behavior: Only IPv4 bind address was allowed under ePDG Service.

New Behavior: Both IPv4 and IPv6 address can be bind simultaneously under ePDG Service.

Customer Impact: No.

bind address

ePDG supports IPv6 bind address.

bind address bind_address crypto-template crypto_template_service_name

CSCul15285 - Local PGW resolution required for ePDG

Feature Changes

Local PGW resolution required for ePDG

Previous Behavior: The local PGW resolution is not available.

New Behavior: The local PGW resolution is supported with apn-profile, operator-policy and subscriber-map.

Customer Impact: No.

apn-profile

ePDG-service supports local PGW resolution.
ePDG is enabled to configure pgw address.

apn-profile profile_name pgw address address
ePDG is enabled to link apn-profile with apn-ni.

operator-policy name name
ePDG is enabled to link operator-policy with subscriber-map.
CSCul88963 - VoLTE enhancement License for 16.0.

Feature Changes

VoLTE enhancement License for 16.0

Previous Behavior: VoLTE service in ICSR framework during ICSR switchover not supported.

New Behavior: VoLTE keyword inside the qci-qos-mapping table is control by the license.

Customer Impact: Can not use VoLTE service in ICSR framework without VoLTE license.
Chapter 6
GGSN Changes in Release 16

This chapter identifies features and functionality added to, modified for, or depreciated from the GGSN in StarOS 16 software releases.
GGSN Enhancements for 16.2

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

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

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

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

---

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

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

---

**CSCun84742 - S6b Assume +ve counter is missing for the Current Subs in system**

**Feature Changes**

**Statistics added for S6b Assume Positive State for Subscribers**

AAA diameter authentication can be configured to assume the subscriber as valid for certain AAR error response code and by-pass S6b from then on. A few counters have been introduced on the GGSN, P-GW, and SAEGW to display the total number of subscribers which are in S6b by-passed state (also called “assumed positive”).

**Previous Behavior:** There was no way to find or display the total number of current subscribers in S6b by-passed state.

**New Behavior:** New counters have been added to display the number of S6b assumed positive subscribers.
Performance Indicator Changes

GTP-C Schema

Following counter has been added to the GTPC schema

- %setup-ggsn-s6b-assume-positive%: Current S6b assumed positive subscriber count

show gtpc statistics

Following counter has been added to the output of this command in order to display the assumed positive subscribers:

- S6b Assume Positive: The number of S6b assumed positive subscriber count being facilitated by the system.

show subscribers ggsn-only summary

Following counter has been added to the output of this command in order to display the current number of S6b assumed positive subscribers:

- Total S6b Assume Positive

CSCuo40814 - [gn-gp]: 2 Bearers with same QCI/ARP combination - QCI Downgrade Case

Feature Changes

Enhancement for two bearers with same QCI/ARP combination

Previous Behavior: If suppress nrupc is enabled and MBR is greater than APN-AMBR in SGSN initiated UPC request, then NRUPC gets generated containing PCRF provided QCI and ARP

New Behavior: If suppress nrupc is enabled and MBR is greater than APN-AMBR in SGSN initiated UPC request, then NRUPC gets generated containing SGSN requested QCI and ARP.
GGSN Enhancements for 16.1

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

---

**CSCun84742 - S6b Assume +ve counter is missing for the Current Subs in system**

**Feature Changes**

**Statistics added for S6b Assume Positive State for Subscribers**

AAA diameter authentication can be configured to assume the subscriber as valid for certain AAR error response code and by-pass S6b from then on. A few counters have been introduced on the GGSN, P-GW, and SAEGW to display the total number of subscribers which are in S6b by-passed state (also called “assumed positive”).

**Previous Behavior:** There was no way to find or display the total number of current subscribers in S6b by-passed state.

**New Behavior:** New counters have been added to display the number of S6b assumed positive subscribers.
Performance Indicator Changes

GTP-C Schema

Following counter has been added to the GTPC schema

- %setup-ggsn-s6b-assume-positive%: Current S6b assumed positive subscriber count

show gtpc statistics

Following counter has been added to the output of this command in order to display the assumed positive subscribers:

- S6b Assume Positive: The number of S6b assumed positive subscriber count being facilitated by the system.

show subscribers ggsn-only summary

Following counter has been added to the output of this command in order to display the current number of S6b assumed positive subscribers:

- Total S6b Assume Positive

CSCuo40814 - [gn-gp]: 2 Bearers with same QCI/ARP combination - QCI Downgrade Case

Feature Changes

Enhancement for two bearers with same QCI/ARP combination

Previous Behavior: If suppress nrupc is enabled and MBR is greater than APN-AMBR in SGSN initiated UPC request, then NRUPC gets generated containing PCRF provided QCI and ARP

New Behavior: If suppress nrupc is enabled and MBR is greater than APN-AMBR in SGSN initiated UPC request, then NRUPC gets generated containing SGSN requested QCI and ARP.
GGSN Enhancements for 16.0

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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

---

**CSCua97985 - Graceful Shutdown of PDN with inactive VoLTE calls**

**Feature Changes**

**Graceful Shutdown Support for VoLTE**

There are likely to be cases where an Operator would need to shut down a P-GW/S-GW/SAEGW for upgrade/maintenance purpose; during that time, 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.

This could also be used in case there is a need to migrate a VoLTE APN from one P-GW to another. This feature will help in doing this VoLTE APN migration in a graceful manner. A new qualifier, `non-volte-call`, has been added to the `clear subscribers` CLI to clean up only those PDNs that have no Active Voice bearer. Identification of the VoLTE PDN and bearer is done using the VoLTE call identification configuration discussed above.

Until the time the upgrade/maintenance is going on, the new calls will be rejected so that an alternate P-GW/S-GW/SAEGW can handle it. This is done using the `new-call policy` configuration.
Below are the set of steps that can be carried out to gracefully clean up VoLTE PDNs on a node:

1. Use call identification configuration to configure the VoLTE APN to do the VoLTE PDN and bearer identification.
2. Using the new call-policy configuration, configure the node to reject any new calls coming on the node, so that these new calls get directed to an alternate PDN.
3. Using the `clear subscribers` CLI with `non-volte-call` qualifier in it, initiate the clean up of PDNs that don’t have any Active Voice bearer.
4. Wait for some time and execute the `clear subscribers` CLI again to clean up any non-active VoLTE PDNs.
   Repeat this step until all of the VoLTE PDNs are cleaned up.

Further enhancements are planned for this feature in future releases.

**Customer Impact:** Several features added for VoLTE in 16.0 will provide a lot of value to Operators; they help Operator in providing high quality VoLTE service to ensure better user experience for VoLTE service users.

**Command Changes**

`clear subscribers`  

`non-volte-call` is a new keyword that initiates the clean up of PDNs that don’t have any Active Voice bearer.

`clear subscribers apn apn_name non-volte-call`

`clear subscribers apn apn_name non-volte-call max-subscribers max_count uniform`

`clear subscribers all non-volte-call`

`clear subscribers all non-volte-call max-subscribers max_count uniform`

Notes:

- `non-volte-call`: Disconnects PDN connections that do not have an active voice call.
- `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.

**CSCua99366, CSCui04214 - Dedicated bearer timeout action**

**Feature Changes**

**Dedicated Bearer Timeout Support on the GGSN**

**Important:** For this release, this feature is Lab/Trial Quality only.

The GGSN has been enhanced to support a bearer inactivity timeout for GBR and non-GBR bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value.
**Previous Behavior:** Earlier only one timer was there for any kind of bearer.

**New Behavior:** Different timer values provide for GBR and non GBR types of bearers for bearer inactivity

**Customer Impact:** Operators now can configure a bearer inactivity timeout for GBR and non-GBR bearers for more efficient use of system resources.

**Command Changes**

```
timeout bearer-inactivity
```

The command `timeout bearer-inactivity` now supports a bearer inactivity timeout for GBR and non-GBR GGSN bearer type sessions.

```
configure

custom context context_name

    apn apn_name

    timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold [ downlink | total | uplink ] bytes

    timeout bearer-inactivity exclude-default-bearer

    no timeout bearer-inactivity [ exclude-default-bearer | gbr | non-gbr ]

end
```

Notes:

- **timeout:** Specifies that a bearer time out value will be configured for this APN.
- **bearer-inactivity:** Specifies that the system will check for low activity for a bearer.
- **gbr:** Specifies that the GGSN will check for low activity on a GBR bearer.
- **non-gbr:** Specifies that the GGSN will check for low activity on a non-GBR bearer.
- **dur_seconds:** Specifies the timeout for the bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).
- **volume-threshold:** Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.
- **downlink:** Threshold value of the downlink data traffic in a bearer.
- **total:** Specifies that the total of both uplink and downlink data will be used as a volume threshold.
- **uplink:** Threshold value of the uplink data traffic in a bearer.
- **bytes:** must be a value from 1 to 4294967295.
- **exclude-default-bearer:** Ignore bearer inactivity handling for default/primary bearer.

**Performance Indicator Changes**

```
show apn name
```
This command has been enhanced to list bearer inactivity timeout settings, if configured.

- bearer inactivity timeout (GBR Bearers)
- bearer inactivity timeout (Non-GBR Bearers)
- bearer inactivity exclude-default-bearer

**CSCug38359 - QCI Based Stats for CLI and Bulkstats**

**Feature Changes**

**QCI-based stats in CLI and Bulkstats**

New stats have been introduced under APN level for QCI support.

**Previous Behavior:** No Bearer Rejection counters and Uplink/Downlink Packet/Byte Dropped Excd MBR stats for each QCI under APN level.

**New Behavior:** Bearer Rejected counters and Uplink/Downlink Packet/Byte Dropped Excd MBR stats are added per QCI [QCI 1 to 9] in CLI and Bulkstats under APN level.

**Performance Indicator Changes**

**show apn statistics**

Following stats have been added in the output of the above command:

- QCI1: Bearer Rejected
- QCI1: Uplink Bytes dropped(MBR Excd)
- QCI1: Downlink Bytes dropped(MBR Excd)
- QCI1: Uplink pkts dropped(MBR Excd)
- QCI1: Downlink pkts dropped(MBR Excd)
- QCI2: Bearer Rejected
- QCI2: Uplink Bytes dropped(MBR Excd)
- QCI2: Downlink Bytes dropped(MBR Excd)
- QCI2: Uplink pkts dropped(MBR Excd)
- QCI2: Downlink pkts dropped(MBR Excd)
- QCI3: Bearer Rejected
- QCI3: Uplink Bytes dropped(MBR Excd)
- QCI3: Downlink Bytes dropped(MBR Excd)
- QCI3: Uplink pkts dropped(MBR Excd)
- QCI3: Downlink pkts dropped(MBR Excd)
- QCI4: Bearer Rejected
- QCI4: Uplink Bytes dropped(MBR Excd)
- QCI4: Downlink Bytes dropped(MBR Excd)
- QCI4: Uplink pkts dropped(MBR Excd)
- QCI4: Downlink pkts dropped(MBR Excd)
- QCI5: Bearer Rejected
- QCI5: Uplink Bytes dropped(MBR Excd)
- QCI5: Downlink Bytes dropped(MBR Excd)
- QCI5: Uplink pkts dropped(MBR Excd)
- QCI5: Downlink pkts dropped(MBR Excd)
- QCI6: Bearer Rejected
- QCI6: Uplink Bytes dropped(MBR Excd)
- QCI6: Downlink Bytes dropped(MBR Excd)
- QCI6: Uplink pkts dropped(MBR Excd)
- QCI6: Downlink pkts dropped(MBR Excd)
- QCI7: Bearer Rejected
- QCI7: Uplink Bytes dropped(MBR Excd)
- QCI7: Downlink Bytes dropped(MBR Excd)
- QCI7: Uplink pkts dropped(MBR Excd)
- QCI7: Downlink pkts dropped(MBR Excd)
- QCI8: Bearer Rejected
- QCI8: Uplink Bytes dropped(MBR Excd)
- QCI8: Downlink Bytes dropped(MBR Excd)
- QCI8: Uplink pkts dropped(MBR Excd)
- QCI8: Downlink pkts dropped(MBR Excd)
- QCI9: Bearer Rejected
- QCI9: Uplink Bytes dropped(MBR Excd)
- QCI9: Downlink Bytes dropped(MBR Excd)
- QCI9: Uplink pkts dropped(MBR Excd)
- QCI9: Downlink pkts dropped(MBR Excd)
- Invalid/ Not-Configured QCI: Bearer Rejected

**show bulkstats variables apn**

Following bulkstats have been added in the output of the above command in support of the QCI:

- qci1-uplinkpkt-drop-mbrexcd
- qci1-dwlinkpkt-drop-mbrexcd
- qci1-uplinkbyte-drop-mbrexcd
- qci1-dwlinkbyte-drop-mbrexcd
- qci1-rejbearer
- qci2-uplinkpkt-drop-mbrexcd
- qci2-dwlinkpkt-drop-mbrexcd
- qci2-uplinkbyte-drop-mbrexcd
- qci2-dwlinkbyte-drop-mbrexcd
- qci2-rejbearer
- qci3-uplinkpkt-drop-mbrexcd
- qci3-dwlinkpkt-drop-mbrexcd
- qci3-uplinkbyte-drop-mbrexcd
- qci3-dwlinkbyte-drop-mbrexcd
- qci3-rejbearer
- qci4-uplinkpkt-drop-mbrexcd
- qci4-dwlinkpkt-drop-mbrexcd
- qci4-uplinkbyte-drop-mbrexcd
- qci4-dwlinkbyte-drop-mbrexcd
- qci4-rejbearer
- qci5-uplinkpkt-drop-mbrexcd
- qci5-dwlinkpkt-drop-mbrexcd
- qci5-uplinkbyte-drop-mbrexcd
- qci5-dwlinkbyte-drop-mbrexcd
- qci5-rejbearer
- qci6-uplinkpkt-drop-mbrexcd
- qci6-dwlinkpkt-drop-mbrexcd
- qci6-uplinkbyte-drop-mbrexcd
- qci6-dwlinkbyte-drop-mbrexcd
- qci6-rejbearer
- qci7-uplinkpkt-drop-mbrexcd
- qci7-dwlinkpkt-drop-mbrexcd
- qci7-uplinkbyte-drop-mbrexcd
- qci7-dwlinkbyte-drop-mbrexcd
- qci7-rejbearer
- qci8-uplinkpkt-drop-mbrexcd
CSCuh35139 - PGW SM sync up with driver [Phase 1]

Feature Changes

Change in message generation towards access side

**Previous Behavior:**
1. In case of GTP-U error indication, P-GW was sending out Delete Bearer Request and was waiting for response before doing the clean up.
2. If there was a collision between GTP messages and the older transaction got aborted, until now any PCRF rules coming in the response for that transaction were getting aborted.

**New Behavior:**
1. In case of GTP-U error indication, P-GW will align with GGSN and not send any Delete Bearer Request out. It will do the required clean up locally.
2. If there is a collision between GTP messages and the older transaction gets aborted, the old behavior will be retained if the transaction was pending at Gy/Rf when it got aborted. If, however, it was pending at PCRF, these rules will now be processed.

**Customer Impact:**
1. In case of GTP-U error indication, the message was not needed since the peer does not have that particular bearer.
2. Customer will start seeing some rules processed, in case of collision, which were not processed before.

CSCul59203 - GGSN Rf Record populated with SGSN MCC-MNC AVP as ???

Feature Changes

Support for Invalid MCC-MNC Received in GTPC ULI

**Previous Behavior:** Earlier GGSN decoded invalid MCC-MNC in GTPC parameter User Location Information (ULI) into ASCII special characters like “?” etc. This invalid value was sent over Rf and Gx in AVP: 3GPP-SGSN-MCC-MNC.
**New Behavior:** A new CLI has been introduced which configures GGSN to decode invalid MCC-MNC in ULI into hexadecimal digits. When this new CLI is disabled, the previous behavior is in effect. The received MCC-MNC is decoded assuming that it contains decimal digits only. When the CLI is enabled, if the received MCC-MNC is invalid, it is decoded into decimal digits. If the received MCC-MNC is invalid, all digits are decoded into hexadecimal digits, including filler digits, if any.

**Customer Impact:** Handles invalid MCC-MNC received in GTPC ULI gracefully. The invalid value is decoded into hexadecimal digits. The Rf and Gx AVP “3GPP-SGSN-MCC-MNC” contains the decoded hexadecimal digits.

**Command Changes**

```plaintext
gtpc decode-as-hex
```

This is a new command which configures the GGSN to decode the MCC-MNC parameters from the User Location Information (ULI) to hexadecimal digits.

```plaintext
configure
  context context_name
    ggsn-service service_name
      [ default | no ] gtpc decode-as-hex
```

**CSCug41145 - QoS eARP - H & M configuration on GGSN/PGW**

**Feature Changes**

**Configuration Support for ARP Mapping**

**Previous Behavior:** Earlier ARP and Priority-Level AVP used to be derived on the basis of H =3 and M=8. Also if support-earp CLI was configured in a GGSN service earlier and if a UPC Request came without eARP IE from SGSN that has indicated its support in CPC, request used to get rejected.

**New Behavior:** Now with the support of configurable H & M values, ARP and Priority-Level AVP depends on range of H and M. Also, UPC/Sec CPC will not get rejected.

**Customer Impact:** CLI controlled H and M configuration.

**Command Changes**

```plaintext
arp-mapping priority-level
```

This is a new command to support the configuration of high and low level values for ARP mapping.

```plaintext
configure
  peer-profile service-type ggsn-access name peer_profile_name
    arp-mapping priority-level high high_priority medium med_priority
```
[ default ] arp-mapping priority-level high high_priority medium med_priority
end

Notes:
- **default**: Sets default values for the peer profile
- **priority-level**: Configures the high and medium values for peer profile. The `high_priority` is an integer and ranges from 1 to 13 while the `med_priority` is also an integer, ranges from 2 to 14.

### Performance Indicator Changes

**show peer-profile full all**

With the support for the CLI level configuration of high and low level values for ARP mapping, following new fields have been added to the above show command:

- ARP Mapping
  - High Priority Level
  - Medium Priority Level

### CSCug95856 - GGSN - Common flags control through CLI

### Feature Changes

#### Common Flags Control Support

Support has been introduced for the configuration of the common flags: NQN and UQS through CLI.

**Previous Behavior**: No support existed

**New Behavior**: Common flags are now updated based on the new CLI values.

### Command Changes

**no-qos-negotiation**

This is a new command to configure the overriding of No-Qos-Negotiation (NQN) flag in common flag IE received from peer node.

```
configure

peer-profile service-type ggsn-access name peer_profile_name

no-qos-negotiation { set-flag | unset-flag }
[ no ] no-qos-negotiation
end
```
Notes:

- **no**: Disables or removes the configured overriding of No-Qos-Negotiation flag in common flag IE received from peer node.
- **set-flag**: Sets flag value to 1 in common flag IE.
- **unset-flag**: Sets flag value to 0 in common flag IE.

**upgrade-qos-supported**

This is a new command to configure the overriding of upgrade-qos-supported (UQS) flag in common flag IE received from peer node.

```
configure

peer-profile service-type ggsn-access name peer_profile_name

upgrade-qos-supported ( set-flag | unset-flag )

[ no ] upgrade-qos-supported

end
```

Notes:

- **no**: Disables or removes the configured overriding of upgrade-qos-supported flag in common flag IE received from peer node.
- **set-flag**: Sets flag value to 1 in common flag IE.
- **unset-flag**: Sets flag value to 0 in common flag IE.

**Performance Indicator Changes**

**show peer-profile full all**

Following fields have been added to output:

- Upgrade-qos-supported
- No-qos-negotiation

**CSCum15133 - Def Bearer Rejected stats under APN level is inconsistent for HO cases**

**Feature Changes**

**Default Bearers Rejected Statistics**

The behavior of the “Default Bearer Rejected” statistics under APN level is inconsistent for HO scenarios. This statistic is incremented for LTE to WiFi, eHRPD to WiFi, WiFi to LTE, eHRPD to LTE handover when Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch, etc., but not incremented for other error scenarios.
Previous Behavior: “Default bearers rejected” statistics under APN level under CLI `show apn statistics`:
- Incremented - For the plain vanilla new call for P-GW and GGSN if the Default Bearer is rejected.
- Incremented - For eHRPD to LTE, eHRPD to WiFi, WiFi to LTE, and LTE to WiFi - When Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch.
- Not Incremented - For GnGp handoff, LTE to eHRPD. WiFi to eHRPD, eHRPD to WiFi, eHRPD to LTE, LTE to WiFi, and WiFi to LTE.

New Behavior: “Default bearers rejected” statistics under APN level under CLI `show apn statistics`:
- Increment - For the plain vanilla new call for P-GW and GGSN if the Default Bearer is rejected.
- Do NOT Increment - For eHRPD to LTE, eHRPD to WiFi, WiFi to LTE, and LTE to WiFi - When Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch.
- Do NOT Increment - For GnGp handoff, LTE to eHRPD. WiFi to eHRPD, eHRPD to WiFi, eHRPD to LTE, LTE to WiFi, and WiFi to LTE.

CSCum85474 - Wrong data type for Bearer reject bulkstat variable (rejbearer)

Performance Indicator Changes

APN Schema

The following statistics changed to Int32 from Int64.
- qci1-actbear
- qci1-setupbear
- qci1-relbear
- qci2-actbear
- qci2-setupbear
- qci2-relbear
- qci3-actbear
- qci3-setupbear
- qci3-relbear
- qci4-actbear
- qci4-setupbear
- qci4-relbear
- qci5-actbear
- qci5-setupbear
- qci5-relbear
- qci6-actbear
- qci6-setupbear
- qci6-relbear
- qci7-actbear
- qci7-setupbear
- qci7-relbear
- qci8-actbear
- qci8-setupbear
- qci8-relbear
- qci9-actbear
- qci9-setupbear
- qci9-relbear

CSCun51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change

Feature Changes

BCM Mode Derivation during gn-gp Handoff

Previous Behavior: Earlier the UE support for bearer control mode (BCM) was unknown on handover from PGW to GGSN and therefore BCM would not be derived as expected.

New Behavior: With new changes, even if PCO IE is not sent in handover 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 handover rather than assuming BCM in PGW to be always by UE.

CSCTy95123 - Always-ON license for GGSN

Feature Changes

Always On License for GGSN

Previous Behavior: Bulkstats for considering number of active-call for GGSN was not available. Similar type of bulkstat were present for MME, P-GW, and S-GW products.

New Behavior: “ggsn-activedata” bulkstat support has been added.

Customer Impact: Number of active GGSN call count shall be available.

Performance Indicator Changes

System Schema
With this requirement, bulkstat for GGSN are proposed in system schema

- **gsn-activedata**: defines the current number of GGSN sessions actively transmitting and receiving data packets. This statistic is updated once an hour and is defined as having sent and/or received at least one data packet within the last 60 seconds of the update time.

### CSCug70293 - PCO for UE Notification - GGSN Support

#### Feature Changes

**PCO for UE Notification**

The CLI for this feature already exists in support for P-GW and now the same is supported for GGSN as well.

**Previous Behavior:** Earlier no custom PCO values were configurable under the APN configuration for GGSN.

**New Behavior:** Custom PCO values can now be configured for the UE notifications to be sent for GGSN, too.

**Customer Impact:** Customized PCO option for UE notification can be sent for GGSN product as well with the existing CLI options under the APN configuration.

### CSCuh28410 - GTP-U UDP Bundle

#### Feature Changes

**GTP-U UDP Bundle**

Currently, for forwarding GTP-U data packets, standard UDP port (2152) as source and destination port are used for outgoing GTP-U packet. This creates hardship to balance traffic properly over the LAG interfaces between the different L2/L3 elements in the network. Some routers use source UDP port to do load balancing of packets towards destination.

As part of this feature, behavior is changed so that source port outgoing GTP-U packet is different for each SESSMGR. The destination port should remain as 2152, as per protocol.

The usage of non-standard source port number is permitted, as per section 4.4.2 of 3GPP TS 29.281. This feature does not require deviation from any GTP-U protocol aspects as defined in 3GPP TS 29.281.

A new CLI is added in GTP-U Service configuration to enable this behavior. By default, standard port 2152 is used as source port.

**Customer Impact:** Helps in doing effective load balancing of data traffic over LAG interfaces on some routers.

#### Command Changes

**source-port**

This new command configures GTP-U data packet source port related parameters.

```plaintext
configure
  context context_name
```
**GGSN Changes in Release 16**

**GGSN Enhancements for 16.0**

```plaintext
GTPU Service service_name
  source-port { non-standard | standard }
  default source-port
end
```

**Notes:**
- **non-standard**: Configures GTP-U service to use multiple non-standard ports defined by system as a source port for GTP-U data packets. Starting port is 25500. Non-standard port number is unique per session manager instance.
- **standard**: Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.
- **default**: Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.
- By default, standard port 2152 will be configured as GTP-U data packet source port (same as existing behavior).

**Performance Indicator Changes**

```plaintext
show gtpu-service name
```

The following output had been added to show GTP-U source port configuration.
- GTPU Source-port Configuration
Chapter 7
GTPP Changes in Release 16

This chapter identifies GTPP management features and functionality added to, modified for, or deprecated from GTPP in StarOS 16 software releases.
GTPP Enhancements for 16.5

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.

CSCuu12720 - Wrong timeOfFirstUsage value in LOSDV for Service idle out condition

Applicable Products: GGSN, P-GW

Feature Changes

Closing of LOSDV Containers During Service Idle Timeout Scenario

In this release, the interim CDR should not have zero volume LOSDV generated for service idle timeout scenario.

Previous Behavior: If there was a LOSDV bucket created between the packet arrival time and service-idle-out expiry time, no data counts were reported. So, a zero-volume LOSDV was generated for service idle timeout scenario.

New Behavior: If there are no data counts available for a service flow, the LOSDV for service idle timeout will not be created. The service-idle timeout will be started only when the next data packet arrives.

This behavior change is applicable to eG-CDRs and PGW-CDRs for all GTPP dictionaries except custom5 and custom40 dictionaries.
GTPP Enhancements for 16.2

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

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

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

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

CSCun71456 - 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 are 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 is 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>

CSCup59675 - gtpp push-to-active feature password shown in plain text

**Applicable Products:** GGSN, P-GW, SAE-GW, SGSN, S-GW
Feature Changes

Encrypted URL Support for GTPP Push-to-Active Configuration

**Previous Behavior:** The `show configuration` command displayed the `gtp push-to-active url` configuration in a clear text format.

**New Behavior:** A new keyword “encrypted” has been added to the “gtp push-to-active url” command in Global Configuration mode to allow configuring an encrypted password for the push-to-active URL.

The `show configuration` command will display the `gtp push-to-active` configuration in encrypted format. The `show configuration showsecrets` command will display the `gtp push-to-active` configuration in clear text.

Command Changes

`gtp push-to-active url`

*encrypted* is a new keyword in this command to configure and display the `gtp push-to-active url` in encrypted format.

configure

`gtp push-to-active [ encrypted ] url url via-context context_name no gtp push-to-active`

end

Notes:

- *encrypted*- Indicates that the URL is encrypted for security reasons.
GTPP Enhancements for 16.1

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.

CSCuo33140 - SGWRECORD EPCQoSInformation UL/DL GBR/MBR showing negative values

**Applicable Products:** S-GW

**Feature Changes**

**Modified CDR Encoding Syntax**

**Previous Behavior:** The EPC QoS values for these attributes — maxRequestedBandwidthUL/DL, guaranteedBitrateUL/DL, and aPNAggregateMaxBitrateUL/DL in SGW CDRs were previously encoded as “int”.

**New Behavior:** The EPC QoS values for maxRequestedBandwidthUL/DL, guaranteedBitrateUL/DL, and aPNAggregateMaxBitrateUL/DL in SGW CDRs will now be encoded as "unsigned int" (can be upto 5 bytes of encoding).

**Customer Impact:** The CDR decoder should handle this new encoding syntax. In general, there are many other attributes such as uplink and downlink data volume which are unsigned integer. So, this would have already been handled by customer.
GTPP Enhancements for 16.0

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.

---

**CSCua75528 - GGSN/PGW/SGW multiple sessmgr-crashes occurred due to dictionary change**

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

**Feature Changes**

**Display of Warning Message for GTPP Dictionary Configuration/Change**

The following warning message will be displayed whenever an existing GTPP dictionary is being changed or a new GTPP dictionary is configured irrespective of whether or not the calls are active on the system.

Warning: It is not recommended to change the dictionary when the system has active calls.

Are you sure? [Yes|No]: n

**Important:** This change will require user's input on the CLI console for GTPP dictionary configuration / change.

Note that this warning message will be displayed for all GTPP dictionaries. This prompt is thrown to avoid any crashes happening in the system.

---

**CSCue50610, CSCui11709 - PGW CDR for session from S4SGSN (with CGI, RAI) has only CGI in ULI field**

**Applicable Products:** P-GW

**Feature Changes**

**Populate Missing ULI Identities in PGW-CDR**

The User Location Information (ULI) Information Element (IE) contains the user location where the UE is located during the service data container. ULI is a variable length Information Element (IE) having various identity types such as CGI, RAI, SAI, etc.
As per 3GPP TS 29.274, ULI received by P-GW in Create Session Request (CSReq) can have various combinations of the different identity types. The same is now populated in the PGW-CDR whatever the type of ULI is received in the Create Session Request by the P-GW.

This support is extended to Create Session Request, Create Bearer Response, Modify Bearer Request and Delete Session Requests.

**Important:** The changes are applicable to Release 10 GTPP dictionaries for P-GW.

**Previous Behavior:** Currently, only a fixed number of combinations of ULI identity types is supported. That is, Release 10 ULI values were only partially populated in PGW-CDRs as the ULI identity type combinations “CGI & RAI” and “SAI & RAI” introduced in 3GPP Release 10 specification were not supported.

**New Behavior:** Release 10 ULI values are populated as received in PGW-CDRs.

**Customer Impact:** PGW-CDR now accurately reflects the ULI information as reported by various nodes. This helps the operator to reconcile the user location information reported by various nodes in the network and charge accordingly.

---

**CSCue68228 - IPSG: Support SN-Transparent-Data and SN-Assigned-VLAN-ID in eGCDRs**

**Applicable Products:** IPSG

**Feature Changes**

**SN-Transparent-Data AVP on IPSG**

SN-Transparent-Data AVP carries current PDP session information. Once the session specific information such as operator-id, GPS id, satellite-id, etc are made available to the gateway via RADIUS or PCRF interfaces, the same session information can be carried over to other interfaces such as Gy and Gz (eGCDR) for billing and charging purposes. Any change in SN-Transparent-Data AVP will not be triggering an update, and the updated values will be reported during the next CCR-Request.

This feature is currently applicable to only GGSN and IPSG products and is available only in custom46 for eGCDR and dynamic-dictionary for Gy.

A new GTPP dictionary “custom46” has been added to support SN-Transparent-Data and SN-Assigned-VLAN-ID AVPs in eGCDRs.

**Customer Impact:** This feature helps the operator to do subscriber specific billing. By co-relating the same subscriber specific information across various interfaces, billing can be easily reconciled and charged to the subscriber accurately.

---

**CSCug95458 - CDRs on CGW and SaMOG GW**

**Applicable Products:** SaMOG

**Feature Changes**

**Support for CDRs on CGW and SaMOG**
With this release, SaMOG supports generation of CDR files for offline charging. In Offline Charging, charging information is collected concurrently with resource usage. The charging information is then passed through a chain of logical charging functions, and the CDR files are generated by the network, which are then transferred to the network operator's Billing Domain.

As 3GPP specifications does not define a CDR format for SaMOG, the S-GW CDR and SGSN CDR record formats are used to define the CDR format for SaMOG 4G/3G subscribers. The record format can be selected using a CLI command under the GTPP Group Configuration Mode. By default, for an SaMOG license, the S-GW record type is used, and for an SaMOG 3G license, the SGSN record type is used.

**CSCuh13699 - CDR LIFO**

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

**Feature Changes**

**New CDR Streaming Mode**

This feature introduces a new CDR streaming mode, wherein the newly generated CDRs from AAA Managers are sent to CGF server along with the streamed CDRs from hard disk.

With streaming mode enabled, CDRs are written to HDD when the OCG connectivity is down. Once the OCG connectivity is up, the HDD contents are sent in a First-In-First-Out (FIFO) order. New records should be written to disk as long as all contents from disk are not fully flushed. If the disk is completely flushed, the records can be sent to OCG directly.

With parallel mode, this behavior is changed to send new CDRs directly to CGF when streaming from HDD is in progress.

The existing CLI command, to set the streaming mode, is extended. The “parallel” keyword enables the new parallel streaming mode.

**Previous Behavior:** In the old FIFO mode, when the CGF becomes active, all CDRs in HDD are streamed in a First-In-First-Out (FIFO) order. Any new CDR generated during the streaming (i.e. till all CDRs are flushed from HDD) will be written to HDD and from there sent to CGF.

In the current implementation, during streaming, GTPP requests are read from HDD and sent to CGF server, till configured max outstanding is reached.

**New Behavior:** In the new “PARALLEL” mode introduced, when the CGF becomes active, CDRs in HDD are streamed at a slower pace. Newly generated CDRs from AAA Managers are sent directly to CGF servers when streaming is in progress. In PARALLEL mode, rate of streaming from HDD will be slow.

Billing domain should be capable of handling Out-Of-Order CDRs in parallel streaming mode.

**Command Changes**

```
gtpp attribute
```

The existing streaming CLI is extended to add a new mode of streaming “parallel”.

```
configure

  context context_name
```
**GTPP Changes in Release 16**

```plaintext
gtpp group group_name

gtpp storage-server mode streaming parallel

default gtpp storage-server mode

end
```

Notes:

- **streaming**: In this mode, when the CGF becomes active, CDRs in HDD are streamed in a First-In-First-Out order. Any new CDR generated during the streaming (till all CDRs are flushed out from HDD) will be written to HDD and from there sent to CGF.

- **parallel**: In this mode, when the CGF becomes active, CDRs in HDD are streamed at slower pace. Newly generated CDRs are sent directly to CGF servers.

---

**CSCuh30721 - Stranded CDR on ICSR automated solution**

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

**Feature Changes**

**Automation in Transferring Stranded CDRs**

In the event of chassis failure, the CDRs will remain on HDD until the chassis becomes active. This feature provides a way to move the stranded CDRs from the new standby chassis to the new active chassis and stream them to the OCG.

**Previous Behavior:** CDRs from current standby chassis were manually transferred to current active chassis using the CLI command "gtpp storage-server streaming start". Once the transfer is complete, a CLI command in the Exec mode was configured to stream the CDRs to CGF.

**New Behavior:** The stranded CDRs in the standby ICSR node (moved from active to standby) are automatically transferred to the newly active ICSR node. This automation process is achieved through the use of "gtpp push-to-active url" CLI command in the Global Configuration mode.

**Customer Impact:** This feature could lead to duplicate CDRs. When streaming is in progress and ICSR switchover happens, the current file being streamed, will not complete the streaming as interface with CGF went down. This file will be transferred to new active chassis and streamed from beginning from new chassis. The accounting contexts should be in same order in both the chassis. The directory names are created using vpn-id. If the accounting contexts are in different order, vpn-id will be different and the sub-directories in HDD will be different in both the chassis for same GTPP group.

**Command Changes**

`gtpp push-to-active`

This is a new CLI command used to enable the automatic transfer of stranded CDRs to active chassis.

```plaintext
configure
gtpp push-to-active url url via-context context_name
```
no gtpp push-to-active

end

Notes:

- **url**: This keyword denotes the peer chassis URL in this format: sftp://user:password@host:[port]/hd-raid/records/cdr/. This keyword accepts a string of size 1 to 1024.

- **context name**: This is the context name through which the active chassis is reachable. **context name** must be an alphanumeric string of 1 through 79 characters.

- This CLI is applicable only to GTPP groups having streaming mode.

**gtpp storage-server streaming start**

This command is obsolete in release 16.0. This CLI was used to start streaming after manually transferring CDR files to new active chassis.

**Performance Indicator Changes**

**show gtpp storage-server streaming file statistics**

The following fields are removed from the output of this show command as these were used for the manual transfer of stranded CDRs.

- Total Files moved to active
- Total CDRs moved to active

**show gtpp storage-server streaming file statistics**

The following new fields are added in support of this feature.

- Automatic File Transfer Statistics
  - Total Gtpp-Groups transferred
  - Total Files transferred
  - File Transfer Status
  - Total file transfer initiated count
  - Total file transfer stopped count

**CSCui95971, CSCuj13956 - Rel10 Compliance for SGW-CDRs**

**Applicable Products**: S-GW

**Feature Changes**

**3GPP Rel. 10 Compliant SGW-CDRs**

**Previous Behavior**: S-GW dictionaries “custom24” and “custom35” were earlier compliant to 3GPP Rel. 8 spec.
New Behavior: The GTPP dictionaries for SGW-CDRs “custom24” and “custom35” are now partially Rel. 10 compliant.

The following new attributes are added to these custom dictionaries:

- S-GW Address IPv6
- Serving Node IPv6 Address
- P-GW Address IPv6

In support of this feature, these existing attributes “IMSI Unauthenticated Flag” and “Dynamic Address Flag extension” are also added to custom24 and custom35 GTPP dictionaries.

Command Changes

gtpp attribute

Three new attributes are added to this command to support Release 10 SGW-CDR compliance.

configure
  context context_name
  gtpp group group_name
  [ no ] gtpp attribute { pgw-ipv6-addr | sgw-ipv6-addr | sna-ipv6-addr }
end

Notes:
- These new attributes can be controllably configured in custom24 and custom35 SGW CDR dictionaries.

CSCuj99515 - Disabling the triggers for closing CDR service containers.

Applicable Products: P-GW

Feature Changes

Suppression of LOSDV Addition Trigger Generated for DCCA and Service Idle Out Triggers

Previous Behavior: CLI was not available to disable DCCA and service-idle out triggers for CDR generation.

New Behavior: With this release, configurable options are provided to disable the addition of LOSDV in PGW-CDR for DCCA generated triggers and when a service idles out.

Command Changes

gtpp trigger

Two new keywords options “service-idle-out” and “dcca” are added to the GTPP Group configuration to provide an option to disable the closure of Service container for PGW-CDRs.
configure
c
context context_name
gtpp group group_name
gtpp trigger { service-idle-out | dcca }
no gtpp trigger { service-idle-out | dcca }
end

CSCul23630 - Change the max outstanding configuration for GTPP

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

Feature Changes

Max Outstanding Configuration for GTPP

Currently, the CLI command “gtpp server server_address max ” allows the max value (max-outstanding requests with CGF server) to be configured up to 255. But actually in the GTPP stack, there is an additional restriction because of which the actual limit is 100. A warning message is displayed if the user tries to configure a value greater than 100 and the max-outstanding is configured as 100.

Command Changes

gtpp server

There are no changes to this CLI command except for displaying a warning message when the user tries to configure the max outstanding value greater than 100. This is because there is an internal limit in configuring the max-outstanding requests with CGF server.

c
context context_name
gtpp group group_name
gtpp server ip_address max msgs
no gtpp server ip_address
end

CSCul77461 - aaaproxy in warn state during call model run

Applicable Products: S-GW
Feature Changes

Limited GTPP Group Configuration for APN

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 3 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 per APN.

**New Behavior:** Now there is a limit of configuring only up to six GTPP groups per APN. 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 due to AAA proxy kill as CDRs are archived in AAA manager when AAA proxy goes to warn state.

CSCul88752 - Std GTPP dictionaries should support multiple data record format version

**Applicable Products:** S-GW

Feature Changes

Support for Multiple Data Record Format Versions

**Previous Behavior:** Currently, the value of the data record format version was taken according to the GTPP dictionary being used. Due to this, same data record format version was maintained for all 3GPP Release versions i.e. for Rel. 8, Rel. 9 and Rel. 10.

With default configuration, because of version mismatch the GTPP request was discarded while using Rel.10 attributes.

**New Behavior:** A new CLI command “gtpp data-record-format-version” is being introduced to configure the data record format version for the GTPP group.

With this release, the data record format version can be configured based on the 3GPP release version.

**Important:** This behavioral change is applicable only to custom24 standard and custom35 GTPP dictionaries for S-GW.

Command Changes

`gtpp data-record-format-version`

This is a new command to configure the data record format version for the GTPP group.

**Important:** This behavioral change is applicable only to custom24 standard and custom35 GTPP dictionaries for S-GW.
configure

context context_name
  gtpp data-record-format-version version_num
  no gtpp data-record-format-version
end

Notes:
  - data-record-format-version: Configures the data record format version to be encoded. The version should be of format “a.b” indicating 3GPP release version.
  - By default, the data record format will be encoded based on the GTPP dictionary used.

Performance Indicator Changes

show configuration verbose

The following new field has been added to the output of this show command.
  - gtpp data-record-format-version

CSCum14682 - The tag values of ambr uplink and downlink should be made 3gpp compliant

Applicable Products: S-GW

Feature Changes

Change in ASN Tag Values of apnAmbrUplink and apnAmbrDownlink Attributes

Previous Behavior: During the initial implementation, the tag values of “apnAmbrUplink” and “apnAmbrDownlink” attributes were not present in 3GPP standards. So, proprietary values (50 and 51) were used for these uplink and downlink attributes respectively.

New Behavior: Now the tag values of “apnAmbrUplink” and “apnAmbrDownlink” attributes are modified as 7 and 8 to be compliant with 3GPP standards.

Important: This behavioral change is applicable to all GTPP dictionaries for S-GW except custom34 and custom35 as these dictionaries are already using 3GPP compliant values for apn-ambr attribute.

Customer Impact: Customers should adjust for the mentioned changes in APN-AMBR tag values.

CSCum55255 - behavior change in PGW-CDR

Applicable Products: P-GW
Feature Changes

Correction to PGW-CDR IE Name

The Information Element (IE) “packet count” has been changed to “packetCount”. This IE is present in the record Extension field of custom35 GTPP dictionary for P-GW.

CSCum72801 - custom24 dictionary not supporting qos req/neg length >15 in CDRs

Applicable Products: SaMOG, SGSN

Feature Changes

Configuration Option for QoS Maximum Length

Previous Behavior: For all SGSN GTPP dictionaries, the maximum length of QoS was restricted to either 12 or 15.

New Behavior: Now, CLI configuration option is provided to accept the maximum length of QoS up to 24. This feature is introduced to support Rel.7+ QoS formats.

Command Changes

gtppp attribute

qos max-length is a new keyword in this command added to modify the length of QoS sent in CDR.

configure

context context_name

gtppp group group_name

gtppp attribute qos max-length qos_value

no gtppp attribute qos

end

Notes:

- qos max-length qos_value: This option is used to modify the length of QoS sent in CDR.
  The qos_value must be an integer from 4 through 24.

Performance Indicator Changes

show configuration

The following new field has been added to the output of this show command to display the configured value of QoS length.
• qos max-length

show configuration verbose

The following new field has been added to the output of this show command to display the configured value of QoS length.

• qos max-length

show gtpp group

The following new field has been added to the output of this show command to display the configured value of QoS length.

• qos max-length

CSCum76702 - CDR File transfer of Stranded CDR at new standby is very slow

Applicable Products: GGSN

Feature Changes

Increased Range for max server CLI to Support Stranded CDR Feature

Previous Behavior: The range for the CLI command “max server” used to configure the number of sshd server connections is 1 through 40.

New Behavior: For Stranded CDR feature, the chassis can schedule to push a maximum of 4000 files. To support this, the range for “max server” command is increased to 1-4000.

Customer Impact: The default value (40) is not changed. So, there is no impact on any customer.

CSCum99631 - To add ps fci related fields to custom43.

Applicable Products: P-GW

Feature Changes

PS FCI based CDR Handling in custom43 Dictionary

Previous Behavior: For custom43 GTPP dictionary, with OCS enabled, in 15.0, when PS-FCI was received on Gy in CCR-I CCA-I exchange, CDR was generated with causeForRecClosing as FCI Change.

New Behavior: In this release, CDR will not be generated for custom43 during initial handshake i.e. on initial exchange of CCR-I and CCA-I messages.
Chapter 8
HeNBGW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 16 software releases.
HeNBGW Enhancements for 16.1

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 *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 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

---

**CSCtx74503 - HENBGW: Access side SCTP params configuration template support**

**Feature Changes**

**SCTP Parameter Configuration support**

Configuration changes to associate the template for access service, show config changes to highlight the association and show command changes in the access service to indicate the template associated and the sctp values applied in the service.

**Previous Behavior:** Only SCTP default parameter will apply to both the service.

**New Behavior:** SCTP parameters can be configured as per the global level parameter template configured values.

**Customer Impact:** Gives flexibility to configure SCTP tunable parameters for the access service towards HeNB and network service towards MME.
Command Changes

`associate sctp-param-template`

New command `associate sctp-param-template` is introduced in this release.

```
configure

henbgw-access-service  henbgw_access_svc
associate sctp-param-template  param_template_name
no associate sctp-param-template
end
```

Performance Indicator Changes

`show henbgw-access-service all`

Below SCTP parameters are introduced in this release for `show henbgw-access-service all` command.

- SCTP Param Template Associated
- SCTP Param Timestamp
- SCTP Alpha
- SCTP Beta
- SCTP Checksum Type
- SCTP Valid Cookie Lifetime
- SCTP Max Assoc Retrans
- SCTP Max Number of In Streams
- SCTP Init Retransmissions
- SCTP Max MTU
- SCTP Max Number of Out Streams
- SCTP Max Path Retransmissions
- SCTP Min MTU
- SCTP RTO Initial
- SCTP RTO Max
- SCTP RTO Min
- SCTP Sack Frequency
- SCTP Sack Period
- SCTP Start MTU
- SCTP Heartbeat Status
• SCTP HeartBeat Timer
• SCTP Bundle Status
• SCTP Bundle Timer
• SCTP Alternate Accept Flag

CSCtx74512 - HENBGW: Network side SCTP params configuration template support

Feature Changes

SCTP Parameter Configuration support

Configuration changes to associate the template for network service, show config changes to highlight the association and show command changes in the network service to indicate the template associated and the scpt values applied in the service.

Previous Behavior: Only SCTP default parameter will apply to both the service.

New Behavior: SCTP parameters can be configured as per the global level parameter template configured values.

Customer Impact: Gives flexibility to configure SCTP tunable parameters for the access service towards HeNB and network service towards MME.

Command Changes

associate sctp-param-template

New command associate sctp-param-template is introduced in this release.

configure

henbgw-network-service henbgw_network_svc
associate sctp-param-template param_template_name
no associate sctp-param-template
end

Performance Indicator Changes

show henbgw-network-service all

Below SCTP parameters are introduced in this release for show henbgw-network-service all command.

• SCTP Param Template Associated
• SCTP Param Timestamp
• SCTP Alpha
- SCTP Beta
- SCTP Checksum Type
- SCTP Valid Cookie Lifetime
- SCTP Max Assoc Retrans
- SCTP Max Number of In Streams
- SCTP Init Retransmissions
- SCTP Max MTU
- SCTP Max Number of Out Streams
- SCTP Max Path Retransmissions
- SCTP Min MTU
- SCTP RTO Initial
- SCTP RTO Max
- SCTP RTO Min
- SCTP Sack Frequency
- SCTP Sack Period
- SCTP Start MTU
- SCTP Heartbeat Status
- SCTP HeartBeat Timer
- SCTP Bundle Status
- SCTP Bundle Timer
- SCTP Alternate Accept Flag

### CSCtz94825 - HeNBGW IPSec: Need to support Certificate based IKEv2 authentication

**Feature Changes**

**Certificate based IKEv2 authentication**

This is a mandatory requirement from 3GPP standards 33.320 v10.5. HeNBGW prior to this release was supporting only EAP-AKA authentication mechanism. With this verification, HeNBGW is more aligned to the 3GPP standards.

**Previous Behavior:** SW support for this feature was not verified for HeNBGW product.

**New Behavior:** SW support for this feature is now verified for HeNBGW product.
CSCun51912 - HENBGW: Need support for displaying secgw detail under henbgw access svc

Feature Changes

SECGW support for HENBGW Access Service

Performance Indicator Changes

show henbgw-access-service -all

Below output is introduced in this release for show henbgw-access-service all command.

- Security GW service Address
- Security GW Context
- Crypto-Template
- Service in IPSec
HeNBGW Enhancements for 16.0

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.

**CSCtx74447 - HENBGW: S1-MME over IPV6 support for HENBGW network side**

**Feature Changes**

**S1-MME over IPV6**

S1-MME over IPV6 should be supported for HENBGW network side.

**Previous Behavior:** The Network Service in HeNBGW supports IPv4 address for binding logical Enodebs to communicate with MME (with multi-homing).

**New Behavior:** Supports IPv6 address on S1-MME interface, towards MME (with multi homing).

**Customer Impact:** IPv6 Support in HeNBGW Network Service is now available.

**Command Changes**

```
bind sl-mme

IPv6 support for HENBGW network side.

configure

  context context_name

  henbgw-network-service service_name

bind sl-mmeipv6-address addr_val max-subscribers max_sub

mme-pool

Mme pool configuration in lte-policy.

configure

  lte-policy

  henb mme-pool pool_name
```
Feature Changes

S1-MME over IPV6 support

Previous Behavior: The access service in Henbgw supports IPv4 address for binding access service to communicate with HEnodeBs.

New Behavior: This feature enhances the product by supporting IPv6 address on S1-MME interface, towards HEnodeB.

Customer Impact: Support for IPv6 address in access service of Henbgw.

Command Changes

```plaintext
[no] bind s1-mme

class

context context_name

henbgw-access-service service_name

bind s1-mme { ipv4-address | ipv6-address } addr_val max-subscribers max_sub

no bind s1-mme

end
```

Feature Changes

IPv6 PDN Support

With this release, HeNBGW supports IPv6 PDNs.

Feature Changes

IPv4v6 PDN Support
With this release, HeNBGW supports IPv4v6 PDNs.

**CSCuh88668 - HeNBGW: 3GPP release 10 S1AP support**

**Feature Changes**

**3GPP release 10 S1AP support**

- Release 10 3GPP 36.413 (specifically v10.5) support.
  - **Previous Behavior:** Release 9.5 3GPP support.
  - **New Behavior:** Release 10.5 3GPP support
  - **Customer Impact:** Standards upgrade.

**CSCuh89047 - HeNBGW: X2 Handover support**

**Feature Changes**

**X2 Handover support between two HENBs**

- Support for X2 handovers between 2 HENBs.
  - **Previous Behavior:** X2 handover between 2 HENBs now supported.
  - **New Behavior:** Supports X2 handover between 2 HENBs.
  - **Customer Impact:** X2 handover between 2 HENBs possible.

**CSCuh92913 - HENBGW: AP trace using HeNB ID or IP**

**Feature Changes**

**AP trace using HeNB ID or IP**

- **Previous Behavior:** AP(subscriber) cannot be traced.
  - **New Behavior:** The AP (subscriber) can be traced via “monitor subscriber ipaddr”.
  - **Customer Impact:** AP can be traced using HeNB ID or IP.

**Performance Indicator Changes**

```
monitor subscriber
```

- Individual AP tracing using monitor subscriber can be done with two options: monitor subscriber <IP Address> and monitor subscriber <Global enb ID>

```
monitor subscriber ipaddr ip_address
```

CSCuh95440 - HENBGW Session recovery enhancements

Feature Changes

HENBGW session recovery enhancements

Session recovery enhancements.

Previous Behavior: No session recovery for HENBGW SCTP/UE Sessions.

New Behavior: Recover HENBGW SCTP/UE session in case of sessmgr crash or restart.

Customer Impact: No call disconnect in case of sessmgr restart.

Command Changes

```
henb session-recovery
```

New command `henb session-recovery` is introduced in this release.

```
configure

  henbgw session-recovery [ idle-timeout secs ]

no henbgw session-recovery

end
```

CSCum08897 - KT HeNBGW : Trap support for Congestion control

Feature Changes

Trap support for Congestion control

Previous Behavior: No trap support to generated when Critical/Major/Minor Congestion thresholds exceed or drop.

New Behavior: SNMP Traps are generated when Critical/Major/Minor Congestion thresholds exceed or drop.

Performance Indicator Changes

New Traps introduced

New traps introduced for HNEBGW service introduced.

- starEnhancedCongestion
- starEnhancedCongestionClear
CSCul94489 - KT HeNBGW : HeNBGW does not send HB REQ after primary path recovery

Feature Changes

HB REQ after primary path recovery

**Previous Behavior:** only support 2 SCTP paths.

**New Behavior:** Multi-homing support is now extended with path management.

CSCuj62727 - HeNBGW-nsvc : Cli to reflect multihomed log enb - mme assoc paths

Feature Changes

mme assoc paths

**Previous Behavior:** Henbgw MME association does not reflects the path states in the current association.

**New Behavior:** Henbgw MME association now reflects the path states in the current association.

Command Changes

```
henb session-recovery
```

New command `henb session-recovery` is introduced in this release.

Performance Changes

```
show henbgw-network-service mme-association full all
```

With this release, the following fields have been introduced:

- HenbgwMgr
- Peerid
- MME Pool Name
- HENBGW Network Service Name
- HENBGW Network Service Address
- HENBGW Network Service Port
- MME IP Address:
  - Primary
  - secondary
- MME Port
- Relative MME Capacity
- Path Source IP Address
- Path Destination IP Address
- Path State
- Path Source IP Address
- Path Destination IP Address
- Path State
- Path Source IP Address
- Path Destination IP Address
- Path State
Chapter 9
HNBGW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from HNBGW in StarOS 16 software releases.
HNBGW Enhancements for 16.1

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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 HNBGW.

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

---

**CSCuc09745 - ASR5K-HNBGW-00141 - Cell Broadcast Service support - Phase 2**

**Important:** For this release, only bulkstats support is available.

---

**Cell Broadcast Service support - Phase 2**

For this release Cell Broadcast Service Support - Phase 2 is provided.
CSCun30746 - [HNBGW] RUA connect for emergency-call fails if newcall policy is reject

Feature Changes

Handling emergency calls during IURH handoff

Handling for emergency calls changed during IURH handoff

**Previous Behavior:** When a UE with establish cause normal having emergency IUs was undergoing IURH relocation, it was subject to congestion and other checks and was liable to get dropped.

**New Behavior:** When a UE with establish cause normal having emergency IUs undergoes IURH relocation, the UE is changed to emergency UE and hence it will not get dropped due to congestion, access control etc.

CSCuc09745 - ASR5K-HNBGW-00141 - Cell Broadcast Service support - Phase 2

---

**Important:** For this release, this feature is Lab/Trial Quality only.

Performance Indicator Changes

**show configuration**

Output of this CLI is updated to show information regarding newly added configuration CLIs in configuration.

```plaintext
cbs-service cbs1
  bind address 193.168.151.2

cbc-server address 193.168.151.1 port 3452 secondary-address 193.168.151.3 port 3452
tcp-keepalive idle-timeout 65 max-retransmission-count 4 interval 15
cbc-address-validation
tcp-mode server-only
sabp-class2-aggregation timeout 8
end
```

**show configuration verbose**

Output of this CLI is updated to show information regarding newly added config CLIs in configuration.

```plaintext
cbs-service cbs1
  bind address 193.168.151.2
```
cbc-server address 193.168.151.1 port 3452 secondary-address 193.168.151.3
no tcp-keepalive
no cbc-address-validation
tcp-mode server-only
no sabp-class2-aggregation
exit

CSCup01809 - [CBS] Incorrect value of CLI "sabp timer <timer_value>"

Important: For this release, this feature is Lab/Trial Quality only.

Feature Changes

sabp timer value

sabp timer value corrected.

Important: The tested limit for HNB's registered for SABP messages is 65K.

Previous Behavior: Default sabp value - 10 sec, Range - 1 to 300 sec
New Behavior: Default sabp value - 5 sec, Range - 1 to 20 sec
HNBGW Enhancements for 16.0

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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 HNBGW.

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

---

**CSCuc30440 - ASR5K-HNBGW-00151 - Femto to Femto Handover (Iurh interface, 3GPP R10)**

**Feature Changes**

**Femto to Femto Handover**

Femto to Femto handover based on the 3GPP R10 (TS 25.467) Iurh interface shall be supported.

**Previous Behavior:** Femto to Femto handoff supported with anchor point as CN.

**New Behavior:** Femto to Femto handoff supported with anchor point as HNBGW.

**IURH based F2F Handoff Requirements**

The IURH interface to connect UEs between HNBs is defined in 3GPP. Following is the protocol stack of the IURH interface:
HNBGW will not route messages at IP level as well as not terminate RNA. HNBs will talk to each other over proprietary interface directly.

CSCui37617, CSCuc30447 - ASR5K-HNBGW-00161 - Zonal Presence/Application services API support

Feature Changes

API support for Zonal Presence/Application services

Zonal Presence/Application services API support shall be supported.

**Previous Behavior:** Information of HNB sessions is not sent to MINE server.

**New Behavior:** HNBGW is equipped to send information of HNB sessions to MINE server depending on VSA named 'Presence' sent by AAA and its overriding.

**Customer Impact:** The requirements of Customer regarding MINE are fulfilled.

MINE (Mobile and IP Network Enabler) Client referred as IPNE Client for HNBGW cloud service provides a central portal for wireless operators and partners to share and exchange session/network information to realize intelligent services. A MINE client component running on various network nodes like PGW and HNBGW within operator's network to collect and distribute session/network information to MINE servers. The client is named i.e. IP Network Enabler.

CSCui37416 - Enhanced signalling scaling - UE registrations and paging fanout

Feature Changes

Enhanced signalling scaling - UE registrations and paging fanout

New paging phase feature based on Grid-id of last known HNB that comes in between previous two phases is introduced.

**Previous Behavior:** Two phases were used for paging the UE. Phase 1 - uses last known HNB to locate UE and Phase 2 - uses paging area to locate the UE.

**New Behavior:** Paging is done based on Grid-id of last known HNB that comes in between previous two phases.

Enhanced Signalling Scaling

Grid based paging is the way to find a UE amongst the HNBs by the HNBGW. Paging is complicated for the below reasons:
• UE can be in idle/unregistered state when HNBGW tries to page HNBs
• UE may not be at the HNB from which it was registered the last time
• Some HNBGW deployments may have around 500K active HNBs and it is not favorable to page all to locate the UE
• There are policies and optimizations to stop HNBGW from flooding the network with paging requests

CSCul04859 - IPNE: Need support for unsolicited notification

Feature Changes

Need support for unsolicited notification

**Previous Behavior:** No support for unsolicited notification.

**New Behavior:** Support for configuring and triggering unsolicited notifications now available.

**Customer Impact:** Ability to configure for notifications without requirement of having explicit subscriptions installed.
Chapter 10
HSGW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from HSGW in StarOS 16 software releases.
HSGW Enhancements for 16.0

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 *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 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

---

**CSCuc34742 - [HSGW]: Incorrect DSCP marking done on A11**

**Feature Changes**

**Enhancement of DSCP marking**

Previously, DSCP value was copied as Type of Service (TOS) in the IP header of the control packets.

This TOS consists of the following:

- **Differentiated Services Code Point (DSCP): From MSB 6 bits** - This was originally defined as the Type of service field. This field is now defined by RFC 2474 for Differentiated services (DiffServ).

- **Explicit Congestion Notification (ECN): Last 2 bits or from LSB 2 bits** - This field is defined in RFC 3168 and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.
**Previous Behavior:** DSCP was part of TOS but DSCP value was copied as TOS.

**New Behavior:** Configured DSCP directly copied into TOS, where this (DSCP) value has to be copied as MSB 6 bits.

*Important:* This new behavior is only applicable if the `all-signaling-packets ip-header-dscp` is configured inside PDSN/HSGW and FA/HA service configuration.

**Customer Impact:** DSCP will be updated properly to TOS.

---

**CSCuc87231 - HSGW, PGW support Pmipv6 control protocol over ipv4**

**Feature Changes**

**HSGW and P-GW support for Pmipv6 control protocol over ipv4**

**Previous Behavior:** Previously, mag-service could only bind with IPv6 address.

**New Behavior:** With this new behavior, mag-service is capable of binding on IPv4 interface as well.

**Command Changes**

```
bind address
```

A new keyword `ipv4-address` has been added to bind MAG service with IPv4 address.

```
configure
  context context_name
    mag-service service_name
      bind ipv4-address ip_address
      no bind ipv4-address
    end
```

---

**CSCud56103 - HSGW Support MSISDN in PBU to PGW through S2a interface**

**Feature Changes**

**HSGW Support MSISDN in PBU to P-GW through S2a interface**

*Important:* For this release, this feature is Lab/Trial Quality only.
**Previous Behavior:** The HSGW read the MSISDN information from the Diameter message that was sent from the 3GPP AAA. However, the HSGW did not insert the MSISDN into the PBU message. Therefore, the P-GW did not receive the MSISDN information from the HSGW over the S2a interface.

**New Behavior:** The HSGW reads the MSISDN information from the Diameter message which is received from the 3GPP AAA and it inserts the MSISDN into the PBU message. It is then delivered to the P-GW through the S2a interface.
Chapter 11
InTracer Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from InTracer in 16.0 software releases.
InTracer Enhancements for 16.3

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the InTracer 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.

CSCuj46241 - SGSN v 1.1 Header Support

**Feature Changes**

**Support for v1.1 SGSN header**

With SGSN v1.1 header support, the following changes are done:

1. R-Intracer will always send version 1 in heart beat response back to SGSN.
2. R-Intracer will decode TLV tag counts as per IPMS header version.
Chapter 12
IPSG Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from IPSG in StarOS 16 software releases.
IPSG Enhancements for 16.0

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

---

**CSCtr43130 - Support to check lawful-intercept statistics per context level**

**Feature Changes**

**Support for Viewing Lawful Intercept Statistics per Context Level**

All products supporting Lawful Intercept previously supported the viewing of system-wide statistics only. Support is now available for viewing Lawful Intercept statistics at a specified context level. For more information on Lawful Intercept, contact your Cisco representative.

**Previous Behavior:** Lawful Intercept statistics were available only as an aggregate for all LI contexts.

**New Behavior:** Lawful Intercept statistics are now available on a per context level.

**Customer Impact:** New keyword option in `show lawful-intercept statistics` command.
CSCug58900 - Combo IPSG+GGSN required

Feature Changes

IPSG and GGSN Combination

With this release, both GGSN and IPSG services can run colocated on the same ASR 5000 platform. While GGSN handles the Framed-Route AVP from AAA in the Auth-Accept messages, IPSG handles overlapping IPs using VLANs on the Sn interface. IPSG will create eGCDRs, and GGSN creates GCDRs for charging.

CSCui90453 - IPSG+GGSN qualification on ASR5500

Feature Changes

IPSG and GGSN Combination on the ASR 5500

With this release, both GGSN and IPSG services can run colocated on the same ASR 5500 platform.

CSCui90463 - IPSG qualification on SSI

Feature Changes

IPSG on QvPCI-SI Platform

With this release, IPSG is fully qualified on the Quantum vPCI (QvPCI) virtual platform.
Chapter 13
MME Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from the MME in StarOS 16 software releases.
MME Enhancements for 16.5

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

---

**CSCur19886, CSCus74843 - 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.
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 100kbps(<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 100kbps(<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.

CSCus82793 - MME Re-locate UE command to expand range from 0-65536

Feature Changes

Expanded ‘mme-group-id’ Range

MME uses configured values for IMSI, mme-group-id, mme-code, and m-tmsi to identify UEs to relocate.

**Previous Behavior:** The operator could configure a value for the ’mme-group-id’ (as part of the mme relocate-ue command under the Execute mode) from the range 32678 to 65536.

**New Behavior:** The range has been exanded and the operator now can configure a value for the ‘mme-group-id’ (as part of the mme relocate-ue command under the Execute mode) from the range 0 to 65536. This range now matches the configurable range for MME group-id with the mme-id command in the MME service configuration mode.

**Customer Impact:** MME uses this configuration to relocate UEs using IMSI, mme-group-id, mme-code and m-tmsi. Now the MME can relocate subscribers using GUTI-relocate commands for group-ids less than 32768. This allows inter-RAT HO as the GUTI Relocation command in the NAS message to the UE includes a broader range of MME Group IDs as defined with the mme relocate-ue command in the Execute mode.

Command Changes

mme relocate-ue

The range of values for the mme-group-id keyword has been expanded from 32768 to 65535 to 0 to 65535. This command is issued from the Execute mode:

mme relocate-ue imsi imsi_value new-guti mme-group-id mme_group_id mme-code mme_code_value m-tmsi m-tmsi_value
Notes:

- `mme_group_id`: Enter an integer from 0 to 65535 to specify the GUTI Group ID the MME is to use to relocate subscribers using the GUTI Relocation command in the NAS message to the UE.
MME Enhancements for 16.4

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

---

CSCup36013 - Missing TAI bulkstats variable: tai-emm-msgtx-csg-not-subscribed

**Feature Changes**

**Added Missing TAI Bulk Stat**

**Previous Behavior:** The `tai-emm-msgtx-csg-not-subscribed` bulk stat was not pegging and also was not included in the output generated by the `show bulkstat` command.

**New Behavior:** The `tai-emm-msgtx-csg-not-subscribed` bulk stat is now pegging properly and is included in the output generated by the `show bulkstat variables tai` command. This bulk stats maps to "MME_STATS_ENUM_MSG_ATTACH_REJECT_CAUSE_25".
Performance Indicator Changes

tai Schema

Missing stat added to the tai schema for pegging and display.

- tai-emm-msgtx-csg-not-subscribed

CSCuq57243 - MME does E-RAB release at the end of CS HO

Feature Changes

MME Sends UE Context Release after CS HO

Modifications in this release impact the handling of MME call flows to the UE/eNodeb-side after an SRVCC (Single Radio Voice Call Continuity) procedure completes in a scenario where calls are handed between VoLTE and legacy Circuit Switched systems for CS-only handover.

**Previous Behavior:** During the bearer deletion process, the MME used to send an E-RAB Release to the eNodeB at the end of the SRVCC procedure. Typically, the eNodeB responded to the MME’s E-RAB Release with a NAS Non-Delivery message because the UE moved to another RAT due to handover.

**New Behavior:** Now at the end of the CS-only handover SRVCC procedure, the MME sends a UE Context Release, in place of an E-RAB Release, with the cause ‘Successful-handover’. This ensures the eNodeB can properly respond to the Release message and behave appropriately at both the radio-side and the UE-side.

**Customer Impact:** Reduces signaling to the eNodeB.

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

CSCur27407 - NewConnectionsDisallowed SNMP trap firing a lot

Feature Changes

Processing SessMgr Location

Previous Behavior: When the SessMgr Location procedure failed during the MME's processing of a received request (Attach / TAU request with FGUTI, GTPv2 Forward Relocation request, and GTPv1 Forward Relocation request), then the MME rejects the request and sends a trap "MMENewConnectionsDisallowed" with reason "location of sessmgr resource failed".

New Behavior: If the SessMgr Location procedure fails during the MME's processing of a received request (Attach / TAU request with FGUTI, GTPv2 Forward Relocation request, and GTPv1 Forward Relocation request), then a new SessMgr is allocated, the request is processed, and the MME does not send the trap "MMENewConnectionsDisallowed" with reason "location of sessmgr resource failed".

Customer Impact: Fewer requests rejected.

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.

---

**CSCur52162 - Parser error for initial-ue msgs with nas-pdu length from than 127 bytes**

**Feature Changes**

**Parser Code Correctly Decodes Length More than 127 Bytes**

**Previous Behavior:** If an "Initial UE" message was received at an MME demux manager, with the length of the "NAS-PDU" IE more than 127 bytes, then such messages were forwarded to a random Session Manager.

**New Behavior:** If an "Initial UE" message is received at an MME demux manager, with the length of the "NAS-PDU" IE more than 127 bytes, then such messages are now forwarded directly to the specific host Session Manager if the subscriber is known at the MME.

**Customer Impact:** This helps to avoid unnecessary signaling to the MME in situations where the subscriber is already known by the MME.

---

**CSCur73766 - TAU Reject Cause 0 after Auth Req Timeout**

**Feature Changes**

**Prevent Sending of TAU Reject**

**Previous Behavior:** TAU Reject was sent in situations where F-GUTI TAU Failure occurred due to Authentication Request Timeout.

**New Behavior:** TAU Reject is no longer sent in situations where F-GUTI TAU Failure occurs as a result of Authentication Request Timeout.

**Customer Impact:** By not sending TAU Reject in such situations, signalling should be reduced on released S1AP (or radio connection) from an eNB.

---

**CSCur89996 - MME releases UE context with Category NAS : Unspecified for Radio issues**

**Feature Changes**

**Configuring the Cause Code Mapping for UE-CONTEXT-RELEASE Sent from MME**
**Previous Behavior:** By default, when a UE was in connected state with an MME and whenever the MME received a TAU Request over Initial-UE, then the MME initiated a UE-CONTEXT-RELEASE with cause NAS-Unspecified.

**New Behavior:** Now, by default, an MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a TAU Request over Initial-UE if the UE is in the connected state. As well, the CLI has been changed to enable the operator to configure a preferred cause code for init-ue-from-enodeb-for-tau.

**Customer Impact:** This change only impacts a customer if the customer update their KPI calculation based on this cause.

**Command Changes**

`sl-ue-context-release`

This new CLI command enables the operator to specify the cause code to be sent in UE-CONTEXT-RELEASE initiated by the MME upon the reception of TAU Request over INITIAL-UE message when a UE is in connected state.

```
configure
  context context_name
    mme-service service_name
      sl-ue-context-release reason init-ue-from-enodeb-for-tau cause type { nas value nas_value | radio value radio_value }
    default sl-ue-context-release reason init-ue-from-enodeb-for-tau cause
  end
```

**Notes:**

- This CLI enables the operator to configure the MME cause code mapping to be sent in a UE-CONTEXT-RELEASE message initiated from MME due to the reception of TAU procedure on Initial-UE message from the same eNB or from a different eNB. The configured cause code will be sent in the UE-CONTEXT-RELEASE message whenever MME releases the existing S1AP connection upon receiving a TAU procedure in an Initial-UE message.
- Currently, the only release reason possible is ‘init-ue-from-enodeb-for-tau’.
- There are two cause options for which cause code values can be assigned:
  - `nas value nas_value` options are:
    - 0 - Normal Release (default value)
    - 1 - Authentication Failure
    - 2 - Detach
    - 3 - Unspecified
    - 4 - CSG Subscription Expiry
  - `radio value radio_value` must be an integer from 0 to 38.
MME Changes in Release 16

MME Enhancements for 16.4

Release Change Reference, StarOS Release 16

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 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.

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 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.

```plaintext
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
MME Enhancements for 16.3

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 *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

---

CSCuq52247 - SIM-less emergency attach failure when UE does not support EIA0&EEA0

**Feature Changes**

**Emergency Attach Handling with No SIM**

When an emergency call was attempted without a SIM from a UE that does not support EIA0 and EEA0 (i.e., NULL) algorithms, the attach procedure failed. The MME rejected the emergency attach request immediately with attach reject cause: ILLEGAL MS(0x3).

**Previous Behavior:** The MME rejected the emergency call when UE initiated emergency call with IMEI as identifier, if the network capability did not include algorithms including NULL (EIA0/EEA0).

**New Behavior:** The MME now proceeds with SMC using NULL algorithms. This applies only if the ue-validation-level in lte-emergency-profile is set to NONE.
Customer Impact: NULL algorithms are mandated by the 3GPP TS 33.401. This behavior is seen only if a UE is misbehaving. In such case, instead of dropping the call, the MME proceeds with the assumption that UE shall process SMC with NULL algorithms.

CSCup87477 - Card Busy-out CLI on PSC card in the MME causes loss of Service

Feature Changes

Handling of Existing Subscribers During Card Busy-Out

Previous Behavior: When the card busy out is enabled on a certain PSC card in the MME, the expected behaviour is that no new calls (IMSI attaches) attach to this card and the existing users upon detach (GUTI based attaches), would reattach to another card in the same MME. However, when existing users detach (GUTI based attaches) and reattach, they were unable to get service in LTE, as the MME did not assign them to another session manager.

On getting request from already known subscriber, IMSIMgr attempts to send to SessMgr hosting those subscriber. If SessMgr is suspended, the call is dropped and it will keep happening until subscriber info is available at IMSIMgr.

New Behavior: For this scenario, the subscriber info will be cleared from the IMSI Manager and calls will be forwarded to other Session Managers.

Customer Impact: Better KPIs (lesser retransmission) in case of suspended Session Manager (card busy out).
MME Enhancements for 16.2

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 *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**

**CSCum50504 - MME doesn’t release resources after receiving DDN from SGW**

**Feature Changes**

**DDN with RNC Failure Handling**

**Previous Behavior:** When the S-GW triggered a DDN with cause of `EGTP_CAUSE_ERROR_IND_RCVD_RNC_ENODE`, the MME replied immediately with DDA with cause of `EGTP_CAUSE_UNABLE_TO_PAGE_UE`, however the MME did not release the S1 and it did not page the UE.

**New Behavior:** DDN with RNC failure is now handled correctly in connected mode.
CSCuo13234 - MME behavior when receiving NAPTR response with empty flag

Feature Changes

Behavior Change for NAPTR Response RR with Non-terminal Flag

When the MME initiates a NAPTR query toward the DNS and receives a response with an empty ("") flag (nonterminal), the MME follows up with an A record query rather than issuing a further NAPTR query as mandated in RFC3958. This results in the MME failing to resolve APN to P-GW on roamer's home network.

**Previous Behavior:** Non-terminal NAPTR response resource record (RR) does not trigger another NAPTR query.

**New Behavior:** The MME now supports a single level redirection of NAPTR queries which have non-terminal (empty) flag in NAPTR response RR.

**Customer Impact:** Non-terminal NAPTR response RR will trigger another NAPTR query.

CSCuo17932 - MME sending old QoS values to UE after HO from 2G>4G>2G

Feature Changes

External Messaging Behavior Change

**Previous Behavior:** When a subscriber comes to the MME from SGSN, the MME was always sending 4G Native QOS in GMM QOS IE in NAS messages, and re-sending the obsolete QOS value received by SGSN earlier to SGSN in case of a subsequent handoff to GN/GP SGSN.

**New Behavior:** A new command is provided which controls which QOS the MME uses in NAS GMM QOS IE and GTPV1 Context response messages during a handover or inter-rat TAU with a GN/GP SGSN.

The MME can either send the QOS sent from peer SGSN, or the native EPS (4G) QOS value received from HSS. The default behavior is to send the native EPS (4G) QOS to the SGSN.

Command Changes

```
nas gmm-qos-ie-mapping

This new command controls which QOS the MME uses in NAS GMM QOS IE and GTPV1 Context response message during a handover or inter-rat TAU with a GN/GP SGSN.

configure

   context context_name

      mme-service <mme_svc_name>

      nas gmm-qos-ie-mapping { native-eps-qos | gngp-imported-qos }

[ default ] nas gmm-qos-ie-mapping

end
```
Notes:
- The default behavior is to use the native EPS QOS.

Performance Indicator Changes

show mme-service all

The `show mme-service all` command now displays the configuration of this command in the following field:
- NAS GMM QOS Mapped From

CSCuo24135 - SLs: show sls-service peers all CLI output can display mmemgr ID too

Performance Indicator Changes

show sls-service peers

The output for the `show sls-service peers` command has been enhanced to include the MME Manager instance number for each peer connection. The following sample output shows the new MM fields in bold text:

```
[local]asr5000# show sls-service peers all
Total ESMLC:2

    MM  ESMLC-ID  AssocStatus  Uptime  Peer-ID  IP-Addresses-1[state]  IP-address-2[state]
          --------  ----------  --------  --------  ------------------------  ------------------------
       06     1          DOWN  00h00m00s  100925441  192.80.80.73[DOWN]  n/a
       07    150          DOWN  00h00m00s  117637121  192.80.80.71[DOWN]  n/a
```

CSCup29345 - Need MMEmgr CPU and Memory bulkstat counter for MME capacity monitoring

Feature Changes

Bulk Statistic Enhancements

**Previous Behavior:** CPU and memory related bulkstats were not available at the card-level for MMEMGR tasks for performance measurements.

**New Behavior:** The following information can now be collected:
- Total number of mmemgr tasks across all CPUs on this card.
- Average percentage of CPU utilization of all mmemgr tasks across all CPUs on this card.
• Average percentage of allocated memory utilization of all mmemgr tasks across all CPUs on this card.
• Maximum percentage of CPU utilization of the busiest mmemgr task across all the CPUs on this card.
• Maximum percentage of allocated memory utilization of the peak mmemgr task across all CPUs on this card.

Performance Indicator Changes

Card Schema

The following bulk statistics have been added to the Card schema to display card-level information for MME Manager tasks:

- task-mmemgr-num
- task-mmemgr-avgcpu
- task-mmemgr-avgmem
- task-mmemgr-maxcpu
- task-mmemgr-maxmem

CSCup44359 - [CMAS]: Need to restructure few SBC counters for better clarity

Performance Indicator Changes

SBc Schema

The following new bulk statistics have been added to the SBc schema to collect additional information about the number of Write-Replacement Responses and Stop-Warning Responses sent:

- sbcap-transdata-wrwresp-warn-bcast-not-oper
- sbcap-transdata-wrwresp-mme-capacity-exceeded
- sbcap-transdata-stopresp-warn-bcast-not-oper
- sbcap-transdata-stopresp-mme-capacity-exceeded

show sbc statistics

The output of the show sbc statistics command has been changed to clarify counters when Write-Replacement-Warning-Request and Stop-Warning-Request messages are not successful.

Since both the positive and negative causes were previously reported under "Successful", the "Unsuccessful" counter has been removed, and additional success causes (Warning-Broadcast-Not-Operational and Message-Accepted) are now reported.

The following sample shows the new output of this command with the new fields highlighted:

SBc Statistics:

Transmitted SBc Data:

Total Transmitted: 0
Transmit Errors:

Transport Errors: 0
Encode Failures: 0
No buffers: 0
Write Replace Warning Response: 0
Tracking Area Not Valid: 0
MME Capacity Exceeded: 0
Warn Bcast Not Operational: 0
Message Accepted: 0
Stop Warning Response: 0
Tracking Area Not Valid: 0
MME Capacity Exceeded: 0
Warn Bcast Not Operational: 0
Message Accepted: 0
Error Indication: 0

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)
CSCup58544 - sessmgr Fatal Signal 6 __kernel_vsyscall() - show mme-service db record

Feature Changes

Attach Reject for Invalid IMSI

Previous Behavior: On receiving an ATTACH REQUEST with a 16-digit IMSI, the MME did not reject the attach request.

New Behavior: If an ATTACH_REQUEST is received with an IMSI having more than 15 digits, the MME now responds with an ATTACH REJECT with cause "Invalid Mandatory Information".

CSCup70412 - mmemgr resources not used when eSMLC peers are UP

Performance Indicator Changes

show task resources facility mmemgr all

When an sls-service is started and SLs peer connections to the eSMLC are up, the output of the show task resources facility mmemgr all command now includes the number of MME Manager sessions used by these eSMLC connections in the total session count.

In the following example, there are 480 VLRs plus 8 eSMLC connections, for a total of 488 total sessions.

<table>
<thead>
<tr>
<th>task</th>
<th>cpu facility</th>
<th>cputime</th>
<th>memory</th>
<th>files</th>
<th>sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>inst</td>
<td>used allc</td>
<td>used alloc</td>
<td>used allc</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>1 0.6%</td>
<td>95%</td>
<td>64.75M</td>
<td>400.0M</td>
<td>68</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>2 0.7%</td>
<td>95%</td>
<td>66.05M</td>
<td>400.0M</td>
<td>87</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>3 0.6%</td>
<td>95%</td>
<td>65.40M</td>
<td>400.0M</td>
<td>79</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>4 0.6%</td>
<td>95%</td>
<td>64.24M</td>
<td>400.0M</td>
<td>66</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>5 0.6%</td>
<td>95%</td>
<td>65.33M</td>
<td>400.0M</td>
<td>66</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>6 0.6%</td>
<td>95%</td>
<td>65.20M</td>
<td>400.0M</td>
<td>68</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>7 0.6%</td>
<td>95%</td>
<td>65.18M</td>
<td>400.0M</td>
<td>62</td>
</tr>
<tr>
<td>6/0 mmemgr</td>
<td>8 0.5%</td>
<td>95%</td>
<td>64.84M</td>
<td>400.0M</td>
<td>61</td>
</tr>
<tr>
<td>Total</td>
<td>8 5.13%</td>
<td>521.0M</td>
<td>557</td>
<td>488</td>
<td></td>
</tr>
</tbody>
</table>
MME Enhancements for 16.1

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 *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

---

**CSCuh68156 - Demux failover with 32k eNBs, Assert=mmemgr_add_flow_aggregate()**

**Feature Changes**

**eNodeB Association Throttling**

**Previous Behavior:** An MME manager failure could occur when the NPU was unable to handle a large number of flow installation requests (for eNodeB SCTP flows).

**New Behavior:** If the eNodeB association rate is more than the rate that NPU can handle for flow installation, the MME will abort those eNodeB associations.
CSCuh92041 - MME is not sending Destination-Host AVP in LRR

Feature Changes

Support for Sending Destination-Host AVP in LRR

Previous Behavior: The MME did not send the Destination-Host AVP in Location Report Requests (LRR) to the GMLC.

New Behavior: To comply with 3GPP TS29.172, the Destination-Host AVP is now sent to the GMLC for all the LRR messages initiated by MME.

A new CLI has been provided to configure the destination-host AVP in location-service. If this command is not configured, the peer host name configured in the diameter endpoint is encoded as destination-host AVP.

Command Changes

destination-host

This new command configures the destination-host AVP in this location service.

configure

context context_name

location-service svc_name

  destination-host destination-host

  no destination-host

end

Notes:

- destination-host must be a string from 1 to 63 characters.
- If the destination-host is not configured, the peer name configured in the diameter endpoint will be encoded as destination-host AVP. This will be useful if there are multiple GMLCs in the network.

Performance Indicator Changes

show location-service

The show location-service service all command has been enhanced to display the configuration of the Location Service command mode destination-host command, either the configured GMLC host name or NA.

- Destination Host
**CSCui56181, CSCui56247, CSCuh80306, CSCuh80313, CSCuh80317, CSCuo63213 - MME: SLs interface support**

**Feature Changes**

**SLs Interface Support**

**Important:** For this release, this feature is Lab/Trial Quality only.

The SLs interface is used to convey LCS Application Protocol (LCS-AP) messages and parameters between the MME to the Evolved Serving Mobile Location Center (E-SMLC). It is also used for tunnelling LTE Positioning Protocols (LPP between the E-SMLC and the target UE, LPPa between the E-SMLC and the eNodeB), which are transparent to the MME.

**Previous Behavior:** The MME would include ECGI for Mobile Terminated (MT) and Network Induced (NI) Location Requests.

**New Behavior:** The E-SMLC is contacted for Location information if the SLs service is configured.

**Customer Impact:** This feature provides enhanced location services capabilities for Network Induced Location Reporting (NI-LR) for emergency attached users and Mobile Terminated Location Reporting (MT-LR) for normal attached users.

**Command Changes**

**sls-service**

This new command creates (or removes) an SLs service to support the SLs interface on the MME.

configure

    context context_name

    [ no ] sls-service svc_name

    end

Notes:

- **svc_name:** must be an alphanumeric string from 1 to 64 characters.
- Up to 4 SLs services can be configured on the system.
- The SLs service name must be unique across all contexts.

**bind**

This new command is used to specify the IP address, port and sctp parameter to be used for the SLs service. The **bind** command is service critical; removing the configuration will stop the SLs service.

configure

    context context_name
sls-service sls_svc_name

    bind [ ipv4-address ipv4_address_value1 [ ipv4-address ipv4_address_value2 ] | ipv6-address ipv6_address_value1 [ ipv6-address ipv6_address_value2 ] [ port port_num ] ]
sctp-template sctp_param_template_name

    no bind

end

Notes:
- Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes.
- The SCTP template is mandatory for the SLs Service to start.

esmlc

This new command configures an Evolved Serving Mobile Location Center (E-SMLC) within the location service. The E-SMLC provides location information to the MME.

configure

    context context_name

    sls-service sls_svc_name

        esmlc esmlc-id esmlc_id_value { ipv4-address ipv4_address_value1 [ ipv4-address ipv4_address_value2 ] | ipv6-address ipv6_address_value1 [ ipv6-address ipv6_address_value2 ] } port port_num weight weight-val

        no esmlc-id esmlc_id_value

end

Notes:
- Up to 8 E-SMLC entries can be configured per SLs service.
- The SLs service is started when the first E-SMLC is configured. The SLs service is stopped when the last E-SMLC is removed.
- Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes.
- **port**: Enter the SCTP port number of the E-SMLC server. `port_num` must be an integer from 1 through 65535.
- **weight**: The MME performs a weighted round robin selection of E-SMLC based on this weight factor. `weight-val` must be an integer from 1 through 5, where 1 represents the least available capacity and 5 represents the greatest.

t-3x01

This new command defines the T-3x01 timer settings.

The T-3x01 timer is started by the MME on sending a location-request to the E-SMLC, and is stopped when either the requested is responded, aborted, or reset by either the MME or the E-SMLC.
configure

context context_name

sls-service svc_name

t-3x01 low-delay seconds delay-tolerant seconds
default t-3x01
end

Notes:
- **low-delay** defines the number of seconds the MME waits for a “low delay” response from the E-SMLC. 
  seconds must be an integer from 10 to 30. The default setting is 20 seconds.
- **delay-tolerant** defines the number of seconds the MME waits for a “delay tolerant” response from the E-SMLC. 
  seconds must be an integer from 10 to 40. The default setting is 20 seconds.

t-3x02

This new command defines the T-3x02 timer settings.
The T-3x02 timer is started on the MME when the MME sends a RESET REQUEST to the E-SMLC. Once the T3x02 timer expires, the MME can resend the RESET REQUEST to the E-SMLC.

configure

context context_name

sls-service svc_name

t-3x02 seconds
default t-3x02
end

Notes:
- **seconds** must be an integer from 1 to 5. The default setting is 3 seconds.

max-retransmissions

This new command configures the maximum number of times the MME will resend the RESET REQUEST to the E-SMLC.

configure

context context_name

sls-service svc_name

max-retransmissions reset retries
default max-retransmissions reset
Notes:

- `retries` must be an integer from 1 to 5. The default setting is 0.

**lcş-qos**

This new command defines the location service QoS settings to be used for this emergency profile.

```plaintext
configure
lte-policy

lte-emergency-profile profile_name

lcs-qos horizontal-accuracy variable [ vertical-accuracy variable ]

no lcs-qos
end
```

Notes:

- Horizontal and vertical positioning accuracy values must be entered as an integer from 0 to 127, where 0 is the most accurate.
- Configuration of these settings is optional. For Emergency Services, the MME will always set the Response Time to Low Delay. If QoS is configured, the horizontal accuracy is mandatory. If a vertical accuracy is specified in this command, the MME will set the Vertical Requested flag.

**associate sls-service**

This new command associates an SLs service with a Location service. The SLS service provides an interface to the E-SMLC in the context of a Location service.

```plaintext
configure

context context_name

location-service location_svc_name

associate sls-service sls_svc_name

[ no ] associate sls-service
end
```

Notes:

- The SLs service is not a critical parameter for Location services, and the removal of the association does not impact the status of the Location service. Any Location service procedures that were using an E-SMLC will get aborted on the removal of an association of SLs service from a Location service. Note that on removal of SLs service association, the MME will send a RESET message. No individual aborts will be sent to different E-SMLCs configured.
Configures SLS bulk statistics schema.

```
configure
  bulkstats mode
    sls schema schema_name format schema_format
  no sls schema schema_name
end
```

Notes:
- `schema_name` must be an alphanumeric string of 1 through 31 characters.

```
show bulkstats variables sls
```

This command includes the new `sls` keyword to display the SLs schema bulk statistic variables.

```
show bulkstats variables sls [ | { grep  } grep_options | more ]
```

```
logging filter active facility
```

Event logging for the SLs interface can be enabled using the new `sls` keyword in this command.

```
logging filter active facility sls level severity_level
```

```
snmp trap
```

The following command has been modified to enable or disable generation of SNMP traps to track status and conditions for the SLs service.

```
configure
  snmp trap { enable | suppress } { SLSServiceStart | SLSServiceStop }
end
```

The following command has been modified to enable or disable generation of SNMP traps to track status and conditions for the E-SMLC associations.

```
configure
  snmp trap { enable | suppress } { ESMLCAssocDown | ESMLCAssocUp | ESMCAllAssocDown | ESMCAllAssocDownClear }
end
```

```
show sls-service
```

This new command shows configuration information for all SLs services or for the specified SLs service.

```
show sls-service [ all | name svc_name ] [ | { grep grep_options | more } ]
```
show sls-service peers

This new command shows the configuration information of the E-SMLC peers that are connected to the SLs service.

`show sls-service peers [ all | esmlc-id esmlc-id ] [ | { grep grep_options | more } ]`

show sls-service statistics

This new command displays SLs service statistics and/or related SCTP statistics. These statistics can be filtered based on SLs service name or E-SMLC id.

`show sls-service statistics [ name svc_name ] [ sls | sctp ] [ esmlc-id esmlc-id ] [ | { grep grep_options | more } ]`

clear sls-service statistics

This new command clears all SLs service statistics and/or related SCTP statistics. This command can be filtered based on SLs service name or E-SMLC id.

`clear sls-service statistics [ name svc_name ] [ sls | sctp ] [ esmlc-id esmlc-id ] [ | { grep grep_options | more } ]`

Performance Indicator Changes

**MME Schema**

The following new bulk statistics variables have been added to the MME schema to collect NAS and S1-AP statistics relating to location procedures.

- `emm-msgtx-dn-gen-nas-tpt`
- `emm-msgrx-up-gen-nas-tpt`
- `s1ap-up-ue-lppa`
- `s1ap-dn-ue-lppa`
- `s1ap-up-non-ue-lppa`
- `s1ap-dn-non-ue-lppa`

**SLS Schema**

The new SLS bulk statistics schema has been introduced to enable collection of the following statistics:

- `vpname`
- `vpnid`
- `servname`
- `servid`
- `sctp-transdata-init`
- `sctp-transdata-initack`
- `sctp-transdata-shut`
- sctp-transdata-shutack
- sctp-transdata-cookie
- sctp-transdata-cookieack
- sctp-transdata-data
- sctp-transdata-dataack
- sctp-transdata-shutcomp
- sctp-transdata-hb
- sctp-transdata-hback
- sctp-transdata-abort
- sctp-transdata-error
- sctp-recdata-init
- sctp-recdata-initack
- sctp-recdata-shut
- sctp-recdata-shutack
- sctp-recdata-cookie
- sctp-recdata-cookieack
- sctp-recdata-data
- sctp-recdata-dataack
- sctp-recdata-shutcomp
- sctp-recdata-hb
- sctp-recdata-hback
- sctp-recdata-abort
- sctp-recdata-error
- sctp-retransdata-init
- sctp-retransdata-shut
- sctp-retransdata-shutack
- sctp-retransdata-cookie
- sctp-retransdata-data
- sctp-totsent-bytes
- sctp-totrec-bytes
- sctp-totsent-pkts
- sctp-totrec-pkts
- slsap-transdata-reset
- slsap-transdata-resetack
- slsap-transdata-loc-req
- slsap-transdata-loc-abort
- slsap-transdata-conn-info
- slsap-transdata-nonconn-info
- slsap-recvdata-reset
- slsap-recvdata-resetack
- slsap-recvdata-loc-resp
- slsap-recvdata-conn-info
- slsap-recvdata-nonconn-info

**show location-service**

The `show location-service` command has been enhanced to show the following additional configuration settings.

- SLS service
- Destination Host

**show lte-policy lte-emergency-profile name**

The `show lte-policy lte-emergency-profile name` command has been enhanced to show the configured Location Service (LCS) Quality of Service (QoS):

- LCS QOS:
  - Horizontal Accuracy
  - Vertical Accuracy

**show mme-service db record**

The `show mme-service db record imsi` and `show mme-service db record guti` commands have been enhanced to show the last known location of the UE that was derived using the E-SMLC. The following section shows sample output of the new fields:

**ESMLC Location Estimate**

--------------------------------

Location:

  Type: Point

  Co-ordinates: North 245, 3000

Positioning Data:

Positioning Data Set

<table>
<thead>
<tr>
<th>Type</th>
<th>Result</th>
<th>Used for computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CellId</td>
<td>Attempted Successfully</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Type: OTDOA        Attempted Unsuccessfully          No

GNSS Positioning:

<table>
<thead>
<tr>
<th>Method</th>
<th>Type</th>
<th>Result</th>
<th>Used for computation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE-Based</td>
<td>GPS</td>
<td>Successful</td>
<td>Yes</td>
</tr>
<tr>
<td>Conventional</td>
<td>SBAS</td>
<td>Unsuccessful</td>
<td>No</td>
</tr>
</tbody>
</table>

Velocity Estimate:

Horizontal: Bearing 120 Velocity: 256
Requested Accuracy Fulfilled: Yes

**show sls-service all**

This new command shows configuration information for the SLs service(s).

- Service name
- Service id
- Context
- Status
- Bind
- SLs-MME IP Address
- SCTP Port
- T-3x01 (Low Delay)
- T-3x01 (Delay Tolerant)
- T-3x02
- Max Re-Transmission
- SCTP Param Template Associated
- SCTP Alpha
- SCTP Beta
- SCTP Checksum Type
- SCTP Valid Cookie Lifetime
- SCTP Max Assoc Retrans
- SCTP Max Number of In Streams
- SCTP Init Retransmissions
- SCTP Max MTU
- SCTP Max Number of Out Streams
- SCTP Path Retransmissions
- SCTP Min MTU
- SCTP RTO Initial
- SCTP RTO Max
- SCTP RTO Min
- SCTP Sack Frequency
- SCTP Sack Period
- SCTP Start MTU
- SCTP Heartbeat Status
- SCTP HeartBeat Timer
- SCTP Bundle Status
- SCTP Bundle Timer
- SCTP Alternate Accept Flag

**show sls-service peers all**

This new command shows the configuration information of the E-SMLC peers that are connected to the SLS service.

- ESMLC-ID
- AssocStatus
- Uptime
- Peer-ID
- IP-Addresses-1[state]
- IP-Address-2[state]

**show sls-service statistics**

This new command displays SLs service statistics and/or related SCTP statistics. These statistics can be filtered based on SLs service name or E-SMLC id.

**SLS-AP Statistics:**

**Sent Messages:**

- Location Request: 0
- Connection Info: 0
- Reset Request: 0

**Received Messages:**

- Location Response: 0
- Connection Info: 0
- Reset Ack: 0
### SCTP Statistics:

**Transmitted SCTP Data:**

<table>
<thead>
<tr>
<th>Chunk Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Init Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Cookie Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Cookie Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Data Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Data Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Complete Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Heartbeat Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>HeartBeat Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Error Chunks:</td>
<td>0</td>
</tr>
</tbody>
</table>

**Received SCTP Data:**

<table>
<thead>
<tr>
<th>Chunk Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Init Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Cookie Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Cookie Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Data Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Data Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Complete Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Heartbeat Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>HeartBeat Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Error Chunks:</td>
<td>0</td>
</tr>
</tbody>
</table>

**Retransmitted SCTP Data:**

<table>
<thead>
<tr>
<th>Chunk Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Shutdown Ack Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Cookie Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Data Chunks:</td>
<td>0</td>
</tr>
<tr>
<td>Total Bytes Sent:</td>
<td>0</td>
</tr>
<tr>
<td>Total Bytes Received:</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Sent:</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets Received:</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**CSCuj68851 - MME TAC level EMM procedure counter support**

**Feature Changes**

**TAI Based Statistics**
The MME now provides enhanced statistics at the TAI level (MCC/MNC/TAC). A new TAI bulk statistics schema has been introduced for collection of this data, and the `show mme-service statistics` command has been enhanced to display statistics for a given TAI management database name and TAI (MNC/MCC/TAC).

By default these statistics are tracked at a per eNodeB level. A configuration option is provided to change the collection mode to per TAI level. This collection mode configuration is available per MME service.

**Customer Impact:** TAI based statistics help operators localize failures to a particular geographical area. They also provide statistics on the load generated on the MME from different geographies, and help in network planning.

### Command Changes

**tai schema**

Configures TAI (Tracking Area Identifier) bulk statistics schema.

```plaintext
configure
  bulkstats mode
    tai schema schema_name format schema_format
    no tai schema schema_name
  end

Notes:
  * `schema_name` must be an alphanumeric string of 1 through 31 characters.
```

**statistics**

This new command configures the statistics collection mode for the MME service.

```plaintext
configure
  context context_name
    mme-service mme_svc_name
      statistics collection-mode { enodeb | tai } [ -noconfirm ]
      default statistics collection-mode [ -noconfirm ] cmd
  end
```

⚠️ **Caution:** Changing this collection mode will restart the MME service and will clear all statistics at the MME service and eNodeB level.

Notes:
- Use this command to collect statistics for this MME service at the eNodeB level (default), or at the TAI level.
- When configured to collect statistics per TAI, the MME will collect statistics only for the TAs that are configured in the LTE TAI Management Database that is associated with the MME service.
• If a specific TAI is configured within multiple TAI Management Databases, the records collected for that TAI will be a sum of all counters for all TAI Management Databases to which it belongs.

show bulkstats variables tai

This command includes the new tai keyword to display the TAI schema bulk statistic variables.

show bulkstats variables tai [ | { grep | grep_options | more } ]

show mme-service statistics

This command includes the following new keywords:

tai taiddb db_name mcc mcc mnc mnc tac tac

These keywords are used to display TAI statistics for the specified TAI management database name and MCC/MNC/TAC.

show mme-service statistics [ tai taiddb db_name mcc mcc mnc mnc tac tac ] [ verbose ] [ | { grep | grep_options | more } ]

clear mme-service statistics

This command includes the following new keywords:

tai all

taiddb db_name

These keywords are used to clear all TAI statistics, or clear TAI statistics for the specified TAI management database name.

clear mme-service statistics [ tai all | taiddb db_name ] [ verbose ] [ | { grep | grep_options | more } ]

Performance Indicator Changes

TAI Schema

The new TAI bulk statistics schema has been introduced to enable collection of the following statistics. For information about each statistic, refer to the TAI Schema chapter of the ASR 5x00 Statistics and Counters Reference.

• tai-mnc
• tai-mcc
• tai-tac
• tai-mnc-len
• tai-epsattach-attempted
• tai-epsattach-success
• tai-epsattach-failures
• tai-combinedattach-attempted
• tai-combinedattach-success
• tai-combinedattach-failures
• tai-combinedattach-success-eps
• tai-epsattach-emergency-attempted
• tai-epsattach-emergency-success
• tai-epsattach-emergency-failures
• tai-intra-tau-attempted
• tai-intra-tau-success
• tai-intra-tau-failures
• tai-intra-ta-la-update-attempted
• tai-intra-ta-la-update-success
• tai-intra-ta-la-update-failures
• tai-intra-ta-la-update-success-eps
• tai-intra-imsi-tau-attempted
• tai-intra-imsi-tau-success
• tai-intra-imsi-tau-failures
• tai-intra-imsi-tau-success-eps
• tai-tau-periodic-attempted
• tai-tau-periodic-success
• tai-tau-periodic-failures
• tai-inter-tau-attempted
• tai-inter-tau-success
• tai-inter-tau-failures
• tai-inter-ta-la-update-attempted
• tai-inter-ta-la-update-success
• tai-inter-ta-la-update-failures
• tai-inter-ta-la-update-success-eps
• tai-emmevent-detachueinit-attempted
• tai-emmevent-detachueinit-success
• tai-emmevent-detachueinit-failures
• tai-ecmevent-ue-srvcreq-attempt
• tai-ecmevent-ue-srvcreq-success
• tai-ecmevent-ue-srvcreq-failure
• tai-ecmevent-nw-srvcreq-attempt
• tai-ecmevent-nw-srvcreq-success
- tai-emmevent-nw-srvereq-failure
- tai-paging-attempted
- tai-emmevent-x2ho-attempt
- tai-emmevent-x2ho-success
- tai-emmevent-x2ho-failure
- tai-emmevent-s1ho-apply
- tai-emmevent-s1ho-success
- tai-emmevent-s1ho-failure
- tai-emmm-msgtx-attach-accept
- tai-emmm-msgtx-attach-accept-retx
- tai-emmm-msgtx-attach-accept-imei-unknown
- tai-emmm-msgtx-attach-accept-no-msc
- tai-emmm-msgtx-attach-accept-nw-fail
- tai-emmm-msgtx-attach-accept-congestion
- tai-emmm-msgtx-attach-accept-no-cs
- tai-emmm-msgtx-attach-reject
- tai-emmm-msgtx-imsi-unknown-hss
- tai-emmm-msgtx-illegal-ue
- tai-emmm-msgtx-illegal-me
- tai-emmm-msgtx-eps-not-allowed
- tai-emmm-msgtx-network-failure
- tai-emmm-msgtx-decode-failure
- tai-emmm-msgtx-imei-not-accept
- tai-emmm-msgtx-ue-identity-unk
- tai-emmm-msgtx-impl-detached
- tai-emmm-msgtx-roaming-restrict-ta
- tai-emmm-msgtx-plmn-not-allow
- tai-emmm-msgtx-no-suitable-cell-ta
- tai-emmm-msgtx-ta-not-allow
- tai-emmm-msgtx-eps-non-eps-not-allowed
- tai-emmm-msgtx-no-eps-svc-plmn
- tai-emmm-msgtx-esm-failure
- tai-emmm-msgtx-attach-rej-unknown-apn
- tai-emmm-msgtx-attach-rej-gw-reject
• tai-emm-msgtx-attach-rej-gw-auth-failed
• tai-emm-msgtx-attach-rej-svc-not-supported
• tai-emm-msgtx-attach-rej-svc-not-subscribed
• tai-emm-msgtx-attach-rej-insuff-resources
• tai-emm-msgtx-attach-rej-activation-reject
• tai-emm-msgtx-attach-rej-svc-temp-out-of-order
• tai-emm-msgtx-attach-rej-protocol-error
• tai-emm-msgtx-attach-rej-apn-restrict-incompatible
• tai-emm-msgtx-service-reject
• tai-emm-msgtx-service-reject-no-brrs
• tai-emm-msgtx-service-reject-no-csg
• tai-emm-msgtx-service-reject-ta-no-allwd
• tai-emm-msgtx-service-reject-no-roam-in-ta
• tai-emm-msgtx-service-reject-no-cells-in-ta
• tai-emm-msgtx-tau-accept
• tai-emm-msgtx-tau-accept-retx
• tai-emm-msgtx-tau-accept-imsi-unknown
• tai-emm-msgtx-tau-accept-no-msc
• tai-emm-msgtx-tau-accept-nw-fail
• tai-emm-msgtx-tau-accept-congestion
• tai-emm-msgtx-tau-accept-no-cs
• tai-emm-msgtx-tau-inter-accept
• tai-emm-msgtx-tau-inter-accept-retx
• tai-emm-msgtx-tau-inter-accept-imsi-unknown
• tai-emm-msgtx-tau-inter-accept-no-msc
• tai-emm-msgtx-tau-inter-accept-nw-fail
• tai-emm-msgtx-tau-inter-accept-congestion
• tai-emm-msgtx-tau-inter-accept-no-cs
• tai-emm-msgtx-tau-intra-accept
• tai-emm-msgtx-tau-intra-accept-retx
• tai-emm-msgtx-tau-intra-accept-imsi-unknown
• tai-emm-msgtx-tau-intra-accept-no-msc
• tai-emm-msgtx-tau-intra-accept-nw-fail
• tai-emm-msgtx-tau-intra-accept-congestion
- tai-emm-msgtx-tau-intra-accept-no-cs
- tai-emm-msgtx-tau-reject
- tai-emm-msgtx-tau-imsi-unknown-hss
- tai-emm-msgtx-tau-illegal-ue
- tai-emm-msgtx-tau-illegal-me
- tai-emm-msgtx-tau-eps-not-allowed
- tai-emm-msgtx-tau-network-fail
- tai-emm-msgtx-tau-decode-failure
- tai-emm-msgtx-tau-no-bearer-active
- tai-emm-msgtx-tau-ue-identity-unk
- tai-emm-msgtx-tau-implicit-detached
- tai-emm-msgtx-tau-imei-not-accept
- tai-emm-msgtx-tau-roaming-restrict-ta
- tai-emm-msgtx-tau-plmn-not-allow
- tai-emm-msgtx-tau-no-suitable-cell-ta
- tai-emm-msgtx-tau-ta-not-allow
- tai-emm-msgtx-tau-no-eps-svc-plmn
- tai-emm-msgtx-tau-csg-not-subscribed
- tai-emm-msgtx-tau-eps-non-eps-not-allowed
- tai-emm-msgtx-tau-inter-reject
- tai-emm-msgtx-tau-inter-imsi-unknown-hss
- tai-emm-msgtx-tau-inter-illegal-ue
- tai-emm-msgtx-tau-inter-illegal-me
- tai-emm-msgtx-tau-inter-eps-not-allowed
- tai-emm-msgtx-tau-inter-network-fail
- tai-emm-msgtx-tau-inter-decode-failure
- tai-emm-msgtx-tau-inter-no-bearer-active
- tai-emm-msgtx-tau-inter-ue-identity-unk
- tai-emm-msgtx-tau-inter-implicit-detached
- tai-emm-msgtx-tau-inter-imei-not-accept
- tai-emm-msgtx-tau-inter-roaming-restrict-ta
- tai-emm-msgtx-tau-inter-plmn-not-allow
- tai-emm-msgtx-tau-inter-no-suitable-cell-ta
- tai-emm-msgtx-tau-inter-ta-not-allow
The `show mme-service statistics tai taidb` command has been enhanced to display TAI statistics for the specified TAI management database name and MCC/MNC/TAC. The following section shows a sample output of this command:

**EMM Statistics:**

**Attach Request: EPS Only:**
- Attempted: 1  Success: 1
- Failures: 0

**Attach Request: Combined:**
- Attempted: 0  Success: 0
- Success EPS Only: 0  Failure: 0

**Attach Request: Emergency:**
Attempts: 0  Success: 0
Failures: 0

Intra MME TAU Request:
TA Updating:
Attempts: 0  Success: 0
Failures: 0

TA/LA Updating:
Attempts: 0  Success: 0
Success EPS Only: 0  Failure: 0

TA Updating with IMSI Attach:
Attempts: 0  Success: 0
Success EPS Only: 0  Failure: 0

Periodic TAU:
Attempts: 0  Success: 0
Failures: 0

Inter MME TAU Request:
TA Updating:
Attempts: 0  Success: 0
Failures: 0

TA/LA Updating:
Attempts: 0  Success: 0
Success EPS Only: 0  Failure: 0

Detaches UE Initiated:
Attempts: 0  Success: 0
Failures: 0

ECM Statistics:
UE Initiated Service Request Events:
Attempts: 0  Success: 0
Failures: 0
NW Initiated Service Request Events:

- Attempted: 0  Success: 0
- Failures: 0

Paging Initiation:

- Attempted: 1

Handover Statistics:

- X2-based handover:
  - Attempted: 0  Success: 0
  - Failures: 0
- S1-based handover:
  - Attempted: 0  Success: 0
  - Failures: 0

EMM Control Messages:

Sent:

- Attach Accept: 1  Retransmissions: 0
- IMSI Unknown in HSS: 0  MSC Unreachable: 0
- Network Failure: 0  CS Domain Not Available: 0
- Congestion: 0
- Attach Reject: 0
  - IMSI Unknown in HSS: 0  Illegal UE: 0
  - Illegal ME: 0  EPS Not Allowed: 0
  - Network Failure: 0  CSG Not Subscribed: 0
  - Decode Failure: 0  IMEI Not Accepted: 0
  - Roaming Restricted TA: 0  PLMN Not Allowed: 0
  - TA Not Allowed: 0  No suitable cells in TA: 0
  - EPS non-EPS Not Allwd: 0  No EPS Svc in this PLMN: 0
- ESM Failure: 0
- Rejected By PGW/SGW: 0  Authentication Failed: 0
- Svc Opt Not Support: 0  Svc Opt Not Subscribed: 0
Unknown APN: 0  Insufficient Resource: 0
Activation Rejected: 0  Svc Opt Tmp OutOfOrder: 0
Protocol Errors: 0  APN Restrict Incomt: 0
Service Reject: 0
UE Identity Unknown: 0  Implicitly Detached: 0
No Bearer Active: 0  CSG Not Subscribed: 0
Roaming Restricted TA: 0  No Suitable Cells in TA: 0
TA Not Allowed: 0
TAU Accept Total: 0  Retransmissions: 0
IMSI Unknown in HSS: 0  MSC Unreachable: 0
Network Failure: 0  CS Domain Not Available: 0
Congestion: 0
TAU Accept Intra MME: 0  Retransmissions: 0
IMSI Unknown in HSS: 0  MSC Unreachable: 0
Network Failure: 0  CS Domain Not Available: 0
Congestion: 0
TAU Accept Inter MME: 0  Retransmissions: 0
IMSI Unknown in HSS: 0  MSC Unreachable: 0
Network Failure: 0  CS Domain Not Available: 0
Congestion: 0
TAU Reject Total: 0
IMSI Unknown in HSS: 0  Illegal UE: 0
Illegal ME: 0  EPS Not Allowed: 0
Network Failure: 0  IMEI not accepted: 0
Decode Failure: 0  No Bearer Active: 0
UE Identity Unknown: 0  Implicitly Detached: 0
Roaming Restricted TA: 0  PLMN not allowed: 0
TA not allowed: 0  No suitable cells in TA: 0
No EPS Svc in PLMN: 0  CSG Not Subscribed: 0
EPS non-EPS not Allwd: 0

TAU Reject Intra MME: 0

IMSI Unknown in HSS: 0
Illegal UE: 0
Illegal ME: 0
EPS Not Allowed: 0
Network Failure: 0
IMEI not accepted: 0
Decode Failure: 0
No Bearer Active: 0
UE Identity Unknown: 0
Implicitly Detached: 0
Roaming Restricted TA: 0
PLMN not allowed: 0
TA not allowed: 0
No suitable cells in TA: 0
No EPS Svc in PLMN: 0
CSG Not Subscribed: 0
EPS non-EPS not Allwd: 0

TAU Reject Inter MME: 0

IMSI Unknown in HSS: 0
Illegal UE: 0
Illegal ME: 0
EPS Not Allowed: 0
Network Failure: 0
IMEI not accepted: 0
Decode Failure: 0
No Bearer Active: 0
UE Identity Unknown: 0
Implicitly Detached: 0
Roaming Restricted TA: 0
PLMN not allowed: 0
TA not allowed: 0
No suitable cells in TA: 0
No EPS Svc in PLMN: 0
CSG Not Subscribed: 0
EPS non-EPS not Allwd: 0

**CSCum59461, CSCum59592 - SLg Interface - Include MSISDN AVP in procedures**

**Feature Changes**

**Support for MSISDN in Location Services Procedures**

*Important:* For this release, this feature is Lab/Trial Quality only.
Previous Behavior: Location service procedures were supported for both normal and emergency subscribers but with only PSL having IMSI. There was no support for handling PSL with MSISDN alone.

New Behavior: The MME now handles PLR with MSISDN alone as well. The MME also sends SLR for an emergency attached user with MSISDN.

Customer Impact: Together with SLs interface support, this feature provides support for enhanced location services for both normal and emergency attached subscribers based on MSISDN alone as user identity.

CSCun85922 - PDN_Connect by UE rejected during IM exit procedure

Feature Changes

UE PDN Connection Request Message Handling

Previous Behavior: UE PDN connection requests are rejected with "MESSAGE NOT COMPATIBLE WITH THE PROTOCOL STATE(0x65)" error. This occurred when the UE sends the PDN connectivity request before S1AP Initial context setup response is received at MME.

New Behavior: PDN connect is handled and not rejected in this scenario. The MME will now suspend the PDN connect procedure and resume it after completion of IM exit.

CSCuo21484 - Enhance show session subsystem mmemgr CLI for sbc stats

Performance Indicator Changes

show session subsystem facility mmemgr

The output of this command has been enhanced to display the following SBc interface statistics.

Total Services(SBc): 1

SBc Statistics:

Transmitted SBc Data:

Total Transmitted: 0

Transmit Errors:

Transport Errors: 0 Encode Failures: 0

No buffers: 0

Transport Buffer Failure: 0 Encode Buffer Failure 0

Write Replace Warning Response: 0
Successful: 0
Unsuccessful: 0
Tracking Area Not Valid: 0 MME Capacity Exceeded 0
Stop Warning Response:
Successful: 0
Unsuccessful: 0
Tracking Area Not Valid: 0 MME Capacity Exceeded 0
Error Indication: 0

Received SBc Data:
Total Received PDUs: 0 PDU Decode Success 0
Receive Errors: 0
No SBc Association: 0 PDU Decode Failures 0
Write Replace Warning Request: 0
TAI List Not Present: 0
Stop Warning Request: 0
TAI List Not Present: 0
Error Indication: 0
IE Errors: 0

Protocol Error Statistics:
Unknown Procedures: 0 Unknown IEs: 0
Unknown Messages: 0 Missing Mandatory IEs: 0
Transfer Syntax Error: 0 Semantic Error: 0
Message Not Compatible: 0 Others: 0
Abstract Syntax Errors:
Reject: 0 Ignore and notify: 0
Ignore: 0 Falsely Constr Message: 0

SBc Association Statistics:
MME Changes in Release 16

MME Enhancements for 16.1

Total Active: 0  Total Created: 0  Total Closed: 0

CBC Transactions Created: 0  CBC Transaction Failed: 0  CBC Transaction Timeout: 0

SCTP Flows: 0  CBC Not Found: 0

show session subsystem facility mmedemux

The output of this command has been enhanced to display the following SBC interface statistics.

Total SBC Associations Rejected: 0

CSCuo56093 - 'qos ue-ambr max-ul 0 max-dl 0' added automatically in configuration

Feature Changes

Call Control Profile: QoS UE Aggregate Maximum Bit Rate

Previous Behavior: In the Call Control Profile configuration mode, when the qos ue-ambr prefer-as-cap both-hss-and-local minimum command was entered, the system automatically added 'qos ue-ambr max-ul 0 max-dl 0' to the Call Control Profile configuration.

New Behavior: Now the configuration 'qos ue-ambr max-ul 0 max-dl 0' is not automatically added when the qos ue-ambr prefer-as-cap both-hss-and-local minimum command is entered.

In addition, the minimum allowable value (mbr-up and mbr-down) for the qos ue-ambr max-ul mbr-up max-dl mbr-down command has been changed in this release from 0 to 1.

Command Changes

qos ue-ambr

The minimum allowable value for the max-ul and max-dl keywords has been changed in this release from 0 to 1. These values must now be entered as 1 to 1410065408.

configure

   call-control-profile profile_name

   qos ue-ambr max-ul mbr-up max-dl mbr-down

   remove qos ue-ambr
CSCup23821 - NPUMGR Restart causing MME enB SCTP failures and impact to SGs/S1AP

Feature Changes

Statistics and Counters Enhancements

New counters have been added to to the output of the `show session subsystem facility mmemgr` command to display specific packet drop reasons at the MMEMgr.

Several `show` commands now display enhanced information for more clarity and better understanding of any problem in the flow-id creation/deletion process by MMEMgr. Refer to the Performance Indicator Changes section below for complete details.

These enhancements provide additional information to troubleshoot synchronization issues between the MMEMgr and NPUMgr.

Performance Indicator Changes

`show session subsystem facility mmemgr all`

The output of this command has been enhanced to display counters for the following packet drop reasons:

- Incorrect Length - Received PDU length at MED layer is less than Length value found after decoding the IP Packet.
- Oversized PDU - Received PDU length at MED layer is more than DBUF size(10K bytes).
- No Flow exists - There is no SCTP flow existing for the flowId received from underlying layer.
- Flow Inactive Ver - Flow entry is not Active when the message is received.
- Invalid IP Ver - IP Version of the IP packet is not matching with the IP version for the SCTP flow.
- Port Mismatch - Destination SCTP Port of the IP packet is not matching with the SCTP port for the SCTP flow.
- Invalid Protocol - Protocol type is not found to be SCTP in the IP header.

`show mme-service enodeb-association path-info`

The output of this command has been enhanced to display the Flow Id at the MMEMgr level.

- Flow Id

`show mme-service enodeb-association full all`

The output of this command has been enhanced to display the Flow Id at the MMEMgr level.

- Flow Id

The output of this command has also been enhanced to display the individual path status along with flow information.

- Path Source IP Address
• Path Destination IP Address
• Path State
• Flow Id

show sgs-service vlr-status full

The output of this command has been enhanced to display the SCTP flow id. For example:

Assoc Path State

192.80.80.41 192.80.80.33 UP 0x1b046db

CSCup32019 - SLs: MME needs to handle S10 TAU (AF not set) for NI-LR lcs procedure

Feature Changes

Behavior Change for Emergency TAU Attach Without Active Flag Set

Previous Behavior: During a TAU attach, when Active Flag (AF) is not set in TAU request, the UE is moved to idle state.

New Behavior: During inbound TAU of emergency calls, the UE will be moved to connected state even when AF is not set, so that the NI-LR LCS procedure can be successful. This is done only if it is an emergency call and location service is configured. If it is not an emergency call, then the previous behavior will be valid and the UE will move to idle state when AF is not set.

Customer Impact: Support of NI-LR for inbound emergency TAU attach.

CSCzn11186 - MME support for SBc interface (SBc-AP) to Cell broadcast center (CBC)

Feature Changes

SBc-AP interface Support

Important: For this release, this feature is Lab/Trial Quality only.

Previous Behavior: The SBc-AP interface was not supported.

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

The MME complies with the following standards relating to this functionality:

• 3GPP TS29.168 v10.2.0 – Cell Broadcast Centre interfaces with the Evolved Packet Core
Customer Impact: Customers can now enable CMAS functionality in their networks to provide warning notifications to subscribers.

### Command Changes

**sbc-service**

This new command creates (or removes) an SBc service to support the SBc interface on the MME.

```plaintext
configure
  context context_name
    [ no ] sbc-service sbc_svc_name
  end
```

Notes:
- `sbc_svc_name`: must be an alphanumeric string from 1 to 63 characters.
- Up to 8 SGs + MME + SBc + SLs Services can be configured on the system.
- The SBc service name must be unique across all contexts.

**associate sctp-param-template**

This new command specifies the SCTP parameter template to employ for this SBc-AP interface.

```plaintext
configure
  context context_name
    sbc-service sbc_svc_name
      associate sctp-param-template sctp_param_template_name
    no associate sctp-param-template
  end
```

Notes:
- Changes to the configuration will restart the SBc service.
- Configuration of the SCTP parameter template is a pre-requisite for this command.
- Associating the SBc service to the SCTP parameter template is not required for the SBc service to be operational.

**bind**

This new command specifies the IP address to be used for the SBc service.
configure

context context_name

sbc-service sbc_svc_name

   bind { ipv4-address ipv4_address_value1 [ ipv4-address ipv4_address_value2 ] | ipv6-address ipv6_address_value1 [ ipv6-address ipv6_address_value2 ]

   no bind

end

Notes:
- The bind command is service critical; removing the configuration will stop the SBc service.
- Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes.

cbc-associations

This new command configures the maximum number of Cell Broadcast Center (CBC) connections allowed for this SBc service.

configure

context context_name

sbc-service sbc_svc_name

   [ default | no ] cbc-associations maximum number

end

Notes:
- Changes to this configuration will restart the SBc service.
- number must be an integer from 1 to 2.
- Default: 1.

sbc-mme

This new command configures the SCTP port to be used for the SBc interface.

configure

context context_name

sbc-service sbc_svc_name

   sbc-mme sctp port port_num

   [ default | no ] sbc-mme sctp port

end
Notes:
- Changes to the configuration will restart the SBc service.
- \texttt{port\_num} must be an integer from 1 through 65535.
- Default: 29168

\texttt{associate}

This new command associates an MME service with an SBc service.

\texttt{configure}

\begin{verbatim}
context context_name
  mme-service svc_name
    associate sbc-service sbc_svc_name [ context context_name]
  [ no ] associate sbc-service
end
\end{verbatim}

Notes:
- Each MME service can be associated with one unique SBc service.
- The SBc service is \texttt{not} a critical parameter for the MME service. Removing this configuration will \texttt{not} restart the MME service.
- The MME shall always check for a valid SBc service that is up and connected to a CBC before performing any meaningful operations on the Warning Messages received on the S1-AP interface (like attempting to forward the messages).

\texttt{sbc schema}

Configures SBc bulk statistics schema.

\texttt{configure}

\begin{verbatim}
bulkstats mode
  sbc schema schema_name format schema_format
  no sbc schema schema_name
end
\end{verbatim}

Notes:
- \texttt{schema\_name} must be an alphanumeric string of 1 through 31 characters.

\texttt{show bulkstats variables sbc}

This command includes the new \texttt{sbc} keyword to display the SBc schema bulk statistic variables.

\texttt{show bulkstats variables sbc [ | { grep } grep\_options | more ]}
logging filter active facility

Event logging for the SBc interface can be enabled using the new `sbc` keyword in this command.

logging filter active facility sbc level severity_level

snmp trap

The following command has been modified to enable or disable generation of SNMP traps to track status and conditions for the SBc service.

```
configure

    snmp trap { enable | suppress } { SBCServiceStart | SBCServiceStop }

end
```

The following command has been modified to enable or disable generation of SNMP traps to track status and conditions for the CBC associations.

```
configure

    snmp trap { enable | suppress } { CBCAssocDown | CBCAssocUp }

end
```

show sbc-service

This new command shows configuration information for all SBc services, for the specified for the specified SBc service, or for the specified Cell Broadcast Center.

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

show sbc statistics

This new command displays all statistics related to the SBc service. These statistics can be filtered based on peer-id or SBc service name.

```
show sbc statistics { all | peer-id peer_id | sbc-service-name sbc_svc_name } [ verbose | { | grep grep_options | more } ]
```

clear sbc statistics

This new command clears all statistics related to the SBc service. These statistics can be cleared based on peer-id or SBc service name.

```
clear sbc statistics { all | peer-id peer_id | sbc-service-name sbc_svc_name } [ verbose | { | grep grep_options | more } ]
```

Performance Indicator Changes

MME Schema
The following new bulk statistics variables have been added to the MME schema to collect S1-AP data statistics relating to the SBc interface.

- s1ap-transdata-wrwreq
- s1ap-transdata-killreq
- s1ap-recdata-wrwresp
- s1ap-recdata-killresp

**SBC Schema**

The new SBc bulk statistics schema has been introduced to enable collection of the following statistics:

- vpnname
- vpnid
- servname
- servid
- scpt-transdata-init
- scpt-transdata-initack
- scpt-transdata-shut
- scpt-transdata-shutack
- scpt-transdata-cookie
- scpt-transdata-cookieack
- scpt-transdata-data
- scpt-transdata-dataack
- scpt-transdata-shutcomp
- scpt-transdata-hb
- scpt-transdata-hback
- scpt-transdata-abort
- scpt-transdata-error
- scpt-recdata-init
- scpt-recdata-initack
- scpt-recdata-shut
- scpt-recdata-shutack
- scpt-recdata-cookie
- scpt-recdata-cookieack
- scpt-recdata-data
- scpt-recdata-dataack
- scpt-recdata-shutcomp
- sctp-recdata-hb
- sctp-recdata-hback
- sctp-recdata-abort
- sctp-recdata-error
- sctp-retransdata-init
- sctp-retransdata-shut
- sctp-retransdata-shutack
- sctp-retransdata-cookie
- sctp-retransdata-data
- sctp-totsent-bytes
- sctp-totrec-bytes
- sctp-totsent-pkts
- sctp-totrec-pkts
- sbcap-recdata-wrwreq
- sbcap-recdata-wrwreq-tailist-notprsnt
- sbcap-recdata-stopreq
- sbcap-recdata-stopreq-tailist-notprsnt
- sbcap-recdata-errorind
- sbcap-transdata-errorind
- sbcap-transdata-wrwresp-msgaccept
- sbcap-transdata-wrwresp-taiinvalid
- sbcap-transdata-stopresp-msgaccept
- sbcap-transdata-stopresp-taiinvalid
- sbcap-err-tfr-synerr
- sbcap-err-semanticerr
- sbcap-err-msgnotcompatible
- sbcap-err-aserej
- sbcap-err-aseignore-notify
- sbcap-err-asefalsely-constrmsg
- sbcap-cbc-asoc

**show mme-service all**

This command has been enhanced to display the following information about the SBc service which has been associated with each MME service.

- SBc Service Context
• SBc Service

**show mme-service statistics s1ap**

This command has been enhanced to display the following S1-AP statistics relating to the SBc interface. The new fields are highlighted in the sample output below:

**S1AP Statistics:**

**Transmitted S1AP Data:**

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

...  
**Kill Response:** 0  **Write-Replace Warning Response:** 0

**show sbc-service all**

This new command displays the following configuration information about the SBc service(s).

• Service name  
• Context  
• Service-Id  
• Status  
• Bind  
• SBc-MME IP Address  
• SCTP Port  
• Max SBc Associations Allowed  
• SCTP Parameters  
• SCTP Alpha  
• SCTP Beta  
• SCTP Checksum Type  
• SCTP Valid Cookie Lifetime  
• SCTP Max Assoc Retrans  
• SCTP Max Number of In Streams  
• SCTP Init Retransmissions  
• SCTP Max MTU  
• SCTP Max Number of Out Streams  
• SCTP Path Retransmissions
- SCTP Min MTU
- SCTP RTO Initial
- SCTP RTO Max
- SCTP RTO Min
- SCTP Sack Frequency
- SCTP Sack Period
- SCTP Start MTU
- SCTP Heartbeat Status
- SCTP HeartBeat Timer
- SCTP Bundle Status
- SCTP Bundle Timer
- SCTP Alternate Accept Flag

**show sbc-service cbc-associations all**

This new command displays configuration information about the Cell Broadcast Center (CBC) associations for each SBC service. The following section shows a sample output of this command:

<table>
<thead>
<tr>
<th>MM</th>
<th>PEERID</th>
<th>Sbc Service Name</th>
<th>Assoc UpTime</th>
<th>CBC IP:Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>33816577</td>
<td>sbcsvc1</td>
<td>00h00m01s</td>
<td>192.168.101.1:25</td>
</tr>
<tr>
<td>02</td>
<td>33816578</td>
<td>sbcsvc2</td>
<td>00h02m01s</td>
<td>192.168.101.2:25</td>
</tr>
<tr>
<td>02</td>
<td>33816578</td>
<td>sbcsvc2</td>
<td>00h02m01s</td>
<td>192.168.101.3:25</td>
</tr>
<tr>
<td>02</td>
<td>33816578</td>
<td>sbcsvc2</td>
<td>00h02m01s</td>
<td>192.168.101.4:25</td>
</tr>
<tr>
<td>02</td>
<td>33816578</td>
<td>sbcsvc2</td>
<td>00h02m01s</td>
<td>192.168.101.5:25</td>
</tr>
</tbody>
</table>

In the above sample output, the last four entries display a single CBC association with SCTP multi-homing.

**show sbc statistics all**

This new command displays all statistics related to the SBC service.

SBC Statistics:

Transmitted SBC Data:

Total Transmitted: 0

Transmit Errors:

Transport Errors: 0

No Buffers: 0
Transport Buffer Failure: 0
Encode Buffer Failure: 0
Encode Failures: 0
Write Replace Warning Response: 0
Successful: 0
Unsuccessful: 0
Tracking Area Not Valid: 0
MME Capacity Exceeded: 0
Stop Warning Response:
Successful: 0
Unsuccessful: 0
Tracking Area Not Valid: 0
MME Capacity Exceeded: 0
Error Indication: 0
Received SBC Data:
Total Received PDUs: 0
Receive Errors: 0
No SBC Association: 0
PDU Decode Failures: 0
PDU Decode Success: 0
Write Replace Warning Request: 0
TAI List Not Present: 0
Stop Warning Request: 0
TAI List Not Present: 0
Error Indication: 0
IE Errors: 0
Protocol Error Statistics:
Unknown Procedures: 0
Unknown IEs: 0
Unknown Messages: 0
Missing Mandatory IEs: 0
Transfer Syntax Error: 0
Semantic Error: 0
Message Not Compatible: 0
Others: 0
Abstract Syntax Error:
  Reject: 0
  Ignore and Notify: 0
  Falsely Constr Message: 0
SBC Association Statistics:
  Total Active: 0
  Total Created: 0
  Total Closed: 0
  Total Rejected: 0
CBC Transactions Created: 0
CBC Transactions Failed: 0
CBC Transactions Timeout: 0
SCTP Statistics:
  Transmitted SCTP Data:
    Init Chunks: 0
    Init Ack Chunks: 0
    Shutdown Chunks: 0
    Shutdown Ack Chunks: 0
    Cookie Chunks: 0
    Cookie Ack Chunks: 0
    Data Chunks: 0
    Data Ack Chunks: 0
    Shutdown Complete Chunks: 0
    Heartbeat Chunks: 0
    HeartBeat Ack Chunks: 0
    Abort Chunks: 0
    Error Chunks: 0
  Received SCTP Data:
    Init Chunks: 0
    Init Ack Chunks: 0
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Sent: 0</th>
<th>Ack: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown Chunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookie Chunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Chunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown Complete Chunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HeartBeat Ack Chunks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error Chunks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Retransmitted SCTP Data:        |         |        |
| Init Chunks                     |         |        |
| Shutdown Ack Chunks             |         |        |
| Data Chunks                     |         |        |

| Total Bytes Sent:               |         |        |
| Total Bytes Received:          |         |        |
| Total Packets Sent:            |         |        |
| Total Packets Received:        |         |        |
MME Enhancements for 16.0

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
- NAT Enhancements
- NFL Enhancements
- SNMA MIB Enhancements
- System and Platform Enhancements

**CSCtr43130 - Support to check lawful-intercept statistics per context level**

**Feature Changes**

**Support for Viewing Lawful Intercept Statistics per Context Level**

Lawful Intercept on the MME previously supported the viewing of system-wide statistics only. Support is now available for viewing Lawful Intercept statistics at a specified context level. For more information on Lawful Intercept, contact your Cisco representative.

**Previous Behavior:** Lawful Intercept statistics were available only as an aggregate for all LI contexts.

**New Behavior:** Lawful Intercept statistics are now available on a per context level.

**Customer Impact:** New keyword option in *show lawful-intercept statistics* command.
CSCtt33631 - session disconnect-reason - mme-regional-zone-code needs to be removed

Performance Indicator Changes

System Schema

The system disconnect reason `disc-reason-484: mme-regional-zone-code(484)` has been deprecated in this release as it was duplicated by `disc-reason-492: mme-zone-code-validation-failed`.

This disconnect reason (484) is now reused for tracking non-3gpp-access disconnects. Refer to CSCzn16621, CSCzn16622 in this document for more information.

CSCtt40129 - MME(LI)-Support for Request Type TLV in TYPE x14 IRI event

Feature Changes

Request Type TLV Support in Lawful Intercept

Lawful Intercept has been enhanced to send the Request Type TLV. When a PDN connectivity is requested from the mobile to allow multiple PDN connections, a UE requested PDN connectivity event is generated by the MME. The purpose of the Request type information element is to indicate whether the MS requests to establish a new connectivity to a PDN or keep the connection(s) to which it has connected via non-3GPP access.

CSCtt61742 - MME should support configuration to distinguish between HENBGW and eNBs

Feature Changes

Configuration Support for Differentiation Between HeNB-GW and eNodeBs

The MME now can be configured to distinguish the Home eNodeB Gateway (HeNB-GW) from other eNodeBs. This is required to support S1 HANDOVERs to Home eNodeBs connected via a HeNB-GW.

As per 3GPP TS 36.300, section 4.6.2, the TAI used in a HeNB-GW should not be reused in another HeNB-GW. The global eNodeB id of the HeNB-GW can now be configured in the lte-policy.

In case of S1-based handovers to Home eNodeBs served by a HeNB-GW, the lookup at MME for the target eNodeB based on global ENB id will fail, as MME is aware of only the HeNB-GW. In those cases additional lookup needs to be done based on TAI to find the HeNB-GW serving the Home eNodeB.

**Customer Impact:** This feature allows operators to configure the global eNodeB ids of HeNB-GWs in the mme-service. The MME uses this information to perform HeNB-GW related functions.

Command Changes

```
mme henbgw mgmt-db
```
This new command creates a new MME HeNB-GW management database or specifies an existing database and enters the MME HeNB-GW Management Database Configuration Mode.

```
configure
  lte-policy
    mme henbgw mgmt-db db_name
  end

Notes:
  •  `db_name` is an alphanumeric string of size 1 through 64 characters.
```

**henbgw-global-enbid**

This new command configures the Global eNodeB Id and TAI of the HeNB-GW within the MME HeNB-GW management database.

```
configure
  lte-policy
    mme henbgw mgmt-db db_name
    henbgw-global-enbid mcc mcc_value mnc mnc_value enbid enbid_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.
  •  `enbid_number`: Specifies the Global eNodeB ID for this HeNB-GW as an integer value from 1 through 1048575.
  •  A maximum of 8 HeNB-GWs can be configured within the HeNB-GW management database.
```

**associate**

This command includes a new `henbgw-mgmt-db` keyword, which associates the specified HeNB-GW management database with the MME service.

```
configure
  context ctxt_name
    mme-service svc_name
      associate henbgw-mgmt-db db_name
  end
```
Notes:

- `db_name` specifies the name of an LTE MME HeNB-GW Management Database to associate with the MME service as an alphanumeric string of 1 through 64 characters. This is required to support S1 HANDOVERs to Home eNodeBs connected via a HeNB-GW.

Performance Indicator Changes

**show lte-policy henbgw-mgmt-db name**

This command displays the configuration information for the specified MME HeNB-GW management database. For example:

 HenbGW Management DB henbgwl

 HenbGW Global Enbid mcc 123 mnc 456 enbid 12345

**show mme-service name**

This command now displays the name of the MME HeNB-GW management database which has been associated with the specified MME service. For example:

 HenbGW Management DB : henbgwl

**show mme-service enodeb-association full**

The `show mme-service enodeb-association full` command now displays whether the eNodeB is an HeNB-GW. As shown in the following example, the eNodeB Type field will include “(HeNB-GW)”.

 eNodeB Type : Macro (HeNB-GW)

This command also includes a new `henbgw` keyword. When this keyword is used (show mme-service enodeb-association full henbgw), only HeNB-GWs will be displayed in the output.

 eNodeB Type : Macro (HeNB-GW)

**CSCty04851 - Standards-based tracing enhancements**

Feature Changes

**Enhanced Session Tracing Capabilities**

The MME supports standard signaling-based tracing (typically initiated from HSS and distributed from MME to SGW and eNodeB) and management-based initiation of local tracing with the `session trace subscriber` command. In this release, this command has been extended to provide additional configuration for management-initiated trace at MME:

- Propagate trace signaling to adjacent eNodeB, S-GW and P-GW Network Elements (NEs) based on local configuration at MME.
- Limit tracing at other NEs to specified interfaces.
Customer Impact: This feature enables an operator to activate session tracing on eNodeB, S-GW, and P-GW from the MME in order to trace subscriber activity at various points in the network and at various levels of detail. This was only possible from HSS before this feature.

Command Changes

```
session trace subscriber network-element mme
```

This command includes two new keyword options, `target-ne { enb | pgw | sgw }` and `target-all-ne` to specify the target Network Elements (NEs) to propagate the trace. It also includes a new optional keyword `target-interface` to specify the target interfaces to be traced on the specified NEs.

```
session trace subscriber network-element mme { imei id | imsi id | interface { all | interface } | target-all-ne | target-ne { enb [ target-interface { all | interface } ] | pgw [ target-interface { all | interface } ] | sgw [ target-interface { all | interface } ] } trace-ref id collection-entity ip_address
```

```
no session trace subscriber network-element mme [ trace-ref id ]
```

Notes:
- Multiple network elements can be specified using the `target-ne` option.

Performance Indicator Changes

```
show session trace subscriber network-element mme trace-ref
```

This command now shows information about the target network elements and interfaces for the specified trace session, for example:

```
Target Network Elements:

SGW

Target Interfaces:
  S4
  S5
  S8b
  S11
  Gxc

PGW

Target Interfaces:
  S2a
  S2b
```
CSCua84681 - LI: LI Provisioning does support IPv6 address subscriber provisioning

Feature Changes

Support for Lawful Intercept Provisioning of IPv6 Subscriber

Lawful Intercept has been enhanced on the MME to support the provisioning of IPv6 subscriber addresses.

Previous Behavior: Lawful Intercept provisioning supported IPv4 subscriber addresses only.

New Behavior: Lawful Intercept provisioning supports both IPv4 and IPv6 subscriber addresses.

Command Changes

lawful-intercept

This command has been enhanced to add support for the provisioning of IPv6 subscriber addresses.

lawful-intercept ip-addr ipv4addr/ipv6addr

Refer to the Lawful Intercept Configuration Guide for more information.
CSCub06145 - MME: SGS VLR re-selection in case of loss of VLR association

Feature Changes

Automatic VLR Reselection on Failure

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.

In previous releases, the MME supported the manual ability to offload UEs associated with a specific VLR during an SGs association failure or for a planned maintenance window where a VLR would be unavailable.

In this release, this capability has been enhanced to automatically initiate the VLR offload feature when a SGs association failure is detected.

The configuration of this feature allows a detach rate to be configured. This detach rate (in subscribers per 5 second interval) determines the rate at which subscribers are detached.

The existing manual failure handling capability cannot be used simultaneously with this new functionality. The MME will report a command line error if an attempt is made to configure/enable this function if it is currently active.

Customer Impact: This feature provides operators with a more proactive approach to deal with SGs association failures. This enhancement enables the MME to automatically initiate a change in the configuration based on current network conditions.

Command Changes

`vlr-failure`

This new command configures automatic VLR failure handling for the SGs service.

```
configure

context context_name

sgs-service name

vlr-failure duration minutes backoff-timer seconds detach-rate number [ -noconfirm ]

[ no ] vlr-failure [ -noconfirm ]

end
```

Notes:

Refer to the MME SGs Service Configuration Mode Commands chapter in the Command Line Interface Reference for more information about this command.

Performance Indicator Changes

`show sgs-service vlr-status full`

This command shows if the feature is enabled (Yes or No), as well as detach statistics relating to this feature.
CSCub06763 - Paging Load Control

Feature Changes

MME Message Rate Control

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.

Customer Impact: This feature provides controls to mitigate the undesirable effects of congestion due to excessive S1 Paging load or upon failure of an EGTPC path.

S1 Paging Rate Limit

In this release, the MME includes support for a new configuration to limit the rate of S1 paging requests sent per eNodeB per second. S1 Paging requests exceeding the configured rate threshold are dropped. All S1 Paging requests are treated uniformly without any special considerations for the type of paging request (CS/PS).

Pacing UE Deactivation

During an EGTPC (S11/S10/S3) path failure, the MME detects the failure and begins the process of deactivating all UE sessions affected. The MME now supports two separate configurable internal pacing queues for deactivating UEs: one for active UEs and a second for idle mode UEs. This enables the path failure processing and deactivation pacing rate to be different for each of these queues.

Upon detecting an EGTPC path failure, the impacted EGTPC tunnels are added to separate queues based on ECM-State and deactivations are scheduled based on the respective configured rates.

Command Changes

```
configure
    network-overload-protection mme-tx-msg-rate-control { egtp-pathfail ecm-idle rate ecm-connected rate | enb s1-paging rate }

    [ default ] network-overload-protection mme-tx-msg-rate-control

end
```

Notes:

- The `enb s1-paging` keyword configures an S1 paging rate limit applicable to all eNodeBs connected to all MME services. S1 Paging requests to an eNodeB will be rate limited at this threshold value. S1 Paging requests to an eNodeB exceeding this threshold will be dropped.
rate specifies the rate threshold in messages per second per eNodeB as an integer from 1 through 65535.

- The egtp-pathfail keyword configures the UE deactivation pacing rate for MME S11/S10/S3 interfaces (any EGTPC service with interface type “interface-mme”). Separate pacing rates must be defined for ECM Connected and ECM Idle UEs using the ecm-connected and ecm-idle keywords respectively.

rate specifies rate threshold in sessions per second per session manager (SessMgr) as an integer from 1 through 5000.

Note: Configuring a high deactivation rate can have a negative effect on performance. Appropriate dimensioning exercises should be performed to arrive at the optimum rate.

- The default keyword applies the default MME message rate control configuration; S1 paging rate limit is disabled and a path failure processing rate of 1000 per second per session manager without distinguishing between idle/active sessions.

Performance Indicator Changes

MME Schema

The following new bulk statistic has been added to the MME schema to track the total S1 paging requests dropped by all eNodeBs.

- s1ap-transdata-pagingdrop

show network-overload-protection mme configuration

This new command displays the network overload protection configuration, for example:

MME message rate control

S1 paging per eNodeB : 150 pages/second

EGTP path failure ECM-Idle : 10 sessions/second/smgr

EGTP path failure ECM-Connected : 20 sessions/second/smgr

show mme-service statistics

The show mme-service statistics command now includes a new output field to display the number of S1 Paging requests dropped for all MME services:

S1AP Statistics:

Transmitted S1AP Data:

... Downlink UE LPPaTpt: 0 Paging Dropped: 0

show session subsystem facility mmemgr instance

The show session subsystem facility mmemgr instance command now includes a new output field to display the number of S1 Paging requests dropped for the specified mmemgr instance:
S1AP Statistics:

Transmitted S1AP Data:

...  

S1AP Encode Failure: 0  
Paging Dropped: 0

show mme-service enodeb-association full

The show mme-service enodeb-association full command now includes new output field to display configured S1 paging rate limit:

S1 Paging Rate Limit: 150 per second

show session subsystem facility sessmgr instance

The show session subsystem facility sessmgr instance command now includes a new output field to display path failure pacing queue statistics for the specified session manager instance:

0 Current MME EGTP path failure queued for ecm-idle sessions  
0 Current MME EGTP path failure queued for ecm-connected sessions  
0 Maximum MME EGTP path failure queued for ecm-idle sessions  
0 Maximum MME EGTP path failure queued for ecm-connected sessions

CSCub29503 - MME: Sv Improvements - MSC selection using DNS

Feature Changes

MSC Selection using DNS

This feature requires that a valid SRVCC license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

As defined in 3GPP TS 29.303, the MME now supports the DNS-based method of using the Sv interface. In the NAPTR query response, the MME will analyze the “Service Parameter” of “x-3gpp-msc:x-sv”, and select a specific MSC from a pool list provided in the DNS response. The provisioned weights and priorities on the DNS server are used to load share proportionally between the MSC servers.

The DNS query FQDN will be based on RAC, LAC, MNC, MCC as follows:

rac<RAC>.lac<LAC>.rac.epc.mnc<MNC>. mcc<MCC>.3gppnetwork.org

MSC selection using DNS takes precedence over locally configured MSCs.

If DNS lookup fails, the MSC will be selected from local configuration.

Customer Impact: This feature provides flexibility to simplify SRVCC configuration.
Command Changes

DNS based MSC selection can be defined for an MME service, or for a Call Control Profile. Both configuration options specify the context in which a DNS client configuration has been defined.

**dns**

The `msc` keyword has been added to configure DNS selection of an MSC for a specific MME service:

```markdown
configure
c ontex t ctxt_name
   mme-service service_name
dns msc context ctxt_name
   [ no ] dns msc
   exit
```

Notes:
- Refer to the *Single Radio Voice Call Continuity* chapter in the *MME Administration Guide* for more information.

**dns-msc**

The `dns-msc` command has been added to configure DNS selection of an MSC based on a Call Control Profile. Configuration via Call Control Profile takes precedence in cases where DNS selection is also configured in the MME service (see above).

```markdown
configure
c all-control-profile profile_name
dns-msc context ctxt_name
   [ remove ] dns-msc
   exit
```

Notes:
- Refer to the *Single Radio Voice Call Continuity* chapter in the *MME Administration Guide* for more information.

Performance Indicator Changes

**show mme-service name <svc_name>**

This command displays the context ID configured for the specified MME service name. This context contains the DNS client configuration used for DNS-based MSC selection.

- DNS MSC Context : ingress

The same command also displays all MSC servers configured in the specified MME service.
show call-control-profile full name <profile_name>

This command displays the context ID configured for the specified call control profile name. This context contains the DNS client configuration used for DNS-based MSC selection.

DNS MSC Context : ingress

CSCub29525 - MME: Sv Improvements: MSC fallback on failure

Feature Changes

MSC Fallback on Failure

This feature requires that a valid SRVCC license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

To provide added SRVCC resiliency, the MME now supports fallback (resending the Sv PS to CS Request) to a different MSC in the following cases:

- No response is received (timeout) from the MSC to a Sv PS to CS Request.
- A failure response is received from the MSC to a Sv PS to CS Request.

If no alternate MSC is configured, or if the second MSC fails as well, the SRVCC handover fails. A new MSC is attempted only for the initial PS to CS Request. All MSC returned failure codes will trigger a fallback.

When an MSC is selected by DNS, and multiple results are returned, the second MSC result will be used for fallback. In case DNS selection returns just one MSC, the second MSC for fallback will be from local configuration if it exists. If DNS lookup fails, the MSC for fallback will be selected from local configuration.

This functionality is enabled by default. No additional configuration is required.

Customer Impact: This feature provides advanced failure handling mechanisms for increased robustness and resiliency.

CSCuc96756, CSCuh04626, CSCun73028 - MME: Extend paging-map for PS to include QCI

Feature Changes

Paging Map Enhancements

This feature requires that a valid Optimized Paging license key be installed to use this feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

The existing Intelligent Paging functionality of the MME has been enhanced in this release. The paging-map configuration now includes additional configuration options for selecting a paging-profile in order to control the pace, volume and behavior of a given paging state.
Within a paging map, precedence can now be defined for paging requests based on the following traffic types:

- **CS traffic (Mobile Terminated CSFB)** types can now be defined according to specific subtypes of **voice**, **sms**, and **other**.
- **PS traffic** (all data and control messaging that involve packet services as well as IMS Voice) types can now be defined according to the QoS **QCI value** from the EPS Bearer ID (EBI) in the Downlink Data Notification (DDN) received on S11 from the S-GW.
- **Signaling** (UE-level signaling requests) traffic types can now be defined. This option can be further qualified with the **Detach** and **LCS** (Location Services) traffic subtype options.

**Customer Impact:** This new functionality enables operator to fine-tune the paging preferences. This feature is particularly beneficial in VoLTE deployments.

### Command Changes

**precedence**

The following new keywords have been added:

- Use the new **voice**, **sms** and **other** keywords to define traffic sub-types for CS traffic type.
- Use the new **qci** keyword for PS traffic type to define QoS QCI values.
- Use the new **signaling** keyword to define a paging map for signaling traffic, as well as the new **lsc** and **detach** keywords to define signaling traffic sub-types.

```plaintext
cfg
lte-policy
  paging-map paging_map_number
    precedence precedence traffic-type { cs [ voice | sms | other ] | ps [ qci qci_value ] | signaling [ detach | lcs ] } paging-profile paging_profile_name
    [ no ] precedence precedence
  end
```

**Notes:**

- Refer to the *LTE Paging Map Configuration Commands* chapter of the Command Line Interface Reference for more information about this command.

### Performance Indicator Changes

#### MME Schema

The following new bulkstats have been introduced in this release to track paging based on the new options provided in this enhancement.

- **ps-qci-1-paging-init-events-attempted**
- **ps-qci-1-paging-init-events-success**
- ps-qci-1-paging-init-events-failures
- ps-qci-1-paging-last-enb-success
- ps-qci-1-paging-last-tai-success
- ps-qci-1-paging-tai-list-success
- ps-qci-2-paging-init-events-attempted
- ps-qci-2-paging-init-events-success
- ps-qci-2-paging-init-events-failures
- ps-qci-2-paging-last-enb-success
- ps-qci-2-paging-last-tai-success
- ps-qci-2-paging-tai-list-success
- ps-qci-3-paging-init-events-attempted
- ps-qci-3-paging-init-events-success
- ps-qci-3-paging-init-events-failures
- ps-qci-3-paging-last-enb-success
- ps-qci-3-paging-last-tai-success
- ps-qci-3-paging-tai-list-success
- ps-qci-4-paging-init-events-attempted
- ps-qci-4-paging-init-events-success
- ps-qci-4-paging-init-events-failures
- ps-qci-4-paging-last-enb-success
- ps-qci-4-paging-last-tai-success
- ps-qci-4-paging-tai-list-success
- ps-qci-5-paging-init-events-attempted
- ps-qci-5-paging-init-events-success
- ps-qci-5-paging-init-events-failures
- ps-qci-5-paging-last-enb-success
- ps-qci-5-paging-last-tai-success
- ps-qci-5-paging-tai-list-success
- ps-qci-6-paging-init-events-attempted
- ps-qci-6-paging-init-events-success
- ps-qci-6-paging-init-events-failures
- ps-qci-6-paging-last-enb-success
- ps-qci-6-paging-last-tai-success
- ps-qci-6-paging-tai-list-success
MME Changes in Release 16

MME Enhancements for 16.0

- ps-qci-7-paging-init-events-attempted
- ps-qci-7-paging-init-events-success
- ps-qci-7-paging-init-events-failures
- ps-qci-7-paging-last-enb-success
- ps-qci-7-paging-last-tai-success
- ps-qci-7-paging-tai-list-success
- ps-qci-8-paging-init-events-attempted
- ps-qci-8-paging-init-events-success
- ps-qci-8-paging-init-events-failures
- ps-qci-8-paging-last-enb-success
- ps-qci-8-paging-last-tai-success
- ps-qci-8-paging-tai-list-success
- ps-qci-9-paging-init-events-attempted
- ps-qci-9-paging-init-events-success
- ps-qci-9-paging-init-events-failures
- ps-qci-9-paging-last-enb-success
- ps-qci-9-paging-last-tai-success
- ps-qci-9-paging-tai-list-success
- cs-voice-paging-init-events-attempted
- cs-voice-paging-init-events-success
- cs-voice-paging-init-events-failures
- cs-voice-paging-last-enb-success
- cs-voice-paging-last-tai-success
- cs-voice-paging-tai-list-success
- cs-sms-paging-init-events-attempted
- cs-sms-paging-init-events-success
- cs-sms-paging-init-events-failures
- cs-sms-paging-last-enb-success
- cs-sms-paging-last-tai-success
- cs-sms-paging-tai-list-success
- cs-other-paging-init-events-attempted
- cs-other-paging-init-events-success
- cs-other-paging-init-events-failures
- cs-other-paging-last-enb-success
• cs-other-paging-last-tai-success
• cs-other-paging-tai-list-success
• signaling-detach-paging-init-events-attempted
• signaling-detach-paging-init-events-success
• signaling-detach-paging-init-events-failures
• signaling-detach-paging-last-enb-success
• signaling-detach-paging-last-tai-success
• signaling-detach-paging-tai-list-success
• signaling-lcs-paging-init-events-attempted
• signaling-lcs-paging-init-events-success
• signaling-lcs-paging-init-events-failures
• signaling-lcs-paging-last-enb-success
• signaling-lcs-paging-last-tai-success
• signaling-lcs-paging-tai-list-success

The following bulk statistics have been deprecated in this release and replaced by the bulk statistics above:
• ps-paging-init-events-attempted
• ps-paging-init-events-success
• ps-paging-init-events-failures
• ps-paging-last-enb-success
• ps-paging-last-tai-success
• ps-paging-tai-list-success

show mme-service statistics

The following groups of PS paging initiation event counters have been added in this release to track individual events for each QCI level (1-9). The following sample shows only the fields for QCI-1. Additional groups of fields are provided for QCI-2 through QCI-9.

Paging Initiation for PS QCI-1 Events:

Attempted: 0 Success: 0

Failures: 0

Success at Last n eNB: 0 Success at Last TAI: 0

Success at TAI List: 0

The following group of general PS paging initiation event counters have been deprecated in this release and replaced by the individual groups for each QCI level (QCI-1 – QCI-9) as described above.

Paging Initiation for PS Events:
The following groups of Signaling event counters have been added in this release to track individual Detach and LCS (Location Services) paging events.

Paging Initiation for SIGNALING DETACH Events:
Attempted: 0 Success: 0
Failures: 0
Success at Last n eNB: 0 Success at Last TAI: 0
Success at TAI List: 0

Paging Initiation for SIGNALING LCS Events:
Attempted: 0 Success: 0
Failures: 0
Success at Last n eNB: 0 Success at Last TAI: 0
Success at TAI List: 0

`show lte-policy paging-map name`

This command has been enhanced to display the new configuration options available, for example:

Paging Map : pml
Precedence 1 : Packet-Switched (PS) QCI: 1 2 3 4; Paging is performed as per paging-profile ppl
Precedence 2 : Circuit-Switched SMS (CS-SMS); Paging is performed as per paging-profile ppl
Precedence 3 : Signaling-LCS; Paging is performed as per paging-profile ppl

CSCug50843 - Improved UX for status commands

Feature Changes

Improvements to Output of Show Commands
The output of the following commands are now provided in a tabular format for easier comprehension using the optional `wf1` keyword.

- `show mme-service enodeb-association full`
- `show mme-service enodeb-association path-info`
- `show sgs-service vlr-status full`

A new `Assoc Uptime` field has also been added to the output of the following commands to display the Uptime of the association to the MME:

- `show mme-service enodeb-association full`
- `show sgs-service vlr-status full`

**Customer Impact:** This feature provides improved operational debugging and troubleshooting experience for the customer.

**Command Changes**

**Performance Indicator Changes**

**show mme-service enodeb-association full**

The following new field is included in the output of this command to display the uptime of the association between the MME and the eNodeB:

- `Assoc Uptime`

The format of Assoc UpTime is `0000d00h00m` (where `d`=day, `h`=hour, `m`=minutes) when `h` > =24 hrs, otherwise it will be displayed as `00h00m00s`.

**show sgs-service vlr-status full**

The following new field is included in the output of this command to display the uptime of the association between the MME and the VLR:

- `Assoc Uptime`

The format of Assoc UpTime is `0000d00h00m` (where `d`=day, `h`=hour, `m`=minutes) when `h` > =24 hrs, otherwise it will be displayed as `00h00m00s`.

**CSCuh31686 - Authentication vector management in MME and S4 SGSN**

**Feature Changes**

**Authentication Vector Management**
The MME provides a mechanism to define the number of authentication vectors (AVs) that can be requested from the HSS/HLR in an Authentication Info Request (AIR) message. New vectors are fetched when no more vectors are available.

**Previous Behavior:** Prior to Release 16, the maximum configurable number of authentication vectors to be retrieved from HSS/HLR was 3.

**New Behavior:** The new maximum configurable number of authentication vectors to be retrieved from the HSS/HLR is 5.

### Command Changes

**auth-request**

The value range for the `num-auth-vectors` keyword of this command has been extended from 3 to 5.

**configure**

```plaintext
context context_name
  hss-peer-service service_name
    auth-request num-auth-vectors num
    default auth-request num-auth-vectors
end
```

**Notes:**

- `num` must be an integer from 1 to 5.
- `default` returns the AV configuration to 1.

### CSCuh35890 - MME Optimization of S1 reset handling in MME

#### Feature Changes

##### Optimization of S1 Partial Reset Handling

**Previous Behavior:** When the MME received a Partial Reset message from the eNodeB which contained more than one UE Id, the MME Manager process would initiate a vector call with the Partial Reset message to all Session Manager processes. If the message had only 1 UE Id, the message was sent to only the Session Manager that handled that UE.

**New Behavior:** The MME Manager now sends the Partial Reset message to only those Session Managers which are handling those specific UEs mentioned in the Reset. Reset messages containing multiple UEs are now bundled together in a single message to the appropriate Session Manager.

**Customer Impact:** Prevents the over-utilization of the messenger path when large numbers of Partial Requests are received from the eNodeBs.
Performance Indicator Changes

show session subsystem facility mmemgr instance

This command now includes a counter to show the number of Partial Reset messages received by each Session Manager:

- S1AP Partial Reset to Sessmgr(Non-Vector)

CSCuh38256 - LCS : LR Answer Dropped stat not pegged

Performance Indicator Changes

LCS Schema

The following bulk statistic has been removed from the LCS schema.

- msg-lr-ans-drop

show location-service statistics all

The following statistic has been removed from the output of the `show location-service statistics all` command.

- LR Answer Dropped

CSCuh47311 - Need CLI visibility into id database in S1AP stack

Command Changes

show mme-service id summary

The `show mme-service id summary` command now includes the following additional keywords: `peer-id`, `sessmgr` and `service-name`. These optional keywords enable the operator to filter the information reported by this command.

`show mme-service id summary [ service-name name [ sessmgr instance ] ] [ peer-id id [ sessmgr instance ] ] [ [ grep grep_options | more ] ]`

Notes:

- `service-name name`: Filters the output of the command by for an existing MME service name specified as an alphanumeric string of 1 through 63 characters.
- `peer-id id`: Filters the output of the command by a MME peer identifier specified as an integer from 1 through 4294967295.
- `sessmgr instance`: Filters the output of the command by the specified session manager instance as an integer from 1 through 4294967295.
Performance Indicator Changes

show mme-service session full all

The `show mme-service session full all` command now displays the UE eNodeB associations for the UE, including the MME UE S1AP Id and the eNodeB UE S1AP Id, as well as the total count of S1AP IDs present in the stack.

If the information from stack is different than that stored in MME, it is indicative of an issue with UE-state at the MME. The new fields are highlighted in the sample output below:

Active ENodeB information:

- **Global ENodeB ID**: 123:123:456
- **S1AP End Point**: 192.60.60.4
- **Crypto-map Name**: n/a

**MME UE S1AP ID**: 1048577  **ENodeB UE S1AP ID**: 12346

**MME UE S1AP ID (stack)**: 1049075  **ENodeB UE S1AP ID (stack)**: 353

**MME UE S1AP ID (stack)**: 1049076  **ENodeB UE S1AP ID (stack)**: 354

**MME UE S1AP ID (stack)**: 1049077  **ENodeB UE S1AP ID (stack)**: 355

Total S1AP ID (stack): 5

CSCuj16369 - MME is not sending S1-Setup response when 33 PLMNs are configured

Feature Changes

S1-Setup Response Behavior Change

**Previous Behavior**: All the configured PLMs under the mme-service from the `plmn-id`, `network-sharing` and `inter-rat-nnsf` commands were considered while forming the `gummei_ie` for sending an "S1-Setup Response".

**New Behavior**: A maximum of 32 PLMs can be sent in an "S1-Setup Response", even if the operator configured more than 32 PLMs using all the 3 CLIs.

The MME now populates the serving PLMs from the `plmn-id` command, then PLMs from `network-sharing` command, and finally the PLMs from `inter-rat-nnsf` command until the 32 PLM limit is reached.

Once the limit is reached, even if there are more PLMs to be fetched from "inter-rat-nnsf", these entries will be ignored.

**Customer Impact**: Any PLMN entries beyond the 32 PLMN limit are ignored.
CSCuj42591 - Setting ‘IMS voice over PS session indicator’ per TAI list

Feature Changes

IMS Voice over PS Indicator Support Per Tracking Area Identity List

The MME now supports configuration of the ‘IMS voice over PS Session Supported’ indication per TAI List. The MME reflects the ‘IMS Voice over PS session’ support indicator in the S6a Insert-Subscriber-Data Answer message.

Command Changes

ims-voice-over-ps

This command enables support for IMS Voice over PS Session for the specified TAI management object.

configure

lte-policy

tai-mgmt-db db_name

tai-mgmt-obj obj_name

[ no ] ims-voice-over-ps

end

Notes:

- The MME also supports a global ‘IMS Voice over PS session’ support indicator (configured under Call Control Profile) that indicates whether all (or none) of the TACs support ‘IMS Voice over PS session’. The global indicators have priority over the per-TAI list configuration. In case of mismatch between the global and per-TAI list based configuration, the global indicator will be honored.

Performance Indicator Changes

show lte-policy tai-mgmt-db name

The following field is now displayed when the TAI Management Object has been configured to support IMS Voice over PS Session.

- ims-voice-over-ps
CSCuj42608, CSCuj63683 - Setting ‘Homogenous Support of IMS Voice over PS Sessions’ indication in Update Location Request message

Feature Changes

Support for ‘Homogenous Support of IMS Voice over PS Sessions’ AVP

**Previous Behavior:** The MME supports the ‘IMS Voice Over PS Sessions’ indicator on a global basis. This is set as a global configuration under the Call Control Profile as part of the `network-feature-support-ie` command. This indicator allows the MME to indicate that ‘IMS Voice Over PS’ is supported in all TAs. However, there was no setting to indicate that IMS Voice Over PS was not supported in any TA.

**New Behavior:** The MME now can be configured to include the “Homogenous Support of IMS Voice over PS Sessions” AVP in the S6a Update-Location-Request messages to the HSS. This AVP will be sent with the value set to “Not Supported” or “Supported” based on the configuration. If not configured, the AVP will not be sent.

**Customer Impact:** This provides operators implementing VoLTE services the configurable capability to include these indications in ULR message towards the HSS.

Command Changes

```
network-feature-support-ie

configure

    call-control-profile profile_name

    network-feature-support-ie ims-voice-over-ps { not-supported | supported }

    [ remove ] network-feature-support-ie

end
```

**Notes:**

- **not-supported:** Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to “Not Supported”. This indicates that IMS Voice over PS is not supported in any Tracking Areas.

- **supported:** Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to “Supported”. This indicates that IMS Voice over PS is supported in all Tracking Areas.

- If the command is entered without either the **supported** or **not-supported** keywords, the AVP will not be sent.
CSCuj42615 - Purge requirement for PS -> CS handoff after SGSN Context Transfer

Feature Changes

HSS Purge After SRVCC Handoff

The MME now supports a configuration capability to perform the Purge UE procedure to the HSS for UEs which support Dual Transfer Mode (DTM). This feature is configurable via the CLI and is disabled by default. If configured, the MME initiates an HSS Purge after the following two SRVCC Handoff (HO) scenarios:

For SRVCC Handoff with PS Handoff support, the Purge S6a message is sent immediately after successful completion of the Handoff. For this scenario, the configurable purge timer is not used.

For SRVCC Handoff without PS Handoff support, a configurable timer is initiated and the Purge S6a message is sent if a SGSN Context Request is received prior to timer expiry. If a Context Failure occurs, no HSS Purge S6a message is sent.

Customer Impact: This feature ensures the HSS has a reliable UE status on whether it is currently operating on the LTE network.

Command Changes

policy srvcc purge-timer

This new command configures the MME to initiate an HSS Purge after the SRVCC HO where the UE supports DTM. It also allows configuration of a purge timeout value in seconds.

configure

context ctxt_name

mme-service srvc_name

policy srvcc purge-timer seconds

[ no ] policy srvcc purge-timer

[ default ] policy srvcc

end

Notes:

- **purge-timer seconds**: defines how long in seconds the Purge Timer will run. This is applicable only for SRVCC Handoff without PS Handoff support scenarios.
- For example, if **purge-timer** is set to 20 seconds:
  - If the Context Transfer happens 10 seconds after SRVCC HO, the MME initiates an HSS Purge.
  - If the Context Transfer happens 30 seconds after SRVCC HO, the MME will NOT initiate an HSS Purge because the Purge Timer has expired.
- **seconds**: must be entered as an integer from 1 through 24000.
• Both the default and no keyword options disable this feature.

CSCul54893 - Support on MME for Tracing s13 interface

Feature Changes

S13 Interface Session Tracing

The MME now supports tracing of the S13 interface. This tracing is done locally in the MME and can be enabled via the CLI. If S13 tracing is enabled, this activation information is sent in the following three S10 messages during inter-RAT handover: Forward Relocation Request, Context Response, Identification Response.

Command Changes

```
session trace subscriber network-element mme interface
```

S13 interface tracing in the MME can be enabled by using the following command. The s13 keyword has been added to support this function.

```
session trace subscriber network-element mme interface { all | s1mme | s3 | s6a | s10 | s11 | s13 }
```

Performance Indicator Changes

```
show session trace subscriber network-element mme trace-ref
```

This command now includes an S13 field when an S13 interface trace is active. The S13 field is highlighted in the following sample output:

```
Traced Interfaces:
   S1mme
   S3
   S6a
   S10
   S11
   S13
```
CSCul61714 - Support for statistics to distinguish between CLI or HSS initiated Trace

Performance Indicator Changes

show session trace subscriber subscriber network-element mme trace-ref

The following field has been introduced to the output of this command to indicate the source of the session trace, either HSS-initiated (Signaling) or CLI-initiated (Management).

- MME: Trace Type: Management or Signaling

CSCun28592 - S6a Feature List AVP is hardcoded in MME

Feature Changes

Feature-List AVP Value in Messages Sent to HSS

**Previous Behavior:** The MME always sent the Feature-List AVP value as 67110415 (0x400060F) as specified in TS 29.272 (prior to Version 10).

**New Behavior:** To comply with TS 29.272 Version 10 which changed the position of the T-ADS bit, the value sent in the Feature-List AVP is now configurable using the existing `diameter update-dictionary-avps` command in the HSS Peer Service Configuration Mode.

If this command is configured using the `3gpp-r9` keyword, 0x400060f is sent. If this command is configured using the `3gpp-r10` keyword, 0x800060f is sent.

CSCzn16621, CSCzn16622 - MME needs to support non-3gpp-to-LTE handover

Feature Changes

Unoptimized Non-3GPP Handover Support

This feature provides MME support for Non-3GPP to EUTRAN and EUTRAN to Non-3GPP un-optimized handovers. These include the LTE-eHRPD handover scenarios in sections 8.2.1.1 and 8.2.1.2, and 8.2.2 and 8.2.3 of 3GPP TS 23.402-910.

No configuration is required to enable this functionality on the MME.

Note:

- PDN Connectivity request should contain Request Type as HANDOVER.
- P-GW is selected only through HSS-provided P-GW address or FQDN (MIP6-Info), with P-GW allocation type as static always.
- In the case of multiple PDN connectivity during handover from non-3gpp access to EUTRAN, the ESM PDN connectivity message from UE is transported via S1AP Uplink NAS transport. All other such PDN connectivity requests shall be rejected.
- Handovers to other access (such as UTRAN, GERAN) are only supported after the S11 modify bearer procedures with S-GW have been completed for all PDNs.

**Performance Indicator Changes**

**MME Schema**

The following new MME schema bulk statistics have been added to track the number of outbound and inbound non-3GPP handovers that were attempted, were successful, and which failed.

Note: During an inbound relocation, both the handover statistics and relevant attach/PDN connectivity statistics will be incremented.

- out-non-3GPP-ho-attempted
- out-non-3GPP-ho-success
- out-non-3GPP-ho-failures
- in-non-3GPP-ho-attempted
- in-non-3GPP-ho-success
- in-non-3GPP-ho-failures

**System Schema**

The system disconnect reason `disc-reason-484` has been repurposed in this release as `mme-reloc-to-non-3GPP` and now tracks the total number of session disconnects resulting from outbound handovers.

**show mme-service statistics**

The output of the `show mme-service statistics` command now displays the number of outbound and inbound non-3GPP handovers that were attempted, were successful, and which failed. Note that these counters increment on a per-PDN basis, where all other handover counters increment on a per-UE basis.

EUTRAN<-> non-3GPP Unoptimized Handovers:

Outbound relocation (Per PDN):

- Attempted: 0
- Success: 0
- Failures: 0

Inbound relocation (Per PDN):

- Attempted: 0
- Success: 0
- Failures: 0
CSCzn59071 - Improve logging and debug stats in MMEMGR

Performance Indicator Changes

show session subsystem facility mmemgr

The show session subsystem facility mmemgr command now displays the following additional counters.

- Service Start Request
- Service Modify Request
- Service Stop Request
- Paging Messages Sent
- Temporary EnodeB entries (For Trap Generation)
- PLMN Validation Failure
- EnodeB Id Validation Failure
- usap (SCTP Endpoints) Allocated
- Current Number of SCTP Flows
Chapter 14
MVG Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from MVG in StarOS 16 software releases.
**MVG Enhancements for 16.0**

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.

---

**CSCug89455 - Video detection using HTTP payload contents**

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

**Feature Changes**

**Video Detection using HTTP Payload**

Readdressing to CAE is done only for HTTP video traffic. Non-video traffic will be sent to the origin server (until flow is readdressed to CAE for the first video request). The mechanism for detection of HTTP video traffic is based on inspection of HTTP payload for video signatures. Only Response payloads will be inspected and not request payloads. MVG supports video types such as FLV, ISOM (mp4, 3gp, 3g2, qt, f4v, m4v, etc.), moov, wmv, MPEG2_TS, AVI, and so on.

**Limitations:**

- This mechanism may have some performance impact.
- Only the first packet of the response video header will be inspected. If video header is not complete in the first packet of the payload due to TCP fragmentation, then video detection may not happen by this mechanism.
- Chunk encoded video responses, and compressed/encoded videos may not be detected by this mechanism.

**Command Changes**

**http reply payload**

This new command allows you to define rule expressions to enable video detection using HTTP payload content.

```
configure

active-charging service  <acs_name>

ruledef  <ruledef_name>

[ no ] http reply payload type = video

end
```

CSCug89478 - Adding support for content-range HTTP header

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

Feature Changes

Support for Content-Range HTTP Header

The ECS HTTP Analyzer now supports parsing for content-range HTTP headers in addition to several HTTP headers. This header is useful in detecting HTTP video requests when using ECS-DPI ruledefs based on HTTP headers/URI. A new CLI command is added in the ACS Ruledef Configuration mode to define rule expressions for CAE re-addressing.

Command Changes

http content range

This new command allows you to define rule expressions for CAE re-addressing to verify if the HTTP Response has content-range header or not.

configure

    active-charging service acs_name

    ruledef ruledef_name

    [ no ] http content range = TRUE

    end
Chapter 15
NAT Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from NAT in StarOS 16 software releases.
NAT Enhancements for 16.0

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.

CSCud50942 - Need stats for packets that were bypass nated

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

**Feature Changes**

**Statistics Support for Bypass NAT**

With this release, the *show active charging subsystem all* will display statistics for NATed and Bypass NATed packets.

**Previous Behavior:** The *show active charging firewall statistics* command displayed only the number of flows that were NATed or Bypass NATed.

**New Behavior:** In this release, the number of NATed and Bypass NATed packets can be tracked as part of the *show active charging subsystem all* CLI command. This information is also available at instance level.

**Customer Impact:** The user can view additional NAT statistics for *show active charging subsystem all* CLI command.

**Performance Indicator Changes**

*show active-charging subsystem all*

The following fields are added to the output of this command to display statistics for packets that are bypass NATed.

NAT Packet Statistics:

- Total NAT Bypass packets
- Total NAT44 Bypass packets
- Total NAT64 Bypass packets
- Total NAT packets
- Total NAT44 packets
- Total NAT64 packets
CSCuh25763 - NAT Realm per FW/NAT policy

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

Feature Changes

Support for NAT Realm per FW/NAT Policy

In this release, the number of NAT realms that can be configured in Firewall-and-NAT policy is 20 and a maximum of 3 NAT realms per call/subscriber can be configured.

When NAT realms configured per Firewall-and-NAT policy exceeds more than 20, an error message will be displayed. In case of on-demand NAT, once 3 NAT IPs are allocated to subscribers and traffic sent to the fourth NAT realm, then packets will be dropped.

Previous Behavior: In previous releases, the maximum number of NAT realms per Firewall-and-NAT policy was limited to 3. The same Firewall-and-NAT policy was used for most NAT users and source-IP based rules were used to select NAT realm for subscribers. Although only three NAT realms were used per subscriber, the same Firewall-and-NAT policy will not allow more than three NAT realms to be configured. This caused issues like duplicating of Firewall-and-NAT policy/rulebase and sending rulebase from AAA.

New Behavior: The maximum number of NAT realms per Firewall-and-NAT policy and per subscriber need to be independent of each other. This feature allows 20 NAT realms to be configured in Firewall-and-NAT policy and limits NAT-IP per subscriber to 3 in data path.

CSCuh97978 - [ICSR-Volte] Removing the usage of pacing queue for critical MCs

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

Feature Changes

ICSR Enhancements for VoLTE

A significant number of internal enhancements have been made in support of voice-grade redundancy for Voice over LTE (VoLTE) deployments. ICSR components have been optimized to ensure that failure recovery is accomplished within acceptable limits for VoLTE.

For more details, see the System Enhancements for March 14, 2014 chapter in this Release Notes.

CSCul83326, CSCzm98044 - CLI to filter the subscribers based on on-demand NAT IP usage time

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

Feature Changes

Support for On-Demand NAT Realms
For On-demand NAT realms, support is added to filter NAT required subscribers based on the NAT IP usage time in this release.

**Previous Behavior:** A filter to provide information about how long a subscriber is using NAT IP or port chunks is not present.

**New Behavior:** The `usage-time` option is added to `show subscribers nat required` CLI command to filter subscriber information based on how long a subscriber is using the assigned NAT IP or port chunk.

**Command Changes**

`show subscribers`

A new keyword option `usage-time` is added to the `show subscribers` command to find out how long (in seconds) the subscriber has been using the assigned NAT-IP or port chunk.

```
show subscribers nat required usage-time [ < | > | greater-than | less-than ] value
```

The options are described below:

- `<`: Filters output so that only information less than the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `greater-than`: Filters output so that only information greater than the specified value is displayed.
- `less-than`: Filters output so that only information less than the specified value is displayed.
- `value`: If no other filtering options are specified, only output matching value is displayed. If value is not specified, all data is cleared. `value` must be an integer from 0 through 4294967295.
Chapter 16
PDSN Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from the PDSN in StarOS 16 software releases.
PDSN Enhancements for 16.1

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 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 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

CSCtu38298 - AMBR/MBR/QCI parameter support in PDSN/PCEF

Feature Changes

**AMBR/MBR/QCI Parameter Support Added in PDSN/PCEF**

Support has been added for the PCEF functionality on the PDSN to do the session level bandwidth control according to the QoS information provided by the PCRF on the Gx interface. AMBR received in CCA-I, CCA-U, and RAR from PCRF is updated and traffic policing is done based on the latest values. AMBR is different for uplink and downlink direction. This feature is CLI controlled and works only when APN-AMBR is received from PCRF and only if CLI is configured for that particular direction.

**Important:** This is a customer specific feature.
**Command Changes**

`qos apn-ambr rate-limit`

A new command `qos apn-ambr rate-limit` has been implemented to configure the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface.

```
configure
  context context_name
  subscriber subscriber_name
    [ default | no ] qos apn-ambr rate-limit direction { uplink | downlink } burst-size value violate-action { drop | transmit | lower-ip-precedence }
  end
```

**CSCuh03636 - Need PDSN to support combined ipv4/v6 accounting for dual stack session**

**Feature Changes**

**Support for Combined IPv4/IPv6 Accounting for Dual Stack Session**

In order to migrate the IPv4 network to IPv6 network, ASR5000 and ASR5500 supports PMIPv6 for PDSN/MAG. ASR5000 and ASR5500 also supports separate radius accounting for PDSN IPv4/IPv6. Support has been added for PDSN/MAG to generate combined IPv4/IPv6 radius accounting message for an IPv4/IPv6 dual stack session.

*Important:* This is a customer specific feature.

**Command Changes**

`pdsn-dual-stack combined-radius-accounting`

A new command `pdsn-dual-stack combined-radius-accounting` has been added in subscriber profile for enabling/disabling combined radius accounting for PDSN dual stack session.

```
configure
  context context_name
    [default] pdsn-dual-stack combined-radius-accounting
  end
```

Notes: `combined-radius-accounting` is disabled by default. That is, by default, separate radius accounting would be supported for each ip session.
PDSN Enhancements for 16.0

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

---

**CSCum82051** - Call not up when 802.P is set to odd value in l2-mapping-table

**Feature Changes**

**Change in Help Text for CLI**

The help text for the CLI command “qos l2-mapping name <l2-mapping name> internal-priority cos 0x<0..f> color 0x<0..3> 802.1p-value 0x<0..f>” has been changed as follows:

**Previous Behavior:** Earlier, the help text read as: "map to a 802.1p value. This also includes both p-bits and DEI/CFI. DEI is the lsb bit."

**New Behavior:** The new help text now reads as: "map to a 802.1p value. This also includes both p-bits and DEI/CFI. DEI is the lsb bit. Caution: Setting an odd value(DEI/CFI to 1) makes some switches to drop packets."
CSCun65435 - Assertion at sessmgr_imsa.c:453 Function: sessmgr_authorize_with_imsa()

Feature Changes

IMSA Session for Mobile-IP Call on PDSN and HA

- **Previous Behavior:** Earlier, an IMSA session was being created for mobile-ip call on PDSN and HA together.
- **New Behavior:** For mobile-ip call, the IMSA session is present only on HA, while the earlier IMSA session created by PDSN is terminated. This behaviour is only for IMSA session, while it is consistent for ACS session.

CSCzn10122 - After configuring no max-login failures local user is not granted acces

Feature Changes

No Max-Login Failure Command Behavior Changes

- **Previous Behavior:** The command “no local-user max-failed-logins” sets the max login failures to one (functionally). But the user assumed that the command disabled the feature of checking the max login failures. Instead, the command to disable the max login failures check is “local-user username <username> no-lockout-login-failures password <password>” which disables locking for the specific local-user account on login failures.

- **New Behavior:** The command “no local-user max-failed-logins” now causes the system to not check for max login failures and disables the lock-out feature for all local-users.

- **Customer Impact:** Existing customer who are currently using this feature expecting the old functionality will no longer see the old behavior as described above.

Command Changes

no local-user max-failed-logins

- The CLI “no local-user max-failed-logins” does not check for max login failures. It also disables the lock-out feature for all local-users.
Chapter 17
PSF Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from PSF in StarOS 16 software releases.
PSF Enhancements for 16.0

This section identifies all of the Firewall 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.

CSCtl88372 - SFW: feature parity of the PSFW between uplink and downlink

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

**Feature Changes**

**Firewall Uplink Protection**

The Firewall Uplink protection feature provides security to ISP servers from mobile space devices. In addition to protecting mobiles from Internet vulnerabilities, it is imperative to protect ISP servers from the mobile space originated traffic. Feature Parity of Firewall is aimed at porting all Downlink protection features to support Uplink servers as well. No separate license is required to enable this feature.

The following features will be ported to support Uplink protection.

- IP Options check
- Jolt attack detection
- Teardrop attack detection
- Winnuke attack detection
- Ping of Death attack detection
- TCP Sequence number and ACK Number checks
- MIME Flood attack detection
- TCP RST message threshold
- UDP - ICMP Destination Unreachable message threshold
- ICMP - ICMP Destination Unreachable message threshold

For uplink protection, no additional statistics are added. All the existing statistics will be pegged properly with uplink protection enabled. Uplink Flooding detection, Uplink Port-scan detection and Uplink IP-sweep protection will be enabled separately in Global ACS Service Configuration mode.

**Command Changes**

`firewall protect-servers`
This command is configured to protect ISP servers from mobile space devices.

```
configure

active-charging service acs_name

firewall protect-servers { all | host-pool } policy policy_name

{ default | no } firewall protect-servers

end
```

Notes:
- Uplink protection can be enabled or disabled based on the server IP of the packet.

**Performance Indicator Changes**

```
show active-charging firewall dos-protection
```

This command is new and can be configured to display statistics of the IP Sweep server list involved in IP Sweep attacks.

```
show active-charging firewall dos-protection ip-sweep server-list { all | instance instance_num } [ | { grep grep_options | more } ]
```

**CSCub35955 - ICSR Support for Dynamic Firewall Access Rules**

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

**Feature Changes**

**ICSR Support for Dynamic Firewall Access Rules**

In this release, ICSR recovery is supported for dynamic Firewall access rules. Firewall access rules can be enabled either statically or dynamically. Firewall access rules can be dynamically activated or deactivated from the Gx server. This feature currently works only for default bearers and not for dedicated bearers.

The following attributes are used to activate or deactivate Firewall access rules from the Gx server:

- Charging-Rule-Install
- Charging-Rule-Remove

**Previous Behavior:** Firewall access rules enabled dynamically by PCRF were checkpointed only for standalone recovery. ICSR checkpointing was not done for dynamically enabled access rules. After ICSR switchover, the dynamically enabled Firewall rule will be disabled.

**New Behavior:** In this release, after ICSR switchover, the Firewall access rules will be enabled dynamically from the Gx server.
CSCud50947 - Stats needed for traffic allowed thru default sfw rules/pin-holes

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

Feature Changes

Statistics support for traffic through default SFW rules/pin-holes

Firewall-and-NAT policy can allow or deny traffic based on default firewall rules or pin-holes. In this release, statistics for traffic allowed/dropped through default SFW rules and pin-holes/dynamic routes are added.

Previous Behavior: The output of the `show active charging ruledef statistics` command displayed statistics only for access ruledefs configured in the Firewall-and-NAT policy. These statistics are stored globally per instance.

New Behavior: The output of the `show active charging ruledef statistics` command now displays information for traffic allowed/dropped due to default firewall rules and pin-holes/dynamic routes. These statistics are stored at service level.

Performance Indicator Changes

show active-charging ruledef statistics

The following fields have been added to the output of this command to display packets statistics allowed through default SFW rules/pin-holes.

- Total Default Firewall Ruledefs
- Uplink Packets
- Uplink Bytes
- Downlink Packets
- Downlink Bytes
- Uplink Packets Dropped
- Uplink Bytes Dropped
- Downlink Packets Dropped
- Downlink Bytes Dropped
- Hits

show active-charging ruledef statistics all firewall wide

The following fields have been added to the output of this command to display packets statistics allowed through default SFW rules/pin-holes.

- SFW Default Ruledefs:
  - ALG Pinholes
  - Default Uplink
  - Default Downlink
PSF Changes in Release 16

PSF Enhancements for 16.0

- Total Ruledef(s)
- Total Default SFW Ruledef(s)

CSCue70886 - src-ip based flood attack detection

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

Feature Changes

Source-IP based Flood Attack Detection

The Source-IP based flood attack detection feature is implemented to limit the number of new flows originating from a source IP per unit time to various destinations in both uplink and downlink directions. Limiting the number of connections from a single source IP to different destinations will be applied only per SMGR instance.

CLI support is added for enabling and disabling uplink/downlink IP Sweep protection. Statistics support is added to show details of packets dropped due to IP Sweep protection and the list of internet hosts doing a flood attack.

Command Changes

firewall dos-protection ip-sweep

The ip-sweep keyword is new and is configured to detect Source IP-based flooding for uplink direction.

configure

    active-charging service acs_name

    firewall dos-protection ip-sweep { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name } packet limit packet_limit | downlink-server-limit server_limit | inactivity-timeout timeout | sample-interval interval }

    default firewall dos-protection ip-sweep { downlink-server-limit | icmp | inactivity-timeout | sample-interval | tcp-syn | udp }

    no firewall dos-protection ip-sweep { icmp | tcp-syn | udp }

end

Notes:

- This command is used to enable or disable IP Sweep Protection in the uplink direction for mobile subscribers and internet hosts on a per protocol basis.
- IP Sweep attacks detected in the downlink direction can be configured using the firewall dos-protection ip-sweep command in the FW-and-NAT Policy Configuration mode.
- The configuration values of packet limit and sampling interval are common for both uplink and downlink.

firewall dos-protection

The ip-sweep keyword is new and is configured to detect Source IP-based flooding for downlink direction.
configure

active-charging service acs_name

fw-and-nat policy policy_name

[ no ] firewall dos-protection ip-sweep { icmp | tcp-syn | udp } default firewall dos-protection
end

Notes:
- IP Sweep attacks detected in the uplink direction can be configured using the `firewall dos-protection ip-sweep` command in the ACS Configuration mode.
- The configuration values of packet limit and sampling interval are common for both uplink and downlink.

Performance Indicator Changes

**show active-charging firewall dos-protection**

This command is new and can be configured to display statistics of the IP Sweep server list involved in IP Sweep attacks.

`show active-charging firewall dos-protection ip-sweep server-list { all | instance instance_num } [ | { grep grep_options | more } ]`

**show active-charging firewall statistics verbose**

The following fields have been added to the output of this command to display the number of packets dropped on ICMP/TCP-SYN/UDP attacks in uplink and downlink.

- TCP Stats:
  - Packets Dropped on TCP-SYN IP-Sweep Attack (DL/UL)
- UDP Stats:
  - Packets Dropped on UDP IP-Sweep Attack (DL/UL)
- ICMP Stats:
  - Packets Dropped on ICMP IP-Sweep Attack (DL/UL)

**show active-charging fw-and-nat policy name**

The following fields have been added to the output of this command to display the status of protection for ICMP/TCP-SYN/UDP IP sweep attacks.

- Dos-Protection:
  - UDP IP Sweep
  - ICMP IP Sweep
  - TCP-SYN IP Sweep
CSCue95313 - ASR5k port-scan request timeout should range from 1 to 30 secs

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

Feature Changes

Port scan Request Timeout

The range for the response-timeout CLI command has been changed to provide the least configurable TCP/UDP request timeout to be 1 second. Port scan detection can now happen in less time, and ensures detection at less number of SYN packets.

Previous Behavior: The firewall port-scan protocol { tcp | udp } response-timeout CLI command allowed for a range of 3 to 30 seconds.

New Behavior: The firewall port-scan protocol { tcp | udp } response-timeout CLI command allows for a range of 1 to 30 seconds.

Customer Impact: The customer will be able to configure TCP/UDP response timeout as low as 1 second.
Chapter 18
P-GW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from P-GW in StarOS 16 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 16.1
  - “CSCuh74228 - Unwanted UBRreq/UBResp for apn-ambr/QCI modification” - Enhanced description
P-GW Enhancements for 16.4

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

---

**CSCup32052, CSCup08125 - Congestion is cleared on performing unplanned demux DPC migration**

### Feature Changes

**Congestion State Sent to Session Controller**

**Previous Behavior:** Congestion state was sent from resource manager to session controller only when there was change in congestion state

**New Behavior:** Congestion state is now sent periodically to the session controller.

The following congestion types are recovered after egtpinmgr kill.

1. license-utilization
2. system-cpu-utilization
3. system-memory-utilization
4. port-rx-utilization
5. port-tx-utilization

**Important:** If sessctrl and egtpinmgr is killed back to back then only congestion type is not recovered.

**CSCur72239 - Access point MAC address not displayed in show command**

**Feature Changes**

**Access Point MAC Address was not Displayed in Show Command**

**Previous Behavior:** The `show subs saegw-only full all` CLI command output did not have “Access Point MAC Address” information in cases when wifi calls on S2B landed on P-GW which was part of SAEGW service.

**New Behavior:** The `show subs saegw-only full all` CLI command output will have “Access Point MAC Address” information in cases when wifi calls on S2B land on P-GW which is part of SAEGW service.
P-GW Enhancements for 16.3

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

---

CSCuq88332 - Need EDR records from different rulebases to goto single EDR file

**Feature Changes**

**EDR Records from Different Rulebases in Single EDR File**

High EDR file generation rate. System is going into file deletion mode and filling up HDD. Request is to put the EDR records for all different rulebases of a specific EDR format into a single EDR file instead of generating EDR files for each rulebase.

**Previous Behavior:**

- EDR are generated for matching rule-base and edr-format.
- By default, EDRs generated for different rule-bases and format will be stored in different file.
- Currently, the “File” command that controls the file naming can be modified to include/exclude the rulebase and format name in the filename.
- By including the rulename and format name, customer can know what EDRs are present in each file just by looking at the filename.
- If either rulebase or format name was not added to the filename, then customer has to open the file to determine type of information stored in each file.

**New Behavior:** Customers have started increasing the number of rulebases exponentially. As a result, CDRMOD has to open too many files and this results in inefficient file operation. The system ends up having too many small files, which leads to file transfer delay.

The solution is to bundle records with similar fields (header) into a single file so that there are a few larger files rather than too many small files. This fix helps with this solution.

**Customer Impact:** There should not be any impact on customer backend record processing due to this change.
- If currently configured to include “rulebase” and “format,” then behavior is the same.
- If excluding “rulebase” and/or “format” currently, then backend record processing tool should know how to process the records in each file without looking into the filename.

Going forward, customers will have the option to bundle different SIMILAR records into single file and thereby can increase the number of rule-base.

**CSCur26723 - MAPCON with Wifi and 3G**

**Feature Changes**

**WiFi and 3G Can Co-exist with Matching EBI and NSAPI Values**

This is relevant only for a GnGp setup where associated GGSN and P-GW services exist and WiFi PDN attachments are expected on P-GW. A WiFi PDN connection for Subscriber can now co-exist with a Gn GGSN (3G) PDN connection for the same EBI and NSAPI value.

**Previous Behavior:** When a new Gn GGSN (2G/3G) call comes in, the existing WiFi PDN connection using matching EBI with the NSAPI of existing PDN would get dropped.

Similarly, when a new ePDG (WiFi) call comes in, the old Gn GGSN call (3G) would get dropped when EBI of WiFi PDN request matches with the NSAPI of new PDP Context request from Gn GGSN.

**New Behavior:** An ePDG PDN (WiFi) can now co-exist with a Gn GGSN (3G) PDN with matching EBI and NSAPI.

**Customer Impact:** It is expected that in the above condition, peers will also continue to maintain session and both PDN connections would be valid unless one of the PDN can be considered as stale PDN on GW; the stale PDN would eventually get cleared with idle timer functionality if there is no traffic flowing through it.
P-GW Enhancements for 16.2

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

---

**CSCuo06912 - PGW call fails if Framed-Pool enforced from radius**

**Feature Changes**

**P-GW Call Fails if Framed-Pool Enforced from Radius**

**Previous Behavior:** If radius returns ip pool for ip address allocation method as no-dynamic for P-GW, then the ip address allocation will be successful.

**New Behavior:** If radius returns ip pool for ip address allocation method as no-dynamic for P-GW, then ip address allocation will be successful.
CSCuo95038 - TMOPL: PGW forces lower AMBR values than received

Feature Changes

**P-GW forces lower AMBR values than received**

**Previous Behavior:** In absence of PCRF, the APN AMBR that was received in the MOB BEARER REQUEST during GnGp HO was not applied.

**New Behavior:** In absence of PCRF, the APN AMBR received in MOB BEARER REQUEST during GnGp HO will now be applied.

CSCup44058 - Acct msg shows both v4 and v6 addr even if v4 is denied for static alloc

Feature Changes

**Accounting messages for both IPv4 and IPv6 address**

Accounting start and stop messages showed both IPv4 and IPv6 address even if IPv4 address allocation was denied for static address allocation.

**Previous Behavior:** If IPv4 or IPv6 type failed when a UE request was received for dual PDP type, then the radius account failed IP address/PDP type.

**New Behavior:** If IPv4/IPv6 address allocation fails, then a new PDP type is sent and the correct IP address is in radius accounting.

CSCup51117 - Difference in behaviour for eHRPD and LTE for fragmented output packets

Feature Changes

**Behavior for eHRPD and LTE for Fragment Output Packets**

For P-GW service, Radius accounting was previously done post fragmentation at the session manager for downlink data. However, Gy/Gz accounting was done by ECS which was not aware of the fragmentation.

In order to be in sync, Radius accounting for P-GW service is now done prior to fragmentation. This change is done with acceptance that the P-GW CDR's and the S-GW CDR's may differ in data count because the S-GW does not reassemble these packets.

**Previous Behavior:** For downlink data, the LTE P-GW used to account the additional bytes was added as a result of fragmentation in Radius accounting only.

**New Behavior:** For downlink data, the LTE P-GW does not account for the additional bytes added as a result of fragmentation at the P-GW session manager in Radius accounting.
**Customer Impact:** Radius Accounting will now be exactly the same as Gy/Gz when the P-GW fragments downlink data.

**CSCzn58818 - [gn-gp]: Anomaly in the display of 'IP allocation type' in the o/p of c**

**Feature Changes**

**Anomaly in Display of ‘IP Allocation Type’ in show subscribers pgw/ggsn-only full all output**

The IP allocation type field was not correctly displayed in the `show subscribers pgw-only full all` or `show subscribers ggsn-only full all` CLI commands done by the AAA server.

**Previous Behavior:** The IP allocation type field was previously displayed as “Local Pool” for AAA allocated ip in the `show subscribers pgw-only full all` and `show subscribers ggsn-only full all` CLI commands.

**New Behavior:** Now, the IP allocation type field is displayed as “AAA” for AAA allocated ip in the `show subscribers pgw-only full all` and `show subscribers ggsn-only full all` CLI commands.
P-GW Enhancements for 16.1

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

---

**CSCug23975 - VoLTE: Prioritized handling of for VoLTE/Emergency calls**

**Feature Changes**

**Prioritized Handling for VoLTE/Emergency Calls Under Congestion Conditions**

New CLI has been introduced to configure eGTP-C service for handling prioritized APN/ARP(s).

If prioritized APN/ARP handling is enabled, and if the APN/ARP received in CSReq matches any of the configured prioritized APN/ARP values, any valid CSReq will not be rejected because of congestion control.

This feature impacts only CSReq handling for new incoming calls.

---

**Important:** This functionality requires that a valid VoLTE license key be installed. Contact your Cisco account representative for information on how to obtain a license.
Command Changes

gtpc

*allow-on-congestion* is a new keyword in this command that enables the prioritized handling for calls under congestion conditions for the specified APN/ARP(s).

```bash
configure

context context_name

  egtp-service service_name

[ no ] gtpc allow-on-congestion apn-name apn_name

[ no ] gtpc allow-on-congestion arp priority_level

end
```

Notes:

- *allow-on-congestion*
  
  Enables the prioritized handling for calls under congestion conditions.

- *apn-name* `apn_name`
  
  Configures the gateway to allow calls for this Access Point Name (APN), even under congestion.

  `apn_name` is a string between 1 and 64 alphanumeric characters. A maximum of 3 APNs can be configured.

- *arp* `priority_level`
  
  Configures the gateway to allow calls for this ARP, even under congestion.

  `priority_level` sets the priority value as an integer from 1 through 15. A maximum of 3 ARP values can be configured.

- There is no APN-to-ARP mapping.

- P-GW initiated dedicated bearer creation/updating is not changed due to this configuration.

Performance Indicator Changes

**show egtp-service**

The following new fields have been added:

- GTPC Prioritized APN
- GTPC Prioritized ARP

**show egtpc statistics verbose**

The following keywords have been added to the output to track the number of Create Session Request messages allowed at eGTP demux for each of the configured APN/ARP(s).

- Misc Statistics
- Prioritized APN/ARP Statistics
- APN
- CSReq allowed
- Prioritized APN/ARP Statistics
- ARP
- CSReq allowed

**CSCuh06375 - [PGW-S2a] Session creation after RADIUS Accounting-Response**

**Feature Changes**

**Session creation after RADIUS Accounting-Response**

**Previous Behavior:** Cisco PMIPv6-PGW (LMA) did not support session creation after RADIUS Accounting-Response. The Cisco P-GW already supported sending a “Create Session Response” message after receiving the RADIUS Accounting-Response for GTP.

**New Behavior:** Added support for Cisco PMIPv6-PGW (LMA) session creation after RADIUS Accounting-Response.

**Command Changes**

`mediation-device`

`delay-proxy-binding-ack` is a new keyword in this command that enables delaying PMIPv6 Proxy Binding Ack response until Accounting Start response is received from the accounting device.

`configure`

```
context context_name

  apn apn_name

    mediation-device delay-proxy-binding-ack

[ default | no ] mediation-device

end
```

**Notes:**

- `delay-proxy-binding-ack`: Enables delaying PMIPv6 Proxy Binding Ack response until Accounting Start response is received from the accounting device. Applicable to only PDP type IPv4 and IPv6 calls. Disabled by default.
CSCuh45717 - [PGW/S2a] Need support to Reject PBU (Type LE)

Feature Changes

Support to Reject PBU (Type LE)

Previous Behavior: Cisco PMIPv6 PGW (LMA) accepted a PMIPv6 “Proxy Binding Update” message with lifetime extension (Handoff Indicator type 5) when a GTP tunnel was established. If the HSGW has a junked session, then the HSGW sent a PMIPv6 “PBU” to the P-GW to update the lifetime. The message was accepted and the LTE session was terminated. Therefore, the UE needed to attach to customer's EPC network by user operation.

New Behavior: If a PMIPv6 “Proxy Binding Update” message with lifetime extension (Handoff indicator type 5) is received from the HSGW and a LTE session is already established, then the “Proxy Binding Update” message is rejected. Appropriate reject codes are present in the reject a PMIPv6 “Proxy Binding Acknowledge” message which is sent back to the HSGW.

CSCuh74228 - Unwanted UBRreq/UBResp for apn-ambr/QCI modification

Feature Changes

Combined Default Bearer QoS and APN-AMBR Change in Single UBRreq

Important: This is applicable only for P-GW service.

Previous Behavior:

1. When new default bearer QoS comes through MODIFY_BEARER_COMMAND (MBC) (HSS initiated bearer QoS modification procedure) from MME, P-GW sends 2 UBR
   - with unchanged APN-AMBR
   - with new default bearer QoS
2. When new default bearer QoS and new APN-AMBR come through MBC (HSS initiated bearer QoS modification procedure) from MME, P-GW sends 2 UBR
   - with new APN-AMBR
   - with new default bearer QoS
3. When new default bearer QoS and new APN-AMBR come through CCA-U, RAR from PCRF, P-GW sends 2 UBR
   - with new APN-AMBR
   - with new default bearer QoS

New Behavior:

1. When new default bearer QoS comes through MBC (HSS initiated bearer QoS modification procedure) from MME, P-GW sends only one UBR
   - with new default bearer QoS
2. When new default bearer QoS and new APN-AMBR come through MBC (HSS initiated bearer QoS modification procedure) from MME, P-GW sends only one UBR
   - with new default bearer QoS and new APN-AMBR

3. When new default bearer QoS and new APN-AMBR come through CCA-U, RAR from PCRF, P-GW sends only one UBR
   - with new default bearer QoS and new APN-AMBR

**Customer Impact:** New behavior reduces access-side signaling by way of consolidating IE in single UBR wherever applicable.

**CSCuh75147 - LP support for APN AMBR failure/Default EPS bearer failure**

**Feature Changes**

**LP Support for APN AMBR Failure/Default EPS Bearer Failure**

Local Policy engine shall now support two new event triggers:
- APN AMBR Modification Failure
- Default EPS Bearer Modification Failure

These event triggers are hit when MME/ePDG rejects a PCRF/Local Policy authorized QoS and informs the same to P-GW.

In order to support the new event triggers at Local Policy, two new event CLIs shall be added at Local Policy engine. The CLIs shall be used by Local Policy engine to map any incoming event from IMSA Module. If IMSA posts a Local Policy event for one of these new event triggers, Local Policy Engine does a rule match and selects the appropriate rule entry line inside eventbase configuration. After selecting the appropriate rule, Local Policy engine installs the actions configured against the rule entry.

**Command Changes**

```
rule

The following events have been added:
- apn-ambr-mod-failure
- def-eps-bearer-qos-mod-failure

configure

local-policy-service service_name

eventbase eventbase_name

rule priority priority event apn-ambr-mod-failure
ruledef ruledef_name actiondef actiondef_name [ continue ]

rule priority priority event def-eps-bearer-qos-mod-failure
ruledef ruledef_name actiondef actiondef_name [ continue ]
```
no rule priority priority
end

Notes:
- **apn-ambr-mod-failure**: The event is triggered as a result of an APN AMBR Modification Failure.
- **def-eps-bearer-qos-mod-failure**: The event is triggered as a result of a Default EPS Bearer Modification Failure.

## Performance Indicator Changes

**show local-policy statistics service**

The following output had been added to show the new event triggers.
- Event Statistics
  - APN-AMBR Mod Failure
  - Def EPS bearer Qos Mod Failure

### CSCui11722 - Xheader inserted bytes included in Radius Accounting.

## Feature Changes

### Data Packet Size Calculation

xheader inserted bytes are not counted in P-GW or S-GW CDR, however, the RADIUS accounting stop reported these xheader inserted bytes. Changes have been made to count only the original packet size in RADIUS accounting.

**Previous Behavior**: In RADIUS accounting for P-GW, data packet size was calculated after data was processed with ECS.

**New Behavior**: In RADIUS accounting for P-GW, data packet size is now calculated before data is processed with ECS.

**Customer Impact**: Additional/changed bytes post ECS processing will not be accounted for in RADIUS accounting.

### CSCuj73225 - IPv4 Downlink Data packet forwarding/redirection support

## Feature Changes

### Downlink Data packet forwarding/redirection

When this feature is enabled, the downlink IPv4 data packets received from the SGi will be forwarded/redirected to a configured next-hop address if the subscriber sessions does not exist in the P-GW. If the next-hop is not ARP resolvable, then the packet will be dropped. The appropriate interface stats will be updated with the packets forward/dropped counts.
Important: The `unconnected-address next-system ip address` keyword must be enabled to support the downlink IPv4 data packets forwarding/redirecting.

CSCuj73344 - PGW: IPv6 Network Reachability Server for IPv6 Pools

Feature Changes

IPv6 Network Reachability Server for IPv6 Pools

Previously, the NW-Reachability detection was available only for IPv4 addresses. This feature has introduced NW-Reachability detection for IPv6 address as well. This feature has also introduced VRF support for NW-Reachability detection.

This new configuration is used to restrict IP address allocation from a pool if the configured nw-reachability-server is not accessible. If the configured nw-reachability-server is not accessible, then the P-GW should not assign the address for a new call. Instead, the P-GW will respond back sending a GTPv2 "Create Session Response" with NO_RESOURCE_AVAILABLE.

For IPv4, ICMP pings are used for reachability checking. Usually, this configuration is used along with the next-hop-forwarding address configuration. Also, the nw-reachability server is normally an ISP server beyond the next-hop.

Command Changes

`nw-reachability server`

This command includes a new `vrf` keyword to specify an existing VRF name as an alphanumeric string of 1 through 63 characters.

```
configure
  context context_name
    nw-reachability server server_name
      vrf name
    end
```

`show nw-reachability server`

This command includes two new keywords `ipv4-only` and `ipv6-only` to display IPv4/IPv6 Network Reachability Detection servers.

```
show nw-reachability server server_name
  ipv4-only
  ipv6-only
```
CSCuj73352 - PGW: ICSR support for customer enterprise PGW

Feature Changes

ICSR support for customer enterprise P-GW

Confirmed that ICSR is supported for customer enterprise P-GW.

CSCuj73381 - PGW: PGW capability improvements

Feature Changes

P-GW capability improvements

Confirmed P-GW capability improvements.

CSCuj88821 - Clab: gtpc overload-protection ingress CLIs cause misleading

Feature Changes

‘show configuration’ Output Changed After ‘no gtpc overload-protection ingress’ Command

Previous Behavior: By default, after entering no gtpc overload-protection ingress command, no gtpc overload-protection ingress was displayed for show configuration command.

New Behavior: Overload Protection cannot be disabled on the Ingress side. Therefore, the following default values are now displayed in the CLI output for show configuration command:

gtpc overload-protection ingress msg-rate 20000 delay-tolerance 100 queue-size 10000

CSCuj89567 - show sub subsystem stats incorrect

Feature Changes

Enhancement to SAEGW for RAT-Based Counters

The SAEGW software has been enhanced to provide counters for the active PDNs based on RAT type. Counters have also been added to track successful, attempted, and failed counters for LTE to S4-SGSN, S4-SGSN to LTE, GNGP to S4-SGSN and S4-SGSN to GNGP handovers.
Performance Indicator Changes

P-GW Schema

The following bulk statistics have been added to the P-GW schema to support the enhancement to show subscriber subsystem statistics:

- sesstat-pdn-rat-eutran
- sesstat-pdn-rat-utran
- sesstat-pdn-rat-geran
- sesstat-pdn-rat-wlan
- sesstat-pdn-rat-other
- handoverstat-gngptos4sgnsucc
- handoverstat-gngptos4sgsnfail
- handoverstat-gngptos4sgsnatt
- handoverstat-s4sgsntogngpsucc
- handoverstat-s4sgsntogngpfail
- handoverstat-s4sgntogngpatt
- handoverstat-ltetos4sgnsucc
- handoverstat-ltetos4sgsnfail
- handoverstat-ltetos4sgsnatt
- handoverstat-s4sgsntoltettatt
- handoverstat-s4sgsntoltesucc
- handoverstat-s4sgsntoltefail

SAEGW Schema

The following bulk statistics have been added to the SAEGW schema to support the enhancement to show subscriber subsystem statistics:

- saegw-collapsed-pdn-rat-eutran
- saegw-pgw-anchor-pdn-rat-eutran
- pgw-sesstat-pdn-rat-eutran
- saegw-sgw-anchor-pdn-rat-eutran
- saegw-collapsed-pdn-rat-utran
- saegw-pgw-anchor-pdn-rat-utran
- pgw-sesstat-pdn-rat-utran
- saegw-sgw-anchor-pdn-rat-utran
- saegw-ggsn-pdn-rat-utran
- saegw-collapsed-pdn-rat-geran
- saegw-pgw-anchor-pdn-rat-geran
- pgw-sesstat-pdn-rat-geran
- saegw-sgw-anchor-pdn-rat-geran
- saegw-ggsn-pdn-rat-geran
- saegw-pgw-anchor-pdn-rat-wlan
- pgw-sesstat-pdn-rat-wlan
- saegw-ggsn-pdn-rat-wlan
- saegw-collapsed-pdn-rat-other
- saegw-pgw-anchor-pdn-rat-other
- pgw-sesstat-pdn-rat-other
- saegw-sgw-anchor-pdn-rat-other
- saegw-ggsn-pdn-rat-other
- pgw-handoverstat-gngptos4sgsnsucc
- pgw-handoverstat-gngptos4sgsnfail
- pgw-handoverstat-gngptos4sgsnatt
- pgw-handoverstat-s4sgsntogngpsucc
- pgw-handoverstat-s4sgsntogngpfail
- pgw-handoverstat-s4sgntogngpatt
- pgw-handoverstat-ltetos4sgsnsucc
- pgw-handoverstat-ltetos4sgsnfail
- pgw-handoverstat-ltetos4sgsnatt
- pgw-handoverstat-s4sgsntolteatt
- pgw-handoverstat-s4sgsntoltesucc
- pgw-handoverstat-s4sgsntoltefail

show subscriber summary saegw-only/show subscriber summary pgw only

The output of this command has been enhanced to track 4G, 3G, 2G and Other PDN counters

- Total PDNs by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - WLAN
  - OTHER

show saegw-service statistics all / show saegw-service statistics name
The output of this command has been enhanced to track various handover statistics between network elements based on RAT type.

- Current PDNs By RAT-Type and Operational Mode
  - Colocated PDNs
    - EUTRAN
    - UTRAN
    - GERAN
    - OTHER
  - PGW-Anchor PDNs
    - EUTRAN
    - UTRAN
    - GERAN
    - WLAN
    - OTHER
  - SGW-Anchor PDNs
    - EUTRAN
    - UTRAN
    - GERAN
    - WLAN
    - OTHER
  - GGSN-Anchor PDN
    - UTRAN
    - GERAN
    - WLAN
    - OTHER

**show saegw-service statistics name function pgw verbose**

The output of this command has been enhanced to track handover stats between S4-SGSN and LTE, Gn/Gp SGSN and S4-SGSN, LTE to S4-SGSN and S4-SGSN to Gn/Gp SGSN.

- Handover Statistics
  - GNGP-to-S4SGSN Handover
    - Attempted
    - Succeeded
    - Failed
  - S4SGSN-to-GNGP handover
    - Attempted
- Succeeded
- Failed

- S4SGSN-to-LTE handover
  - Attempted
  - Failed
  - Succeeded

- LTE-to-S4SGSN handover
  - Attempted
  - Succeeded
  - Failed

**show pgw service statistics all / show pgw-service statistics name**

The output of this command has been enhanced to track PDN counts based on RAT type.

- Current PDNs by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - WLAN
  - Other

**show pgw-service statistics all / show pgw-service statistics name**

The output of these commands has been enhanced to track handover statistics between the S4-SGSN and LTE, Gn/Gp SGSN and S4-SGSN, LTE to S4-SGSN and S4-SGSN to Gn/Gp SGSN.

- Inter Technology handover
  - GNGP-to-S4SGSN handover
    - Attempted
    - Succeeded
    - Failed

- S4SGSN-to-GNGP handover
  - Attempted
  - Succeeded
  - Failed

- S4SGSN-to-LTE handover
  - Attempted
  - Succeeded
  - Failed
- LTE-to-S4SGSN handover
  - Attempted
  - Succeeded
  - Failed

**CSCun12922 - Dedicated bearer timeout Min value to be 5 min**

**Command Changes**

```shell
timeout bearer-inactivity
```

This command configures the bearer inactivity timer and the threshold value of the traffic through an APN. The minimum configurable value of bearer inactivity timer has been reduced from 900 seconds to 300 seconds.

```shell
configure
  context context_name
  apn apn_name
    timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { downlink | total | uplink } bytes
    timeout bearer-inactivity exclude-default-bearer
    no timeout bearer-inactivity [ exclude-default-bearer | gbr | non-gbr ]
end
```

Notes:
- `dur_seconds`: Specifies the timeout for the bearer inactivity timer in seconds. Valid entries are from 300 to 2592000 seconds (5 minutes to 720 hours).

**CSCun84742 - S6b Assume +ve counter is missing for the Current Subs in system**

**Feature Changes**

**Statistics added for S6b Assume Positive State for Subscribers**

AAA diameter authentication can be configured to assume the subscriber as valid for certain AAR error response code and by-pass S6b from then on. Counters have been introduced on the GGSN, P-GW, SAEGW to display the total number of subscribers which are in S6b by-passed state (also called “assumed positive”).
Performance Indicator Changes

PGW Schema

The following bulk statistic has been added to display the total number of subscribers in the assumed positive state.

- ue-s6b-assume-positive

SAEGW Schema

The following bulk statistic has been added to display the total number of subscribers in the assumed positive state.

- pgw-ue-s6b-assume-positive

GTP Schema

The following bulk statistic has been added to display the total number of subscribers in the assumed positive state.

- setup-ggsn-s6b-assume-positive

show gtpc statistics

The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Session Stats:
  - S6b Assume Positive:

show subscribers pgw-only full

The output of this command has been enhanced to display S6b Auth Status shown as By-passed if S6b auth failed and in the assumed positive state.

- S6b Auth Status:

show subscribers pgw-only summary

The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Total S6b Assume Positive:

show pgw-service statistics all

The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Subscriber Total
  - Total S6b Assume Positive:

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.

### CSCuo16591 - Radius Acct Interim Update for Qos Change generated for all bearers

**Feature Changes**

**Previous Behavior:**
- In UBResp handling in case of only APN-AMBR change, Radius Acct Interim Update generated only for default bearer.
- In UBResp handling in case of single dedicated bearer QoS change, Radius Acct Interim Update generated for all bearers present in UBReq.

**New Behavior:**
- In UBResp handling in case of APN-AMBR change, Radius Acct Interim Update generated for all non-GBR bearers present in call.
- In UBResp handling in case of single dedicated bearer QoS change, Radius Acct Interim Update generated only for that dedicated bearer.

### CSCup03974 - No syslog generated for nw-reachability server status change Down -> Up

**Feature Changes**

**Previous Behavior:** No syslog generated for nw-reachability server status change Down -> Up.

**New Behavior:** Syslog now generated for nw-reachability server status change Down -> Up.

### CSCup08125 - congestion state is not retained after egtpinmgrp kill and recovery

**Feature Changes**

**Congestion State Sent to Session Controller**

**Previous Behavior:** Congestion state was sent from resource manager to session controller only when there was change in congestion state.

**New Behavior:** Congestion state is now sent periodically to the session controller.
P-GW Enhancements for 16.0

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

---

**CSCts49711 - [GTP-S5] Rad-Acct: No Interim for ULI-chng using ChngNotificationTrigger**

**Feature Changes**

**Radius Accounting Interim Record**

**Previous Behavior:** Radius Accounting Interim Record is not generated for ULI change using the Change Notification Trigger.

**New Behavior:** Radius Accounting Interim Record is now generated for ULI change using the Change Notification Trigger.

**Customer Impact:** In this scenario, ULI change using the Change Notification Trigger will now generate Radius Accounting Interim Record.
CSCua47367, CSCuh30602 - Enhance PGW to report exact failure resulting in CC 73

Feature Changes

Additional Statistics for Cause Code 73: No Resource Available

In many scenarios, the P-GW responds to a Create Session Request by sending a Create Session Response with a Cause Code 73 (NO RESOURCE AVAILABLE), thereby rejecting the session attempt. Cause Code 73 can be sent for multiple reasons.

In this release, new bulk statistics have been introduced to further identify the exact sub-causes of error Cause Code 73. The output of `show pgw-service statistics all verbose` has also been enhanced to show counters for Cause Code 73 sub-causes.

**Important**: These counters are cumulative of GGSN and P-GW. GGSN responds to a Create PDP Context Request by sending a Create PDP Context Response with a Cause Code 73 (NO RESOURCE AVAILABLE), similar to P-GW.

**Customer Impact**: Enhanced statistics will help operators know the exact cause for rejection of the PDN setup at the P-GW and thereby assist in identifying issues.

Performance Indicator Changes

P-GW Schema

The following new statistics have been added to show sub-causes of error cause CC73 (no resource available).

- `sessstat-bearrej-nores-s6brad-ip`
- `sessstat-bearrej-nores-ims-auth-failed`
- `sessstat-bearrej-nores-chrgsvc-auth-failed`
- `sessstat-bearrej-nores-dhcp-ip-failed`
- `sessstat-bearrej-nores-setup-timeout`
- `sessstat-bearrej-nores-aaa-auth-exceed`
- `sessstat-bearrej-nores-no-sess-aaa`
- `sessstat-bearrej-nores-conflict-addr`
- `sessstat-bearrej-nores-static-ip`
- `sessstat-bearrej-nores-msreq-invalid-ip`
- `sessstat-bearrej-nores-other-reason`

SAEGW Schema

The following new statistics have been added to show sub-causes of error cause CC73 (no resource available).

- `pgw-sessstat-bearrej-nores-s6brad-ip`
- pgw-sessstat-bearrej-nores-ims-auth-failed
- pgw-sessstat-bearrej-nores-chrgsvc-auth-failed
- pgw-sessstat-bearrej-nores-dhcp-ip-failed
- pgw-sessstat-bearrej-nores-setup-timeout
- pgw-sessstat-bearrej-nores-aaa-auth-exceed
- pgw-sessstat-bearrej-nores-no-sess-aaa
- pgw-sessstat-bearrej-nores-conflict-ip-addr
- pgw-sessstat-bearrej-nores-static-ip
- pgw-sessstat-bearrej-nores-msreq-invalid-ip
- pgw-sessstat-bearrej-nores-other-reason
- saegw-ggsn-sessstatbearrej-nores-s6brad-ip
- saegw-ggsn-sessstatbearrej-nores-ims-auth-failed
- saegw-ggsn-sessstatbearrej-nores-chrgsvc-auth-failed
- saegw-ggsn-sessstatbearrej-nores-dhcp-ip-failed
- saegw-ggsn-sessstatbearrej-nores-setup-timeout
- saegw-ggsn-sessstatbearrej-nores-aaa-auth-exceed
- saegw-ggsn-sessstatbearrej-nores-no-sess-aaa
- saegw-ggsn-sessstatbearrej-nores-conflict-ip-addr
- saegw-ggsn-sessstatbearrej-nores-static-ip
- saegw-ggsn-sessstatbearrej-nores-msreq-invalid-ip
- saegw-ggsn-sessstatbearrej-nores-other-reason

**show pgw-service statistics all verbose**

The following output had been added to show sub-causes of error cause CC73 (no resource available).
- Create Sess Rsp Denied - No Resource Reasons:
- New Call Policy Reject
- Session Manager Dead
- Session Mgr Not Ready
- ICSR State Invalid
- Charging Svc Auth Fail
- no session in aaa
- Conflict in ip address
- other reasons
- Session Setup Timeout
- S6B/radius IP Validation Failed
- Num license exceeded
- No Session Manager
- Congestion Policy Applied
- Input pacing queue exceeded
- ims auth failed
- aaa auth req exceeded/failed
- static ip not present
- ms req invalid ip
- DHCP IP Address Not Present
- mem_alloc_failed

**CSCua97985 - Graceful Shutdown of PDN with inactive VoLTE calls**

**Feature Changes**

**Graceful Shutdown Support for VoLTE**

There are likely to be cases where an Operator would need to shut down a P-GW/S-GW/SAEGW for upgrade/maintenance purpose; during that time, 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.

This could also be used in case there is a need to migrate a VoLTE APN from one P-GW to another. This feature will help in doing this VoLTE APN migration in a graceful manner. A new qualifier, `non-volte-call`, has been added to the `clear subscribers` CLI to clean up only those PDNs that have no Active Voice bearer. Identification of the VoLTE PDN and bearer is done using the VoLTE call identification configuration discussed above.

Until the time the upgrade/maintenance is going on, the new calls will be rejected so that an alternate P-GW/S-GW/SAEGW can handle it. This is done using the `new-call policy` configuration.

Below are the set of steps that can be carried out to gracefully clean up VoLTE PDNs on a node:

1. Use call identification configuration to configure the VoLTE APN to do the VoLTE PDN and bearer identification.
2. Using the new call-policy configuration, configure the node to reject any new calls coming on the node, so that these new calls get directed to an alternate PDN.
3. Using the `clear subscribers` CLI with `non-volte-call` qualifier in it, initiate the clean up of PDNs that don’t have any Active Voice bearer.
4. Wait for some time and execute the `clear subscribers` CLI again to clean up any non-active VoLTE PDNs. Repeat this step until all of the VoLTE PDNs are cleaned up.

Further enhancements are planned for this feature in future releases.

**Customer Impact:** Several features added for VoLTE in 16.0 will provide a lot of value to Operators; they help Operator in providing high quality VoLTE service to ensure better user experience for VoLTE service users.
Command Changes

**clear subscribers**

*non-volte-call* is a new keyword that initiates the clean up of PDNs that don’t have any Active Voice bearer.

`clear subscribers apn apn_name non-volte-call [ max-subscribers max_count ] [ uniform ]`

`clear subscribers all non-volte-call [ max-subscribers max_count ] [ uniform ]`

`clear subscribers non-volte-call [ max-subscribers max_count ] [ uniform ]`

**Notes:**
- *non-volte-call*: Disconnects PDN connections that do not have an active voice call.
- *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.

**CSCua99366 - Dedicated bearer timeout action**

Feature Changes

**Dedicated Bearer Timeout Support on the P-GW**

---

**Important:** For this release, this feature is Lab/Trial Quality only.

The P-GW has been enhanced to support a configurable bearer inactivity timeout for non-GBR P-GW bearer type sessions. This enables the deletion of bearers experiencing less data traffic than the configured threshold value.

Command Changes

**timeout bearer-inactivity**

The command `timeout bearer-inactivity` now supports a bearer inactivity timeout for GBR and non-GBR P-GW bearer type sessions.

---

**Important:** P-GW only supports non-GBR bearer type sessions.

```
configure

   context context_name

   apn apn_name

   timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { downlink | total | uplink } bytes
```
timeout bearer-inactivity exclude-default-bearing

no timeout bearer-inactivity [ exclude-default-bearing | gbr | non-gbr ]
end

Notes:

- **timeout**: Specifies that a bearer time out value will be configured for this APN.
- **bearer-inactivity**: Specifies that the system will check for low activity for a bearer.
- **gbr**: Specifies that the P-GW will check for low activity on a GBR bearer.
- **non-gbr**: Specifies that the P-GW will check for low activity on a non-GBR bearer.
- **dur_seconds**: Specifies the timeout for the bearer inactivity timer in seconds. Valid entries are from 300 to 2592000 seconds (5 minutes to 720 hours).
- **volume-threshold**: Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.
- **downlink**: Threshold value of the downlink data traffic in a bearer.
- **total**: Specifies that the total of both uplink and downlink data will be used as a volume threshold.
- **uplink**: Threshold value of the uplink data traffic in a bearer.
- **bytes** must be a value from 1 to 4294967295.
- **exclude-default-bearing**: Ignore bearer inactivity handling for default/primary bearer.

**Performance Indicator Changes**

**show apn name**

This command has been enhanced to list bearer inactivity timeout settings, if configured.

- bearer inactivity timeout (GBR Bearers)
- bearer inactivity timeout (Non-GBR Bearers)
- bearer inactivity exclude-default-bearing

**show pgw-service-statistics all verbose**

This command has been enhanced to list bearer inactivity timeout settings, if configured.

- Inactivity timeout:
  - QCI 1: :seconds
  - QCI 2: :seconds
  - QCI 3: :seconds
  - QCI 4: :seconds
  - QCI 5: :seconds
  - QCI 6: :seconds
CSCub27300 - ASR5500 - Newcall support for rejecting calls on PGW

Feature Changes

Newcall Policy Per APN for Rejecting Calls on P-GW

Newcall policy to reject new calls on the P-GW was already supported at the P-GW service level. In this release, support is added to allow configuration of the Newcall policy at the APN-level.

Inter-tech Handover requests (S2b to LTE, LTE to S2b, and eHRDP to LTE) which come as Create Session Requests on the P-GW are now processed (not rejected) when the “Handover Indication” flag is set, otherwise Create Session Request will be treated as new session request and an APN rejection policy will be applied.

Customer Impact: This will assist operators in managing graceful migration of APNs from one node to another.

Command Changes

newcall policy

The keywords `apn name` have been added to enable new call policy for P-GW and SAEGW services configured in the same context.

`newcall policy pgw-service apn name apn_name reject`

`no newcall policy pgw-service apn name apn_name`

Notes:

- `pgw-service`: Associates the new call policy with the specified P-GW service, and any SAEGW service associated with this P-GW service, in this context.
- `apn name apn_name reject`: Associates the new call reject policy with the specified APN name in this context.
- `no`: Disables the new call reject policy with the specified APN name in this context.

CSCuc14962 - LI keep alive sent per sessmgr not per tcp connection

Feature Changes

Support for LI Keepalive Messages Per TCP Connection

Lawful Intercept now sends a single keepalive packet per TCP connection, rather than per sessmgr instance. This enhancement reduces the amount of unnecessary keepalive traffic.
Previous Behavior: Lawful Intercept sent keepalive packets per sessmgr instance.
New Behavior: Lawful Intercept sends a keepalive packet per TCP connection.
Customer Impact: Reduced amount of unnecessary keepalive traffic.

CSCuc87231 - HSGW, PGW support Pmipv6 control protocol over ipv4

Feature Changes

HSGW and P-GW support for Pmipv6 control protocol over ipv4

Previous Behavior: Previously, mag-service could only bind with IPv6 address.

```bash
mag-service mag10
bind address 4124::30:30:2
```

New Behavior: With this new behavior, mag-service is capable of binding on IPv4 interface as well.

```bash
mag-service mag10
bind ipv4-address 192.50.50.6
```

Command Changes

```bash
bind
```

New keyword `ipv4-address` has been added to bind MAG service with IPv4 address.

```bash
configure
mag-service service_name
bind ipv4-address ip_address
no bind ipv4-address
end
```

CSCud60395 - Local Break Out support for VoLTE roaming

Feature Changes

Support for Enabling or Disabling S6b Authentication Per-APN

Local Break Out is the ability of VPMLN to locally break out IP traffic, such as VoLTE traffic, when network policies and user subscription allow it.
**Previous Behavior:** Earlier, S6b authentication could be enabled/disabled on P-GW node level. There was no support to enable/disable it on a per-APN level.

**New Behavior:** Support is now added to enable/disable S6b authentication on a per-APN level.

If S6b authorization is enabled at P-GW service, it can be disabled for a single APN using `ignore-alt-config no-s6b` CLI at APN. This is currently applicable only to P-GW service.

---

**Important:** Configuration in APN will take precedence over configuration in service configuration.

---

**Figure 1.** Flow chart for functioning of CLI “ignore-alt-config no-s6b”, if authorization enabled in P-GW service

---

Configuration in P-GW service is kept for backward compatibility.

**Customer Impact:** Provides flexibility to the Operator to enable S6b authentication on needed APNs only instead of enabling it for all the APNs on that P-GW node.

---

**Command Changes**

`ignore-alt-config`
This new command enables/disables S6b authentication on a per-APN level.

```
configure
  context context_name
    apn apn_name
      [ no ] ignore-alt-config no-s6b
    end
```

Notes:
- Ignores alternate service-level configuration for S6b authorization when S6b authorization is disabled at APN.
- Disables S6b authentication on a per-APN level.

**Performance Indicator Changes**

**show apn name**

The following keyword has been added to the output to display whether S6b authentication is enabled or disabled on a specified APN.
- ignore-alt-config (no-s6b)

**CSCue00897 - PGW - support GTPv2 S2a interface and inter-access mobility**

**Feature Changes**

**P-GW GTP Based S2a**

GTP based S2a is a 3GPP Release 11 feature introduced to support Trusted WiFi integration in the EPC core network using GTP based S2a interface between SAMOG (TWAG) Gateway and P-GW. This support is in addition to the GTP based S2b support for Untrusted WiFi, which was added in Release 15.0

**Important:** Gz (P-GW-CDR) is not supported for GTP based S2a calls.

**Customer Impact:** This feature enables operators to integrate SP WiFi network with EPC Core and share the EPC Core resources and framework for WiFi Access as well.

**CSCue15246 - PGW support - S2a PMIPv6 over IPv4 transport**

**Feature Changes**

**PGW Support - S2a PMIPv6 Over IPv4 Transport**
Customers will have new option to deploy and plan their network using new transport type.

**Important:** This feature is only supported for ASR 5500 platform.

**Previous Behavior:** S2a interface did not have transport support for IPv4-IPv6-MH style encoding.

**New Behavior:** This feature has introduced new transport-level support where PMIPv6 packet will be encoded with IPv6 and IPv4 headers. Packet will be sent on IPv4 transport.

**CSCug24179 - VoLTE related optimization- Fetching of VoLTE needs to be prioritized.**

**Performance Indicator Changes**

**show session subsystem facility aaamgr instance**

Two new counters display the number of priority and non-priority recovery records that are available for recovery while executing the show command.

- Current valid priority recovery records
- Current valid non-priority recovery records

**CSCug38359, CSCug72349 - QCI Based Stats for CLI and Bulkstats**

**Feature Changes**

**Additional QCI Based Statistics at APN and P-GW Levels**

The new statistics/counters are available using the `show bulkstats variables apn` and `show bulkstats variables pgw` commands.

The new bulkstats are available in the APN and P-GW bulkstats schema.

**Customer Impact:** This enhancement enables operators to gain more visibility on per-QCI based activity in the network.

**Performance Indicator Changes**

**APN Schema**

The following new bulk statistics have been added to enable operators to gain more visibility on per-QCI based activity in the network:

- qci1-uplinkpkt-drop-mbrexcd
- qci1-dwlinkpkt-drop-mbrexcd
- qci1-uplinkbyte-drop-mbrexcd
- qci1-dwlinkbyte-drop-mbrexcd
- qci1-rejbearer
- qci2-uplinkpkt-drop-mbrexcd
- qci2-dwlinkpkt-drop-mbrexcd
- qci2-uplinkbyte-drop-mbrexcd
- qci2-dwlinkbyte-drop-mbrexcd
- qci2-rejbearer
- qci3-uplinkpkt-drop-mbrexcd
- qci3-dwlinkpkt-drop-mbrexcd
- qci3-uplinkbyte-drop-mbrexcd
- qci3-dwlinkbyte-drop-mbrexcd
- qci3-rejbearer
- qci4-uplinkpkt-drop-mbrexcd
- qci4-dwlinkpkt-drop-mbrexcd
- qci4-uplinkbyte-drop-mbrexcd
- qci4-dwlinkbyte-drop-mbrexcd
- qci4-rejbearer
- qci5-uplinkpkt-drop-mbrexcd
- qci5-dwlinkpkt-drop-mbrexcd
- qci5-uplinkbyte-drop-mbrexcd
- qci5-dwlinkbyte-drop-mbrexcd
- qci5-rejbearer
- qci6-uplinkpkt-drop-mbrexcd
- qci6-dwlinkpkt-drop-mbrexcd
- qci6-uplinkbyte-drop-mbrexcd
- qci6-dwlinkbyte-drop-mbrexcd
- qci6-rejbearer
- qci7-uplinkpkt-drop-mbrexcd
- qci7-dwlinkpkt-drop-mbrexcd
- qci7-uplinkbyte-drop-mbrexcd
- qci7-dwlinkbyte-drop-mbrexcd
- qci7-rejbearer
- qci8-uplinkpkt-drop-mbrexcd
- qci8-dwlinkpkt-drop-mbrexcd
P-GW Changes in Release 16

- qci8-uplinkbyte-drop-mbrexcd
- qci8-dwlinkbyte-drop-mbrexcd
- qci8-rejbearer
- qci9-uplinkpkt-drop-mbrexcd
- qci9-dwlinkpkt-drop-mbrexcd
- qci9-uplinkbyte-drop-mbrexcd
- qci9-dwlinkbyte-drop-mbrexcd
- qci9-rejbearer
- invalidqci-rejbearer

P-GW Enhancements for 16.0

The following 16 new bulk statistics below have been added to enable operators to gain more visibility on per-QCI based activity in the network:

- servstat-upPrioritymark-p0
- servstat-upPrioritymark-p1
- servstat-upPrioritymark-p2
- servstat-upPrioritymark-p3
- servstat-upPrioritymark-p4
- servstat-upPrioritymark-p5
- servstat-upPrioritymark-p6
- servstat-upPrioritymark-p7
- servstat-downPrioritymark-p0
- servstat-downPrioritymark-p1
- servstat-downPrioritymark-p2
- servstat-downPrioritymark-p3
- servstat-downPrioritymark-p4
- servstat-downPrioritymark-p5
- servstat-downPrioritymark-p6
- servstat-downPrioritymark-p7

show apn statistics all

The following statistics have been added in the output of the above command:

- Subscriber QoS Statistics
- QCI1: Bearer Rejected
- QCI1: Uplink Bytes dropped(MBR Excd)
- QCI1: Downlink Bytes dropped(MBR Excd)
- QCI1: Uplink pkts dropped(MBR Excd)
- QCI1: Downlink pkts dropped(MBR Excd)
- QCI2: Bearer Rejected
- QCI2: Uplink Bytes dropped(MBR Excd)
- QCI2: Downlink Bytes dropped(MBR Excd)
- QCI2: Uplink pkts dropped(MBR Excd)
- QCI2: Downlink pkts dropped(MBR Excd)
- QCI3: Bearer Rejected
- QCI3: Uplink Bytes dropped(MBR Excd)
- QCI3: Downlink Bytes dropped(MBR Excd)
- QCI3: Uplink pkts dropped(MBR Excd)
- QCI3: Downlink pkts dropped(MBR Excd)
- QCI4: Bearer Rejected
- QCI4: Uplink Bytes dropped(MBR Excd)
- QCI4: Downlink Bytes dropped(MBR Excd)
- QCI4: Uplink pkts dropped(MBR Excd)
- QCI4: Downlink pkts dropped(MBR Excd)
- QCI5: Bearer Rejected
- QCI5: Uplink Bytes dropped(MBR Excd)
- QCI5: Downlink Bytes dropped(MBR Excd)
- QCI5: Uplink pkts dropped(MBR Excd)
- QCI5: Downlink pkts dropped(MBR Excd)
- QCI6: Bearer Rejected
- QCI6: Uplink Bytes dropped(MBR Excd)
- QCI6: Downlink Bytes dropped(MBR Excd)
- QCI6: Uplink pkts dropped(MBR Excd)
- QCI6: Downlink pkts dropped(MBR Excd)
- QCI7: Bearer Rejected
- QCI7: Uplink Bytes dropped(MBR Excd)
- QCI7: Downlink Bytes dropped(MBR Excd)
- QCI7: Uplink pkts dropped(MBR Excd)
- QCI7: Downlink pkts dropped(MBR Excd)
- QCI8: Bearer Rejected
- QCI8: Uplink Bytes dropped(MBR Excd)
• QCI8: Downlink Bytes dropped(MBR Excd)
• QCI8: Uplink pkts dropped(MBR Excd)
• QCI8: Downlink pkts dropped(MBR Excd)
• QCI9: Bearer Rejected
• QCI9: Uplink Bytes dropped(MBR Excd)
• QCI9: Downlink Bytes dropped(MBR Excd)
• QCI9: Uplink pkts dropped(MBR Excd)
• QCI9: Downlink pkts dropped(MBR Excd)
• Invalid/ Not-Configured QCI: Bearer Rejected

CSCug41145 - QoS eARP - H & M configuration configuration on GGSN/PGW

Feature Changes

QoS eARP: Support for Configuration of H & M Values

When E-ARP is not supported by the SGSN, it is required to convert Gx ARP-AVP to UMTS ARP value and vice versa. This conversion of ARP value is done as per the table in section B.3.3.3.1 and B.3.3.3.2 of 3GPP TS 29.212. ‘H’ (high priority) and ‘M’ (medium priority) values in these tables are now configurable. In previous release, the values for H and M were hard coded.

Customer Impact: This feature ensures proper treatment of users with higher priority level information, and provides the operator greater control of the end-to-end QoS eARP.

CSCug75135 - PGW LORC mechanism for subscriber billing

Feature Changes

Overcharging Protection - 3GPP V11 Compliance

The Overcharging Protection feature introduced in StarOS Release 15.0 has now been standardized in 3GPP Version 11. Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode.

In StarOS Release 15.0 Overcharging Protection was implemented as a custom feature using Private Extension IEs. In this release, the feature is now updated to align with the 3GPP TS 29.274; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C) specification.

Command Changes

gtpc

private-extension is a new keyword in this command that enables/disables encode/decode of overcharge-protection-related data in/from private extension instead of Indication IE.
configure

context context_name

egtp-service variable

[ no ] gtpc private-extension overcharge-protection

end

Notes:

- By default, this configuration is disabled and encode/decode of overcharge-protection-related data will be done via Indication IE.
- Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Performance Indicator Changes

show egtp-service name

The following keyword has been added to the output to display whether encode/decode of overcharge-protection-related data in/from private extension is enabled or disabled.

- GTPC Private Extension
- Overcharging Protection

CSCug95856 - GGSN - Common flags control through CLI

Feature Changes

Common Flags Control

NQN and UQS flag values needs to be configurable through CLIs.
Common flags are now updated based on new CLI keywords in peer profile configuration for GGSN.

CSCuh28006, CSCul24601, CSCul24817 - Additional application support with DSCP-802.1p Marking per Interface

Feature Changes

Internal-QoS

Important: For this release, this feature is Lab/Trial Quality only.
To consolidate L2-level QoS marking across all interfaces, marking IP-DSCP values will be left to individual applications as applications build IP headers. The DSCP value in IP-header will then be used to derive the L2 QoS Values by platform (NPU). This derivation will be done in two steps.

1. DSCP will be mapped to an Internal-QoS value using a system-wide table.
2. Internal-QoS will be mapped to actual L2 value (either or both of 802.1p/MPLS) using a per-vrf based table.

Internal-QoS (Internal-Per-Hop-Behavior/IPHB) consists of 5 bits. 3 bits of class-of-service is user-configurable, while the remaining 2 bits are left for future use to dynamically stamp a drop eligibility based on a rate-monitor.

The 64 DSCP values will map, each to any of the available 8 COS values of Internal-QoS. The 5 bits of Internal-QoS will then map to 3+1 bits of 802.1p (the tos and drop-eligibility-indicator) and 3 bits of MPLS-Traffic-Class.

In addition, the explicit configuration of 802.1p/MPLS-EXP is being deprecated and it will be replaced by new construct of internal-qos.

**Previous Behavior:** Operator can set 802.1p and mpls priorities in the `qci-qos-mapping` table.

**New Behavior:** Operator can only configure internal-qos parameters.

**Customer Impact:** Due to backward compatibility, previous configuration should still work.

Going forward, customer can only configure `internal-qos` in `qci-qos-mapping` table.

### Command Changes

**associate**

This new command is used to associate an internal QoS L2 mapping table to a VPN context.

```
configure
  context vpn_name
    associate l2-mapping-table name 12_mapping_table_name
    default associate l2-mapping-table
  end
```

**Notes:**
- `l2-mapping-table name 12_mapping_table_name`
  - Specifies the name of an existing internal table from which to map QoS to L2 values.
  - `map_table_name` is an alphanumeric string of 0 through 80 characters.
- `default`: Associates the system-default table with this context.
- If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.
- If no explicit association is created/configured, the system-default mapping table is used.

**associate l2-mapping-table**

This new command is used to associate an internal QoS L2 mapping table to a specific VPN Routing and Forwarding (VRF).

```
configure
  context
    associate l2-mapping-table name 12_mapping_table_name
  end
```

**Notes:**
- `l2-mapping-table name 12_mapping_table_name`
  - Specifies the name of an existing internal table from which to map QoS to L2 values.
  - `map_table_name` is an alphanumeric string of 0 through 80 characters.
- `default`: Associates the system-default table with this context.
- If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.
- If no explicit association is created/configured, the system-default mapping table is used.
context vpn_name

ip vrf vrf_name

associate l2-mapping-table { name l2_mapping_table_name | system-default }

no associate l2-mapping-table

end

Notes:
- **name table_name**: Specifies the name of an existing internal table from which to map QoS to L2 values. 
  *table_name* is an alphanumerical string of 0 through 80 characters.
- **system-default**: Associates the system-default table with this VRF. This is useful if the base-context has a different explicit mapping.
- **no**: Disassociates an existing L2 mapping table from this VRF.
- If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.
- If no explicit association is created/configured, the system-default mapping table is used.

**internal-priority**

This new command is used to map internal QoS priority with Class of Service (COS) values.

configure

qos l2-mapping-table { name map_table_name | system-default }

  internal-priority cos class_of_service_value color color_value [ 802.1p-value 802.1p-value ] [ mpls-tc mpls-tc-value ]

  default internal-priority cos cos_value color color_value

end

Notes:
- **cos**: Maps to the internal QoS priority/class-of-service.
  *class_of_service_value* must be a Hexadecimal number between 0x0 and 0x7.
- **color**: Controls drop precedence of service to map to.
  *color_value* must be a Hexadecimal number between 0x0 and 0x3.
- **802.1p-value**: Map to a 802.1p value. This also includes both P-bits and DEI/CFI. DEI is the Isb bit.

⚠️ **Caution**: Setting an odd value (DEI/CFI to 1) makes some switches drop packets.

*802.1p_value* must be a Hexadecimal number between 0x0 and 0xF.
- **mpls-tc**: Map to an MPLS traffic class.
  *mpls_tc_value* must be a Hexadecimal number between 0x0 and 0x7.
• The **internal-priority** CLI command offers the ability to configure both 802.1p priority and setting of DEI/CFI bit. This flexibility installation will treat the bit as DEI (drop eligibility indicator). However, for installations that treat the bit as CFI (canonical format indicator), this should be set to 0. Otherwise, the packet will be dropped.

**qci**

Keywords **802.1p-value** and **mpls-exp-value** have been deprecated. The values provided using these deprecated keywords will be mapped to new **internal-qos** values.

```
configure

  qci-qos-mapping name

    qci num uplink { encaps-header | internal-qos priority priority | user-datagram }
    downlink { encaps-header | internal-qos priority priority | user-datagram }

    [ default | no ] qci num

end
```

Notes:

- **internal-qos**: Set the internal QoS priority where priority is an integer from 0-7, where 7 is the highest priority and 0 is the lowest priority; these are resolved to L2 values.

**qos ip-dscp-iphb-mapping**

This new command is used to manage Internal QoS (Internal-Per-Hop-Behavior/IPHB). This specific command maps IP Differentiated Services Code Point (DSCP) values in a packet to internal-QoS class of service marking values.

```
configure

  qos ip-dscp-iphb-mapping dscp dscp_value internal-priority cos class_of_service_value

default qos ip-dscp-iphb-mapping dscp dscp_value

end
```

Notes:

- **dscp** **dscp_value**
  
  Map IP DSCP values into internal QoS.
  
  **dscp_value** must be a Hexadecimal number between 0x0 and 0x3F.

- **internal-priority cos** **class_of_service_value**
  
  Maps to the internal QoS priority/class of service.
  
  **class_of_service_value** must be a Hexadecimal number between 0x0 and 0x7.

- **default**: Map any DSCP to an IPHB value of 0.

**qos l2-mapping-table**

This new command is used to create or modify a Level 2 mapping table and enter the QoS L2 Mapping Configuration Mode to map internal QoS priority.
configure

qos l2-mapping-table { name map_table_name | system-default }

no qos l2-mapping-table name map_table_name

end

Notes:
- **name map_table_name**
  Specifies the name of an internal table from which to map QoS to L2 values.
  *map_table_name* must be an alphanumeric string of 0 through 80 characters.
- **system-default**: Configure the system default mapping.
- **no**: Deletes the specified L2 mapping table.
  The system-default table cannot be deleted. Only named tables that were previously created using this CLI command can be deleted.

Performance Indicator Changes

**show apn statistics all**

“802.1p” removed from “802.1p Priority Marking Statistics” field.

**show pgw-service statistics all**

“802.1p” removed from “802.1p Priority Marking Statistics” field.

**show qci-qos-mapping table all**

Output similar to the following is now shown for internal QoS:
- uplink: internal-qos priority 5
- downlink: internal-qos priority 3

**show qos ip-dscp-iphb-mapping**

This new command displays mapping QoS information in a packet to internal-qos marking.

**show qos l2-mapping-table name table_name**

This new command displays named table for the internal to l2 mapping values, like 802.1p and mpls.

**show qos l2-mapping-table system-default**

This new command displays system default internal mapping to l2 values, like 802.1p and mpls.

**show sgw-service statistics all**

“802.1p” removed from “802.1p Priority Marking Statistics” field.
CSCuh28410 - GTP-U UDP Bundle

Feature Changes

GTP-U UDP Bundle

Currently, for forwarding GTP-U data packets, standard UDP port (2152) as source and destination port are used for outgoing GTP-U packet. This creates hardship to balance traffic properly over the LAG interfaces between the different L2/L3 elements in the network. Some routers use source UDP port to do load balancing of packets towards destination.

As part of this feature, behavior is changed so that source port outgoing GTP-U packet is different for each SESSMGR. The destination port should remain as 2152, as per protocol.

The usage of non-standard source port number is permitted, as per section 4.4.2 of 3GPP TS 29.281. This feature does not require deviation from any GTP-U protocol aspects as defined in 3GPP TS 29.281.

A new CLI is added in GTP-U Service configuration to enable this behavior. By default, standard port 2152 is used as source port.

Customer Impact: Helps in doing effective load balancing of data traffic over LAG interfaces on some routers.

Command Changes

source-port

This new command configures GTP-U data packet source port related parameters.

configure

c ontex t context_name

gtpu-service service_name

source-port { non-standard | standard }

default source-port
end

Notes:

- **non-standard**: Configures GTP-U service to use multiple non-standard ports defined by system as a source port for GTP-U data packets. Starting port is 25500. Non-standard port number is unique per session manager instance.
- **standard**: Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.
- **default**: Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.
- By default, standard port 2152 will be configured as GTP-U data packet source port (same as existing behavior).

Performance Indicator Changes

show gtpu-service name
The following output had been added to show GTP-U source port configuration.

- GTPU Source-port Configuration

**CSCuh35139 - PGW SM sync up with driver [Phase 1]**

**Feature Changes**

**Change in Message Generation Toward Access Side**

**Previous Behavior:**
1. In case of GTP-U error indication, P-GW was sending out Delete Bearer Request and was waiting for response before doing the clean up.
2. If there was a collision between GTP messages and the older transaction got aborted, until now any PCRF rules coming in the response for that transaction were getting aborted.

**New Behavior:**
1. In case of GTP-U error indication, P-GW will align with GGSN and not send any Delete Bearer Request out. It will do the required clean up locally.
2. If there is a collision between GTP messages and the older transaction gets aborted, the old behavior will be retained if the transaction was pending at Gy/Rf when it got aborted. If, however, it was pending at PCRF, these rules will now be processed.

**Customer Impact:**
1. In case of GTP-U error indication, the message was not needed since the peer does not have that particular bearer.
2. Customer will start seeing some rules processed, in case of collision, which were not processed before.

**CSCuh85489, CSCui06202 - SR Performance: Periodic FC interval needs to be increased.**

**Feature Changes**

**Increased Periodic Full Checkpoint (FC) interval**

The Background Periodic Full Checkpoint (FC) interval (automatically triggered by the system), has been increased to 15 minutes from the earlier value of 12 minutes. This was done in order to save some CPU cycles. The applications send FC when there is a change in the status of the UE and applications also update intermediate status by sending micro checkpoints. Therefore, the background periodic full checkpoint interval has been increased.

For SR (session recovery) case, this change implies that the system automatically triggers the full check pointing to AAA Manager every 15 minutes.

For ICSR case, this change implies that the system automatically triggers Full check pointing to the standby chassis every 45 minutes instead of the earlier 36 minutes.

**Important:** This time interval is not configurable.
CSCui97899 - When CBResp times out CCR-U is not sent from PGW

Feature Changes

PCC Rule Error Handling

As per 3GPP 29212 sec 4.5.12 (PCC Rule Error Handling): If the installation/activation of one or more PCC rules fails, the PCEF shall include one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules.

Previous Behavior: When Create Bearer Response times out from ePDG side after handoff, a CCR-U should be generated from P-GW toward PCRF with Rule-Failure-Code: RESOURCE_ALLOCATION_FAILURE (10). Instead, after discarding the CBResponse, no CCR-U is generated.

New Behavior: To align with UBReq and DBReq timeout handling, when CBReq times out for dedicated bearer, P-GW will tear down the complete call and send CCR-T to PCRF.

Customer Impact: PCRF did not have any knowledge about the state of dynamic rules which were to be installed for the session.

CSCuj35808, CSCuh85803 - Implement TFT lookup for downlink packets in SMGR

Performance Indicator Changes

show subscribers tft

The following output is now available to display TFT for P-GW.

- username
- callid
- msid
- traffic flow template
- filter id
- direction
- eval prec
- components
- filter id
- direction
- eval prec
- components
- filter id
- direction
• eval prec
• components
• filter id
• direction
• eval prec
• components
• Total tfts matching specified criteria

**show subscribers pgw-only full all**

The following output is now available to display TFT for P-GW:

• traffic flow template
• filter id
• direction
• eval prec
• components
• filter id
• direction
• eval prec
• components
• filter id
• direction
• eval prec
• components

**CSCuj74636 - Discrepancy in pgw-service stats between active and standby chassis**

**Feature Changes**

**P-GW/GGSN Service and APN Bulk Statistics**

P-GW/GGSN service and APN bulk statistics counters not incremented on standby box.
**Previous Behavior:** Previously, active and setup counters were incremented on standby box for P-GW/GGSN service statistics while they should be incremented only on active box. Similarly, active setup and release counters were incremented on standby box for P-GW/GGSN APN statistics and these incremented counters were sent in bulk statistics.

**New Behavior:** Setup and release counters are no longer incremented on standby box for P-GW/GGSN service statistics and P-GW/GGSN APN statistics; these will be incremented only when the box becomes active. Active counts are incremented on standby box, but in bulk statistics active counters are sent as 0 (zero), while setup and release count may be non zero.

For bulk statistics, setup and release counters will reflect counts when this box was last in active state.

**Customer Impact:** Earlier, for single call customer was counted double if they sum up both active and standby statistics. Now, counters are incremented on only one box, which is current active so they will get correct counters value.

This change is applicable only for P-GW and GGSN service.

**Performance Indicator Changes**

**show apn statistics all**

Counters not incremented on standby box.

**show pgw service statistics**

Counters not incremented on standby box.

**CSCul61774 - SM-IPNE auto-association for Gn/Gp setup**

**Feature Changes**

**IPNE Auto Association for Gn/Gp Setup**

**Previous Behavior:** IPNE service was independently associated with GGSN and P-GW.

**New Behavior:** For Gn/Gp setup, whenever IPNE is associated with GGSN, it will be auto-associated with P-GW. In the same way, if associating with P-GW, it will auto-associate with GGSN.

Auto-disassociation will take place similarly. The disassociation between GGSN and P-GW services won't have any effect over IPNE's association with GGSN or P-GW service.

**Customer Impact:** For Gn/Gp setup, if IPNE is associated with GGSN, then 4G calls will also get bound with IPNE. If associated with P-GW, IPNE will also support the 3G calls.

**CSCul72349 - PGW LORC mechanism for subscriber billing**

**Feature Changes**

**Overcharging Protection**
Previous Behavior: Overcharging Protection feature supported only at P-GW service.

New Behavior: Overcharging Protection feature 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.

Command Changes

egtp

The new command `egtp overcharge-protection` has been added to enable/disable the Overcharging Protection feature on an APN service.

```
configure

case context context_name

    apn apn_name

        egtp overcharge-protection [ drop-all | transmit-all ]

        { default | no | remove } egtp overcharge-protection

end
```

Notes:

- `drop-all`: Configures overcharging protection to drop all packets received in LORC.
- `transmit-all`: Configures overcharging protection to send all packets received in LORC mode to S-GW.
- `default`: Disables overcharging protection.
- `no`: Disables overcharging protection.
- `remove`: Removes overcharging protection configuration.
- Use of Overcharging Protection feature requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.
- When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

egtp

Two options have been added to the `overcharge-protection` keyword.

```
configure

    context context_name

    pgw-service service_name

        egtp overcharge-protection [ drop-all | transmit-all ]

        { default | no } egtp overcharge-protection
```
Notes:

- **drop-all**: Configures overcharging protection to drop all packets received.
- **transmit-all**: Configures overcharging protection to send all packets received.
- **default**: Disables overcharging protection.
- **no**: Disables overcharging protection.
- Use of Overcharging Protection feature requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Performance Indicator Changes

**show pgw-service name**

The following output fields have been added to show the status of Overcharging Protection.
- Overcharge Protection
- Drop Policy

CSCul93145 - Enhance the 'no ignore-alt-config' CLI with 'no-dns' and 'no-s6b' option

Feature Changes

'no ignore-alt-config' CLI Enhanced

**Previous Behavior**: no ignore-alt-config disabled both ignore-alt-config no-dns and ignore-alt-config no-s6b.

**New Behavior**: no ignore-alt-config no-dns shall disable ignore-alt-config no-dns only, if enabled.
no ignore-alt-config no-s6b shall disable ignore-alt-config no-s6b only, if enabled.

**Customer Impact**: no ignore-alt-config will be an incomplete syntax of CLI.

Command Changes

ignore-alt-config

This new command enables/disables DNS server address preference or S6b authentication on a per-APN level.

```
configure

   context context_name
    apn apn_name

      [ no ] ignore-alt-config { no-dns | no-s6b }
```
Notes:
- `no`: Disables DNS server address preference or S6b authentication on a per-APN level.
- `no-dns`: Gives preference to DNS server address configured in APN. If name server addresses is not found in APN configuration, it will not be provisioned from SGi context, even if it is configured there.
- `no-s6b`: Ignores alternate service-level configuration for S6b authorization when S6b authorization is disabled at APN.

Performance Indicator Changes

**show apn name**

The following keyword has been added to the output to display whether DNS server address preference or S6b authentication is enabled or disabled on a specified APN.

- `ignore-alt-config (no-dns)`
- `ignore-alt-config (no-s6b)`

**CSCuI93209 - Need show config errors to point inconsistencies in qos configuration**

Performance Indicator Changes

**show configuration errors**

The following keyword has been added to the output of the show configuration errors command to display new errors and warnings related to inconsistencies in QoS configuration.

<table>
<thead>
<tr>
<th><strong>Important:</strong> This new keyword is only available in the verbose option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qos-marking verbose</code></td>
</tr>
</tbody>
</table>

**CSCum09122 - Selectively disable S6b authentication for LTE users**

Feature Changes

**Selectively Disable S6b Authentication**

**Previous Behavior:** Initially, unable to selectively enable or disable the S6b-Authorization based on the interface type.

**New Behavior:** Added flexibility by giving interface-specific options in `authorize-with-hss` CLI.
Command Changes

authorize-with-hss

Interface-specific options added.

configure

custom context context_name

apn apn_name

authorize-with-hss [ egtp [ s2b ] [ s5-s8 ] [ report-ipv6-addr ] ] lma [ s6b-aaa-group aaa-group | report-ipv6-addr ]

[ default | no ] authorize-with-hss

end

Notes:

• s2b: Enables S6b authorization for eGTP S2b.
• s5-s8: Enables S6b authorization for eGTP S5S8
• s6b-aaa-group: AAA group for S6b authorization.
• aaa-group must be an existing AAA group expressed as an alphanumeric string of 1 through 63 characters.

authorize-with-hss

Interface-specific options added.

configure

custom context context_name

pgw-service pgw_service

authorize-with-hss [ egtp [ s2b ] [ s5-s8 ] [ report-ipv6-addr ] ] lma [ s6b-aaa-group aaa-group | report-ipv6-addr ]

[ default | no ] authorize-with-hss

end

Notes:

• s2b: Enables S6b authorization for eGTP S2b.
• s5-s8: Enables S6b authorization for eGTP S5S8
• s6b-aaa-group: AAA group for S6b authorization.
• aaa-group must be an existing AAA group expressed as an alphanumeric string of 1 through 63 characters.
CSCum14805 - show gtpu stats cli change for volte

Performance Indicator Changes

show gtpu statistics

The following output has been added to show VoLTE-specific statistics.

- Current (IMS-media)
- Total Setup (IMS-media)
- Uplink Packets (IMS-media)
- Uplink Bytes (IMS-media)
- Downlink Packets (IMS-media)
- Downlink Bytes (IMS-media)
- Packets Discarded (IMS-media)
- Bytes Discarded (IMS-media)

CSCum15133 - Def Bearer Rejected stats under APN level is inconsistent for HO cases

Feature Changes

Default Bearer Rejected Statistics

The behavior of the “Default Bearer Rejected” statistics under APN level is inconsistent for HO scenarios. This statistic is incremented for LTE to WiFi, eHRPD to WiFi, WiFi to LTE, eHRPD to LTE handover when Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch, etc., but not incremented for other error scenarios.

**Previous Behavior:** “Default bearers rejected” statistics under APN level under CLI show apn statistics:

- Incremented - For the plain vanilla new call for P-GW and GGSN if the Default Bearer is rejected.
- Incremented - For eHRPD to LTE, eHRPD to WiFi, WiFi to LTE, and LTE to WiFi - When Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch.
- Not Incremented - For GnGp handoff, LTE to eHRPD. WiFi to eHRPD, eHRPD to WiFi, eHRPD to LTE, LTE to WiFi, and WiFi to LTE.

**New Behavior:** “Default bearers rejected” statistics under APN level under CLI show apn statistics:

- Increment - For the plain vanilla new call for P-GW and GGSN if the Default Bearer is rejected.
- Do NOT Increment - For eHRPD to LTE, eHRPD to WiFi, WiFi to LTE, and LTE to WiFi - When Mandatory IE IMSI missing, Unauthenticated IMSI, Invalid QCI, PDP type mismatch.
- Do NOT Increment - For GnGp handoff, LTE to eHRPD. WiFi to eHRPD, eHRPD to WiFi, eHRPD to LTE, LTE to WiFi, and WiFi to LTE.
CSCum36827 - Further stats to be implemented for Newcall rejection feature, MFL ID: 577

Feature Changes

New Call Reject Policy Statistics

Support added to display new call reject policy statistics.

Previous Behavior: New call policy reject statistics were not included in show egtpc statistics CLI output.

New Behavior: Added support to display new call reject policy statistics in show egtpc statistics verbose CLI.

Performance Indicator Changes

show egtpc statistics verbose

The following miscellaneous eGTPC output has been added to show new call policy rejection statistics.

- Misc Statistics
- Newcall policy rejection statistics
- NewCall Service Reject
- NewCall APN Reject

CSCum57855 - PGW: Segmentation fault @ acsmgr_match_dyn_rule

Performance Indicator Changes

show srp checkpoint statistics

New counter for ECS internal audit failure is added under “Total CRR recovery failures” to show the number of failures while recovering.

- call-recovery-acs-internal-audit-failure

CSCum82051 - Call not up when 802.P is set to odd value in l2-mapping-table

Feature Changes

Change in Help Text for CLI

The help text for the CLI command “qos l2-mapping name <l2-mapping name> internal-priority cos 0x<0..f> color 0x<0..3> 802.1p-value 0x<0..f>” has been changed as follows:
**Previous Behavior:** Earlier the help text read as: “map to a 802.1p value. This also includes both p-bits and DEI/CFI. DEI is the lsb bit.”

**New Behavior:** The new help text now read as: “map to a 802.1p value. This also includes both p-bits and DEI/CFI. DEI is the lsb bit. Caution: Setting an odd value (DEI/CFI to 1) makes some switches to drop packets.”

**Customer Impact:** None

**CSCum85474 - Wrong data type for Bearer reject bulkstat variable (rejbearer)**

**Performance Indicator Changes**

**APN Schema**

The following statistics changed to Int32 from Int64.

- qci1-actbear
- qci1-setupbear
- qci1-relbear
- qci2-actbear
- qci2-setupbear
- qci2-relbear
- qci3-actbear
- qci3-setupbear
- qci3-relbear
- qci4-actbear
- qci4-setupbear
- qci4-relbear
- qci5-actbear
- qci5-setupbear
- qci5-relbear
- qci6-actbear
- qci6-setupbear
- qci6-relbear
- qci7-actbear
- qci7-setupbear
- qci7-relbear
- qci8-actbear
- qci8-setupbear
- qci8-relbear
CSCum96954 - Emergency inactivity timeout starting for Non-GBR ded bearer deletion

Feature Changes

When to Start “Emergency inactivity timer”

**Previous Behavior:** Emergency inactivity timer gets started upon deletion of Non-GBR dedicated bearer.

**New Behavior:** Emergency inactivity timer only gets started upon deletion of last GBR dedicated bearer.

CSCun06154 - disabled ‘srp-activate’ for non-loopback type interfaces

Feature Changes

Disabled ‘srp-activate’ for Non-loopback Type Interfaces

srp-activate keyword for non-loopback interfaces is no longer supported.

**Previous Behavior:** srp-activate allowed for physical interfaces.

**New Behavior:** srp-activate no longer supported for physical interfaces.

CSCun14620 - PGW sends PBA with wrong checksum in MH

Performance Indicator Changes

LMA Schema

The following bulk statistic had been added to track the total number of LMA heartbeat checksum errors received:

- rxhbcchecksumerror

CSCun63020 - SPGW racing condition between DBREQ and MME MBREQ

Feature Changes

SPGW Racing Condition Between DBREQ and MME MBREQ
**Previous Behavior:** If delete bearer request is pending at P-GW and if modify bearer request is received, then modify bearer request is rejected.

**New Behavior:** Now, as soon as modify bearer request is received, delete bearer response is generated internally, then modify bearer request is processed for remaining bearers. If all the bearers are pending in delete state or bearer in delete bearer pending state is default bearer, then modify request is rejected.
Chapter 19
QvPC-SI Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from QvPC-SI in StarOS 16 software releases.
QvPC-SI Enhancements for 16.1

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 *QvPC-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:** 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 QvPC-SI.

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

---

**CSCup10277 - Change session count redefining SSI-medium SSI-Large**

**Feature Changes**

**Performance Improvements**

Configuration testing and code changes have improved QvPC-SI performance and throughput. The results are summarized below:

- Updates to recommended VMware and Ubuntu/KVM configurations.
- Tuning of interfaces to improve throughput without dropping packets.
- Support for KVM multiqueue.
- Expanded session counts for recommended vCPU/vRAM configurations
- Efficient use of multiple tx queues in vmxnet
For additional information, refer to the *Operator Notes* chapter.
QvPC-SI Enhancements for 16.0

This section identifies all of the QvPC-SI enhancements included in this release:

**Feature Changes** – new or modified features or behavior changes. For details, refer to the *QvPC-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:** 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 QvPC-SI.

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

### CSCui20002 – SSI knpusim

#### Feature Changes

**Fastpath NPU Simulator**

To improve overall performance, the user space npusim (NPU simulator) process for packet processing is now supplemented by a new kernel space knpusim process.

**Previous Behavior:** Packet processing was performed exclusively by npusim which required a buffer copy and transmit to the loopback interface. This required additional buffer copies and loopback transmits to transfer packets between user space processes (slowpath processing).

**New Behavior:** The knpusim process is a kernel loadable Linux module. It processes internally transferred socket buffers that do not require copying (fastpath processing). Packets that cannot be fully dispositioned by knpusim are sent to the user space npusim process.
There are no user-visible changes to the StarOS CLI associated with this feature change.

Customer Impact: Improved performance and throughput
Chapter 20
SAEGW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from the SAEGW in StarOS 16 software releases.
SAEGW Enhancements for Release 16.5

There are no SAEGW enhancements for this release.
SAEGW Enhancements for Release 16.4

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 *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**

**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

Command Changes

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-s2bgtpolteatt
• pgw-handoverstat-s2bgtpoltesucc
• pgw-handoverstat-s2bgtpolfail
• pgw-handoverstat-ltetos2bgtpatt
• pgw-handoverstat-ltetos2bgtpsucc
• pgw-handoverstat-ltetos2bgtfail

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 16.3

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

CSCuo82399 - Collision counter support in GTP layer

Applicable Products: SAEGW

Feature Changes

Collision Counter Support in GTP Layer

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The SAEGW software has been enhanced so that these collisions are now handled based on a pre-defined action for each message collision type.

Performance Indicator Changes

show egtpc statistics verbose
The output of this command has been enhanced to provide information on GTPv2 message collisions, including:

- **Interface**: The interface on which the collision occurred: PGW (S5) or SGW (S4/S11).
- **Old Proc (Msg Type)**: The old procedure message and message type
- **New Proc (Msg Type)**: The new procedure and message type
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - **Abort Old**: Aborts the original (old) message handling and processes the new message.
  - **Reject New**: The new message cannot be processed, so the original (old) message is processed.
  - **Parallel Hndl**: Both the original (old) and new message are handled in parallel.
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
- **Counter**: The number of times each collision type has occurred.

**Table 1. Message Collision Statistics for show egtpc statistics verbose Command**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Old Proc (Msg Type)</th>
<th>New Proc (Msg Type)</th>
<th>Action</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGW</td>
<td>NW Init Bearer Create (95)</td>
<td>Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Create (95)</td>
<td>Non-Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Create (95)</td>
<td>Non-Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Update (97)</td>
<td>Non-Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Update (97)</td>
<td>Non-Handover MBReq (34)</td>
<td>Suspend Old n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Update (97)</td>
<td>Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Delete (99)</td>
<td>Non-Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>PGW</td>
<td>NW Init Bearer Delete (99)</td>
<td>Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Create (95)</td>
<td>Non-Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Create (95)</td>
<td>Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Create (95)</td>
<td>RAB (170)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Create (95)</td>
<td>Non-Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Update (97)</td>
<td>Non-Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Update (97)</td>
<td>RAB (170)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Update (97)</td>
<td>Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Delete (99)</td>
<td>Non-Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Delete (99)</td>
<td>Handover MBReq (34)</td>
<td>Parallel Hndl n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer Delete (99)</td>
<td>RAB (170)</td>
<td>Reject New n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer PDN Delete (99)</td>
<td>Non-Handover MBReq (34)</td>
<td>Reject New n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer PDN Delete (99)</td>
<td>Handover MBReq (34)</td>
<td>Reject New n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Init Bearer PDN Delete (99)</td>
<td>RAB (170)</td>
<td>Reject New n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Trgr Service Req (176)</td>
<td>Non-Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Trgr Service Req (176)</td>
<td>Handover MBReq (34)</td>
<td>Abort Old n</td>
<td></td>
</tr>
<tr>
<td>SGW (S4/S11)</td>
<td>NW Trgr Service Req (176)</td>
<td>RAB (170)</td>
<td>Abort Old n</td>
<td></td>
</tr>
</tbody>
</table>
SAEGW Enhancements for 16.2

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

**CSCun86828 - CBR - MBR collision causing MME to delete dedicated bearer**

**Applicable Products:** SAEGW

**Feature Changes**

**Modification to MBR Collision Procedure**

When the S5/S8 interface detected a collision between an already initiated Create Bearer Request and a 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.

**Previous Behavior:** Create Bearer Request is 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 will be re-transmitted after the Modify Bearer Response.

CSCup67356 - Rule failure counters not incremented

Applicable Products: SAEGW

Feature Changes

Modification to Rule Failure Counters

The fix to CSCup67356 has resulted in a behavior change:

Previous Behavior: In the CLI command `show active-charging service statistics`, the ACS reject reason for no active rule was not being shown.

New Behavior: The CLI command `show active-charging service statistics` shows the number of calls rejected due to no active rule.

CSCuq10038 - NEMO support on SAEGW license request

Applicable Products: SAEGW

Feature Changes

NEMO License Support for SAEGW

An additional customer-specific license for the Network Mobility (NEMO) feature is now available for the SAEGW. When enabled through a feature license key, the SAEGW includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application agnostic between users behind the MR and users or resources on Fixed Network sites. The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

CSCuq25059 - Assertion failure at sess/smgr/sessmgr_ggsn.c:25058

Applicable Products: SAEGW

Feature Changes

Behavior Change to QCI Assigned to Traffic Class

The fix implemented for CSCuq25059 has resulted in a behavior change.

Previous Behavior: A traffic type other than 1,2,3,4 in the 'Create PDP Req' message would result in a crash at the GGSN.
**New Behavior:** If an unknown traffic type (that is, other than 1,2,3,4) is passed to the GGSN it will be mapped to a QCI corresponding to background class and will not result in a crash.
SAEGW Enhancements for 16.1

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

---

**CSCuj89567 - show sub subsystem stats incorrect**

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

**Feature Changes**

**Enhancement to SAEGW for RAT-Based Counters**

The SAEGW software has been enhanced to provide counters for the active PDNs based on RAT type. Counters have also been added to track successful, attempted, and failed counters for LTE to S4-SGSN, S4-SGSN to LTE, GNGP to S4-SGSN and S4-SGSN to GNGP handovers.

**Performance Indicator Changes**

**P-GW Schema**
The following bulk statistics have been added to the P-GW schema to support the enhancement to show subscriber subsystem statistics:

- `sesstat-pdn-rat-eutran`
- `sesstat-pdn-rat-utran`
- `sesstat-pdn-rat-geran`
- `sesstat-pdn-rat-wlan`
- `sesstat-pdn-rat-other`
- `handoverstat-gngptos4sgsnsucc`
- `handoverstat-gngptos4sgsnfail`
- `handoverstat-gngptos4sgsnatt`
- `handoverstat-s4sgstogngpnsucc`
- `handoverstat-s4sgntogngpnsucc`
- `handoverstat-s4sgntogngpfail`
- `handoverstat-s4sgntogngpatt`
- `handoverstat-ltetos4sgsnsucc`
- `handoverstat-ltetos4sgsnfail`
- `handoverstat-ltetos4sgsnatt`
- `handoverstat-s4sgntolteatt`
- `handoverstat-s4sgntoltesucc`
- `handoverstat-s4sgntoltefail`

**SAEGW Schema**

The following bulk statistics have been added to the SAEGW schema to support the enhancement to show subscriber subsystem statistics:

- `saegw-collapsed-pdn-rat-eutran`
- `saegw-pgw-anchor-pdn-rat-eutran`
- `pgw-sesstat-pdn-rat-eutran`
- `saegw-sgw-anchor-pdn-rat-eutran`
- `saegw-collapsed-pdn-rat-utran`
- `saegw-pgw-anchor-pdn-rat-utran`
- `pgw-sesstat-pdn-rat-utran`
- `saegw-sgw-anchor-pdn-rat-utran`
- `saegw-ggsn-pdn-rat-utran`
- `saegw-collapsed-pdn-rat-geran`
- `saegw-pgw-anchor-pdn-rat-geran`
- `pgw-sesstat-pdn-rat-geran`
- saegw-sgw-anchor-pdn-rat-geran
- saegw-ggsn-pdn-rat-geran
- saegw-pgw-anchor-pdn-rat-wlan
- pgw-sesstat-pdn-rat-wlan
- saegw-ggsn-pdn-rat-wlan
- saegw-collapsed-pdn-rat-other
- saegw-pgw-anchor-pdn-rat-other
- pgw-sesstat-pdn-rat-other
- saegw-sgw-anchor-pdn-rat-other
- saegw-ggsn-pdn-rat-other
- pgw-handoverstat-gngptos4sgnsucc
- pgw-handoverstat-gngptos4sgsnfail
- pgw-handoverstat-gngptos4sgsnatt
- pgw-handoverstat-s4sgsntogngpsucc
- pgw-handoverstat-s4sgsntogngpfail
- pgw-handoverstat-s4sgntogngpatt
- pgw-handoverstat-ltetos4sgnsucc
- pgw-handoverstat-ltetos4sgsnfail
- pgw-handoverstat-ltetos4sgsnatt
- pgw-handoverstat-s4sgsntolteatt
- pgw-handoverstat-s4sgsntoltesucc
- pgw-handoverstat-s4sgsntoltefail

**show subscriber summary saegw-only/show subscriber summary pgw only**

The output of this command has been enhanced to track 4G, 3G, 2G and Other PDN counters.

- Total PDNs by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - WLAN
  - OTHER

**show saegw-service statistics all / show saegw-service statistics name**

The output of this command has been enhanced to track various handover statistics between network elements based on RAT type.

- Current PDNs By RAT-Type and Operational Mode
Colocated PDNs
- EUTRAN
- UTRAN
- GERAN
- WLAN
- OTHER

PGW-Anchor PDNs
- EUTRAN
- UTRAN
- GERAN
- WLAN
- OTHER

SGW-Anchor PDNs
- EUTRAN
- UTRAN
- GERAN
- OTHER

GGSN-Anchor PDNs
- UTRAN
- GERAN
- WLAN
- OTHER

**show saegw-service statistics name function pgw verbose**

The output of this command has been enhanced to track handover stats between S4-SGSN and LTE, Gn/Gp SGSN and S4-SGSN, LTE to S4-SGSN and S4-SGSN to Gn/Gp SGSN.

- Handover Statistics
  - GNGP-to-S4SGSN Handover
    - Attempted
    - Succeeded
    - Failed
  - S4SGSN-to-GNGP handover
    - Attempted
    - Succeeded
    - Failed
• S4SGSN-to-LTE handover
  • Attempted
  • Failed
  • Succeeded
• LTE-to-S4SGSN handover
  • Attempted
  • Succeeded
  • Failed

show pgw service statistics all / show pgw-service statistics name

The output of this command has been enhanced to track PDN counts based on RAT type.
  • Current PDNs by RAT-Type
    • EUTRAN
    • UTRAN
    • GERAN
    • WLAN
    • Other

show pgw-service statistics all / show pgw-service statistics name

The output of these commands has been enhanced to track handover statistics between the S4-SGSN and LTE, Gn/Gp SGSN and S4-SGSN, LTE to S4-SGSN and S4-SGSN to Gn/Gp SGSN.
  • Inter Technology handover
    • GNGP-to-S4SGSN handover
      • Attempted
      • Succeeded
      • Failed
    • S4SGSN-to-GNGP handover
      • Attempted
      • Succeeded
      • Failed
    • S4SGSN-to-LTE handover
      • Attempted
      • Succeeded
      • Failed
    • LTE-to-S4SGSN handover
      • Attempted
- Succeeded
- Failed

CSCun35216 - S4 to Gn SGSN HO, CCR-u shows RAT type event for UTRAN

Applicable Products: SAEGW, PGW

Feature Changes

Correction to Incorrect RAT Type Event Being Logged

The fix for CSCun35216 has introduced a behavior change.

Previous Behavior: During a S4-SGSN to GGSN handover, a RAT change was being detected when there was no RAT change.

New Behavior: The SAEGW now does not incorrectly detect a RAT change during a S4-SGSN to GGSN handover when no RAT change occurred.

CSCun84742 - S6b Assume positive counter is missing for the Current Subs in system

Applicable Products: SAEGW

Feature Changes

Statistics added for S6b Assume Positive State for Subscribers

AAA diameter authentication can be configured to assume the subscriber as valid for certain AAR error response codes and by-pass the S6b interface from then on. Counters have been introduced on the SAEGW to display the total number of subscribers which are in S6b by-passed state (also called “assumed positive”).

Performance Indicator Changes

SAEGW Schema

The following bulk statistic has been added to display the total number of subscribers in the assumed positive state.

- pgw-ue-s6b-assume-positive

GTPC Schema

The following bulk statistic has been added to display the total number of subscribers in the assumed positive state.

- setup-ggsn-s6b-assume-positive

show gtpc statistics
The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Session Stats:
  - S6b Assume Positive:

**show subscribers sagew-only summary**

The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Total S6b Assume Positive:

**show saegw-service statistics all**

The output of this command has been enhanced to display the total number of subscribers in the assumed positive state.

- Subscriber Total
  - Total S6b Assume Positive:

### CSCun86828 - CBR - MBR collision causing MME to delete dedicated bearer

#### Feature Changes

**CBR and MBR Collision Detection for Dedicated Bearers**

The software has been enhanced to avoid aborting the existing Create Bearer Request. The Create Bearer Request procedure is buffered until the time Modify Bearer Request procedure is over. The Create Bearer Response received will be handled only after the Modify Bearer Request procedure is over.

**Previous Behavior:** On ASR 5000 P-GW-SAEGW nodes, when the S5/S8 interface detected a collision between an already initiated Create Bearer Request and a new 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/S-GW to be rejected. As a result, the SAEGW/P-GW had one bearer less than the peer.

**New Behavior:** On ASR5000 P-GW-SAEGW nodes, when the S5/S8 interface detects a collision between an already initiated Create Bearer Request and a new incoming Modify Bearer Request, the Create Bearer Request is not aborted at P-GW. The Create Bearer Request procedure is buffered until the time Modify Bearer Request procedure is over. Create Bearer Response received will be handled only after the Modify Bearer Request procedure is over. Normal T3/N3 Timer expiry behavior will continue for Create Bearer Request.
SAEGW Enhancements for 16.0

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

CSCua99366, CSCui04214 - Dedicated bearer timeout action

**Feature Changes**

Dedicated Bearer Timeout Support on the S-GW

> **Important:** For this release, this feature is Lab/Trial Quality only.

The SAE-GW has been enhanced to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value.

**Previous Behavior:** Earlier only one timer was available for any kind of bearer.

**New Behavior:** Different timer values provide configuration options for GBR and non GBR types of bearers for bearer inactivity
Customer Impact: Operators now can configure a bearer inactivity timeout for GBR and non-GBR bearers for more efficient use of system resources.

Command Changes

timeout bearer-inactivity

The new command timeout bearer-inactivity supports a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions.

configure

    apn-profile apn_profile_name

        timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { total bytes | uplink bytes | downlink bytes } | exclude-default-bearer

    remove timeout bearer-inacativity [ gbr | non-gbr ]

end

Notes:

- **timeout**: Specifies that a session time out value will be configured for this APN profile.
- **bearer-inactivity**: Specifies that the system will check for low activity for a bearer.
- **gbr**: Specifies that the system will check for low activity on a GBR bearer.
- **non-gbr**: Specifies that the system will check for low activity on a non-GBR bearer.
- **dur_seconds**: Specifies the timeout for the gbr or non-bgr bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).
- **volume-threshold**: Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.
- **total**: Specifies that the total of both uplink and downlink data will be used as a volume threshold. bytes must be a value from 1 to 4294967295.
- **uplink**: Specifies that an uplink data volume threshold will be used. bytes must be a value from 1 to 4294967295.
- **downlink**: Specifies that a downlink data volume threshold will be used. bytes must be a value from 1 to 4294967295.
- **exclude-default-bearer**: Specifies that inactivity handling for the default bearer will be excluded.

Performance Indicator Changes

show apn-profile full name

This command has been enhanced to list bearer inactivity timeout settings, if configured.

- Bearer inactivity timeout:
- Exclude default bearer : Yes/No
• GBR:
  • Timeout (Seconds) :seconds
  • Threshold (Bytes) :bytes
  • Direction :Downlink/Uplink/Bi-directional

• non-GBR:
  • Timeout (Seconds) :seconds
  • Threshold (Bytes) :bytes
  • Direction :Downlink/Uplink/Bi-directional

**show sgw-service-statistics all verbose**

This command has been enhanced to list bearer inactivity timeout settings, if configured.

• Inactivity timeout:
  • QCI 1: :seconds
  • QCI 2: :seconds
  • QCI 3: :seconds
  • QCI 4: :seconds
  • QCI 5: :seconds
  • QCI 6: :seconds
  • QCI 7: :seconds
  • QCI 8: :seconds
  • QC9 1: :seconds
  • Non-Std QCI: :seconds

**CSCuh13691 - R11 compliance on standard interfaces**

**Feature Changes**

**3GPP Release 11 Compliance on Standard Interfaces on the SAE-GW**

The SAE-GW is now compliant with the following 3GPP Release 11 standards for standard interfaces:

• S-GW:
  • 3GPP TS 23.007
  • 3GPP TS 23.401
  • 3GPP TS 29.274

• P-GW:
  • 3GPP TS 23.007
**CSCuh13694 - ECS Cookie Match support for Websockets**

**Feature Changes**

**ECS Cookie Match Support for Websockets on the SAE-GW**

❗️ **Important**: For this release, this feature is Lab/Trial Quality only.

The SAE-GW can now detect the websocket protocol. This helps in identifying an initial TCP connection for websocket and rate it in certain way. With enabling/disabling the new CLI command `websocket flow-detection http` operators can enable/disable websocket protocol identification.

---

**CSCuh13699 - CDR LIFO**

**Feature Changes**

**Parallel Streaming of CDRs on the SAE-GW**

Once CDRs get buffered to local disk the system then performs a FIFO to transfer CDRs to OCG. So new CDRs continue to buffer even though OCG connectivity is restored until all CDRs are off the disk. To prevent this from happening, the system has been enhanced to allow parallel streaming of the CDRs.

**Previous Behavior**: In the old FIFO mode, when the CGF becomes active, all CDRs in HDD are streamed in a First-In-First-Out order. Any new CDR generated during the streaming (that is, until all CDRs are flushed from the HDD) will be written to HDD and from there sent to CGF.

**New Behavior**: In the new PARALLEL mode, when the CGF becomes active, CDRs in HDD are streamed at a slower pace. Newly generated CDRs from AAAMgrs are sent directly to CGF servers. In parallel mode, rate of streaming from HDD will be reduced. The maximum requests that can be streamed from HDD will be either set to 1 OR 25 percent of available bandwidth (max outstanding / outstanding req) if it's greater than 1.

---

**CSCuh25810 - SGW Session Idle Timer**

**Feature Changes**

**S-GW Session Idle Timer**

A session idle timer has been implemented on the S-GW to remove stale session in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will
tear down those sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

**Important:** The session idle timer feature will not work if the Fast Data Path feature is enabled.

### Command Changes

**timeout idle**

This new command has been added to *SGW Service Configuration Mode* to tear down SGW sessions that remain idle for longer than the configured time limit.

```plaintext
configure
  context context_name
    sgw-service sgw_service_name
      timeout idle dur_seconds
      no timeout idle
      default timeout idle
end
```

**Notes:**

- `idle dur_seconds` specifies the time limit, in seconds, after which the SGW session will be torn down. Valid entries are from 0 to 4294967295.
- `no` disables the SGW session idle timer.
- `default` returns the SGW session idle timer to the default value of 0 (disabled).

### Performance Indicator Changes

**show sgw-service name**

This command has been enhanced to indicate if the Session Idle Timer feature is enabled on the S-GW.

- Idle timeout: 0...n secs/(n/a)

**show sgw-service statistics all**

This command has been enhanced to indicate if the Session Idle Timer feature is enabled on the S-GW:

- Released:
  - Idle timeout : 0...n secs
  - Idle timeout : (n/a)
CSCuj01136 - SAEGW : pdn-count is not working for multi APN scenario

Command Changes

condition

The following variables at Local Policy are no longer used and have been deprecated in this release:

- cgi
- ecgi
- sai
- tai
- timer

CSCui21603 - SGW Honor ingress & egress DSCP & Support DSCP marking @ APN profile

Feature Changes

Support for Honoring DSCP Ingress and Egress and DSCP Marking at the APN Profile

This feature will provide an operator with a configuration to set the DSCP value per APN profile, so different APNs can have different DSCP markings as per QOS requirements for traffic carried by the APN. In addition, the qci-qos mapping table is updated with the addition of a copy-outer for copying the DSCP value coming in the encapsulation header from the S1u interface to the S5 interface and vice-versa.

Previous Behavior:
1. The (qci-qos mapping) table was previously fetched from service.
2. The DSCP value in the encapsulated header was not getting relayed from s1-s5 and vice versa. Instead, a value of 0 (zero) was sent in the encapsulation header.

New Behavior:
1. The (qci-qos-mapping) table will be fetched from the APN profile first. If there is no association in the apn-profile for the qci-qos-mapping table then the service level configuration will be fetched for the qci-qos mapping table.
2. The DSCP value in the encapsulated header will be relayed from s1-s5 and vice versa using the copy-outer option in the qci-qos-mapping table.

Command Changes

associate qci-qos-mapping

The qci-qos-mapping keyword has been added to the associate command in APN Profile Configuration Mode to associate a QCI QOS mapping table with an APN profile.
configure

apn-profile apn_profile_name
associate qci-qos-mapping mapping_table_name
remove associate qci-qos-mapping
end

Notes:
- mapping_table_name is the name of the QCI QOS mapping table that you want to associate with this APN profile.
- remove specifies that the association to the QCI QOS mapping table is to be deleted.

qci

The copy-outer keyword has been added to the qci command in Global Configuration Mode. Enabling this feature for copying the DSCP value coming in a data packet from S1u to the data packet sent on the S5 interface and vice-versa.

configure

qci-qos-mapping mapping_table_name
qci number downlink encaps-header copy-outer
qci number uplink encaps-header copy-outer
end

Notes:
- copy-outer instructs the S-GW to copy the DSCP value coming in an encapsulation header from the S1u interface to the encapsulation header sent on the S5 interface and vice-versa.

Performance Indicator Changes

show qci-qos mapping table name

The output of this command has been enhanced to indicate if the copy-outer option is enabled for uplink and downlink in the QCI QOS table.
- uplink: user-datagram dscp-marking xxxx encaps-header copy-outer
- downlink: user-datagram dscp-marking xxxx encaps-header copy-outer

show apn-profile full all

The output of this command has been enhanced to indicate if a QCI QOS mapping table is associated with a given APN profile configuration.
- APN Profile Name
  - QCI-QOS mapping table :<QCI QOS table name>
CSCui21610 - Dropped call counters granularity

Feature Changes

Increased Granularity for Bearer Released Reason and Drop Type

The system has been enhanced to provide more detailed and granular output to report the reasons for dropped calls, specifically for IMS dropped calls/bearer/Qos Class Identifier (QCI).

**Customer Impact:** More granular reporting of dropped calls/bearers counters is supported. This feature is especially useful for troubleshooting and tracking VoLTE field performance.

Performance Indicator Changes

S-GW Schema

The following bulkstats have been added to the S-GW schema to support increased granularity for bearer released reason and drop type.

- sgw-totepsbearrel-dedrsn-pgw
  - sgw-totepsbearrel-dedrsn-pgw-qci1
  - sgw-totepsbearrel-dedrsn-pgw-qci2
  - sgw-totepsbearrel-dedrsn-pgw-qci3
  - sgw-totepsbearrel-dedrsn-pgw-qci4
  - sgw-totepsbearrel-dedrsn-pgw-qci5
  - sgw-totepsbearrel-dedrsn-pgw-qci6
  - sgw-totepsbearrel-dedrsn-pgw-qci7
  - sgw-totepsbearrel-dedrsn-pgw-qci8
  - sgw-totepsbearrel-dedrsn-pgw-qci9
  - sgw-totepsbearrel-dedrsn-pgw-other
- sgw-totepsbearrel-dedrsn-pcrf
  - sgw-totepsbearrel-dedrsn-s1err
  - sgw-totepsbearrel-dedrsn-s1err-qci1
  - sgw-totepsbearrel-dedrsn-s1err-qci2
  - sgw-totepsbearrel-dedrsn-s1err-qci3
  - sgw-totepsbearrel-dedrsn-s1err-qci4
  - sgw-totepsbearrel-dedrsn-s1err-qci5
  - sgw-totepsbearrel-dedrsn-s1err-qci6
  - sgw-totepsbearrel-dedrsn-s1err-qci7
  - sgw-totepsbearrel-dedrsn-s1err-qci8
• sgw-totepsbearrel-dedrsn-s1err-qci9
  sgw-totepsbearrel-dedrsn-s1err-qci-other
• sgw-totepsbearrel-dedrsn-s5err
  sgw-totepsbearrel-dedrsn-s5err-qci1
  sgw-totepsbearrel-dedrsn-s5err-qci2
  sgw-totepsbearrel-dedrsn-s5err-qci3
  sgw-totepsbearrel-dedrsn-s5err-qci4
  sgw-totepsbearrel-dedrsn-s5err-qci5
  sgw-totepsbearrel-dedrsn-s5err-qci6
  sgw-totepsbearrel-dedrsn-s5err-qci7
  sgw-totepsbearrel-dedrsn-s5err-qci8
  sgw-totepsbearrel-dedrsn-s5err-qci9
  sgw-totepsbearrel-dedrsn-s5err-qci-other
• sgw-totepsbearrel-dedrsn-s4err
  sgw-totepsbearrel-dedrsn-s4err-qci1
  sgw-totepsbearrel-dedrsn-s4err-qci2
  sgw-totepsbearrel-dedrsn-s4err-qci3
  sgw-totepsbearrel-dedrsn-s4err-qci4
  sgw-totepsbearrel-dedrsn-s4err-qci5
  sgw-totepsbearrel-dedrsn-s4err-qci6
  sgw-totepsbearrel-dedrsn-s4err-qci7
  sgw-totepsbearrel-dedrsn-s4err-qci8
  sgw-totepsbearrel-dedrsn-s4err-qci9
  sgw-totepsbearrel-dedrsn-s4err-other
• sgw-totepsbearrel-dedrsn-s12err
  totepsbearrel-dedrsn-s12err-qci1
  sgw-totepsbearrel-dedrsn-s12err-qci2
  sgw-totepsbearrel-dedrsn-s12err-qci3
  sgw-totepsbearrel-dedrsn-s12err-qci4
  sgw-totepsbearrel-dedrsn-s12err-qci5
  sgw-totepsbearrel-dedrsn-s12err-qci6
  sgw-totepsbearrel-dedrsn-s12err-qci7
  sgw-totepsbearrel-dedrsn-s12err-qci8
  sgw-totepsbearrel-dedrsn-s12err-qci9
- sgw-totepsbearrel-dedrsn-local-qci-other
- sgw-totepsbearrel-dedrsn-pdn
  - sgw-totepsbearrel-dedrsn-pdn-qci1
  - sgw-totepsbearrel-dedrsn-pdn-qci2
  - sgw-totepsbearrel-dedrsn-pdn-qci3
  - sgw-totepsbearrel-dedrsn-pdn-qci4
  - sgw-totepsbearrel-dedrsn-pdn-qci5
  - sgw-totepsbearrel-dedrsn-pdn-qci6
  - sgw-totepsbearrel-dedrsn-pdn-qci7
  - sgw-totepsbearrel-dedrsn-pdn-qci8
  - sgw-totepsbearrel-dedrsn-pdn-qci9
  - sgw-totepsbearrel-dedrsn-pdn-qci-other
- sgw-totepsbearrel-dedrsn-pathfail-s1-u
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci1
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci2
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci3
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci4
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci5
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci6
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci7
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci8
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci9
  - sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci-other
- sgw-totepsbearrel-dedrsn-pathfail-s5-u
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci1
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci2
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci3
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci4
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci5
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci6
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci7
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci8
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci9
  - sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci-other
• sgw-totepsbearrel-dedrsn-pathfail-s5
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci2
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci3
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci4
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci5
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci6
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci7
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci8
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci9
  • sgw-totepsbearrel-dedrsn-pathfail-s5-qci-other

• sgw-totepsbearrel-dedrsn-pathfail-s11
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci2
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci3
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci4
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci5
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci6
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci7
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci8
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci9
  • sgw-totepsbearrel-dedrsn-pathfail-s11-qci-other

• sgw-totepsbearrel-dedrsn-pathfail-s12
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s12-qci1
  • sgw-totepsbearrel-dedrsn-pathfail-s4-u
The following counters have been added to provide more granularity in dropped call counters by reason and Qos Class Identifier (QCI)

- PGW Ini:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
- Non-Std QCI:
- S1 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:
- S5 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:
- S4 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:
• S12 Error Ind:
  • QCI 1:
  • QCI 2:
  • QCI 3:
  • QCI 4:
  • QCI 5:
  • QCI 6:
  • QCI 7:
  • QCI 8:
  • QCI 9:
  • Non-Std QCI:

• Local:
  • QCI 1:
  • QCI 2:
  • QCI 3:
  • QCI 4:
  • QCI 5:
  • QCI 6:
  • QCI 7:
  • QCI 8:
  • QCI 9:
  • Non-Std QCI:

• PDN Down:
  • QCI 1:
  • QCI 2:
  • QCI 3:
  • QCI 4:
  • QCI 5:
  • QCI 6:
  • QCI 7:
  • QCI 8:
  • QCI 9:
  • Non-Std QCI:

• Path Failure S1-U:
• QCI 1:
• QCI 2:
• QCI 3:
• QCI 4:
• QCI 5:
• QCI 6:
• QCI 7:
• QCI 8:
• QCI 9:
• Non-Std QCI:
  • Path Failure S5-U
    • QCI 1:
    • QCI 2:
    • QCI 3:
    • QCI 4:
    • QCI 5:
    • QCI 6:
    • QCI 7:
    • QCI 8:
    • QCI 9:
    • Non-Std QCI:
  • Path Failure S5:
    • QCI 1:
    • QCI 2:
    • QCI 3:
    • QCI 4:
    • QCI 5:
    • QCI 6:
    • QCI 7:
    • QCI 8:
    • QCI 9:
    • Non-Std QCI:
  • Path Failure S11:
    • QCI 1:
- QCI 2:
- QCI 3:
- QCI 4:
- QCI 5:
- QCI 6:
- QCI 7:
- QCI 8:
- QCI 9:
- Non-Std QCI:

- Path Failure S4-U:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- Path Failure S12:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- Other:
  - QCI 1:
  - QCI 2:
Feature Changes

Overcharging Protection on the S-GW

Consider the following scenario:

1. When a subscriber has an active session and loses coverage or when the subscriber is Idle, the P-GW is not aware of the subscriber state.
2. If there is valid Downlink Data for the subscriber, the P-GW forwards the data to the S-GW and counts the data towards appropriate Rf and Gy records.
3. In scenarios when the subscriber loses RF coverage or when the subscriber is not reached via paging, the data is dropped at the S-GW and causes an overcharge to users.

The software has been enhanced so that the P-GW stops billing of the data in such scenarios. The S-GW notifies the P-GW of the subscriber state about when to pause and resume charging of the subscriber, this will reduce the overcharging of the subscriber.

Customer Impact: Huge reduction in overcharging by the P-GW in the above scenarios.

Command Changes

gtpc private-extension overcharge-protection

The new command `gtpc private-extension overcharge-protection` has been added to EGTP Service Configuration Mode. This command controls whether the PDU will contain Overcharge-protection related data in the Indication IE or private extension. An Overcharge-protection license is required to enable this feature.

```
configure

context context_name

egtp-service egtp_service_name

    gtpc private-extension overcharge-protection

no gtpc private-extension overcharge-protection

end
```
Notes:

- **no**disables private extension overcharge protection. If this option is not enabled in the egtp-service, then by default the EGTPC layer will encode/decode overcharge-protection related data in the Indication information element. The default setting is disabled.
- If this command is enabled in the egtp-service then EGTPC will encode/decode overcharge-protection related data in/from the private extension instead of the Indication information element.

**Important:** An Overcharge-protection license is required to use this feature. In addition, the overcharge-protection command must be configured in *APN Profile Configuration Mode* for this feature to work properly.

Performance Indicator Changes

**show egtp-service name**

This command has been enhanced to list the private-extension overcharge-protection setting on the S-GW, if configured.

- **GTPC Private Extension**
  - **Overcharging Protection (Seconds):** Enabled or Disabled

CSCui42572 - Error response handling at SGW

Feature Changes

**Improved Error Response Handling at the S-GW**

The software has been enhanced to improve error response handling at the S-GW when an erroneous message is received by EGTPC from a peer. On receiving a bad response from the peer, instead of dropping the message while doing validation, EGTPC informs the S-GW about the bad response received. The S-GW uses this notification from EGTPC that a bad response is received to send a proper response to the other peer. This will reduce load on the S-GW due to retransmissions. This also helps in capturing statistics based on the correct cause code.

**Previous Behavior:** When an erroneous response message is received by the S-GW EGTPC service from a peer, it is dropped while performing validation. After all retries of the request message, the EGTPC service then informs the other peer that there was no response from the peer.

**New Behavior:** If error-response-handling is enabled, and EGTPC receives the first error response, it now sends back *Invalid reply from remote peer* in the response message to the other peer.

**Customer Impact:** There will be no request message retries if the error response is received.

Command Changes

**gtpc error-response-handling**

The new command **gtpc error-response-handling** has been added to *EGTP Service Configuration Mode*. This command controls error response handling at the S-GW when an erroneous message is received by EGTPC from a peer.
configure

context context_name

  egtp-service egtp_service_name

    gtpc error-response-handling

    no gtpc error-response-handling

end

Notes:

- If this command is enabled in the egtp-service then on receiving a bad response from the peer instead of dropping the message while doing validation EGTPC informs the S-GW about the bad response received. The S-GW uses this notification from EGTPC that a bad response is received to send a proper response to the other peer.
- no disables the Error Response handling feature. The default setting is disabled.

CSCui95971, CSCuj13956 - Rel10 Compliance for SGW-CDRs

Feature Changes

Release 10 Charging Compliance for S-GW CDRs

To more fully comply with 3GPP Release 10, the following TLVs have been added to S-GW Call Detail Records (CDRs):

- IMSI Unauthenticated Flag
- Dynamic Address Flag extension
- S-GW Address IPv6
- Serving Node IPv6 Address
- P-GW Address IPv6

The new attributes are added to S-GW custom dictionaries CUSTOM24 and CUSTOM35.
Chapter 21
SaMOG Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from SaMOG in StarOS 16 software releases.
SaMOG Enhancements for 16.0

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

---

**CSCue39756, CSCuh83489, CSCue00861, CSCug95521, CSCue39761 - Ethernet over GRE Support on SaMOG Gateway**

**Feature Changes**

**Ethernet over GRE Support on SaMOG**

With this release, SaMOG supports Ethernet over GRE (EoGRE) based access. SaMOG can now use both PMIP (supported from Release 15.0 onwards) and EoGRE based access from a trusted WLAN network to connect subscribers to 3G/4G networks.

This feature enables 4G/3G subscribers to connect to EPC/Internet using the trusted WiFi SSIDs served by EoGRE enabled Residential Gateways in SaMOG. SaMOG acts as the tunnel endpoint for the EoGRE tunnel initiated from the Residential Gateway. Using the SSID-based WLAN access, users are authenticated based on the SSID they select to connect to WLAN. The Residential Gateway/WLC maintains separate SSIDs to provide 3G/4G access, and users can select the appropriate SSID based on their subscription to obtain 3G or 4G access through the WiFi network.
With this feature, SaMOG acts as the AAA server and DHCP server to the user equipment (UE) that connects to the WLAN network. SaMOG processes all the control packets from the UE and maintains the subscriber session to provide 3G/4G access. Acting as the DHCP-server, SaMOG creates the PDP context with GGSN/PGW and obtains the IP address to allocate to the UE through DHCP-Response in the access-side. The interface with GGSN is similar to the TTG's Gn' interface with GGSN for 3G, and the existing SaMOG's S2a interface with PGW for 4G. The DHCP and data packets originating from the UE are forwarded by the Residential Gateway/WLC node through the EoGRE tunnel to SaMOG.

The MRME service maintains all the access network parameters (Radius client and access client details) locally. The MRME service determines the session’s access-type and if a request should be accepted or rejected, based on the NAS IP (AVP in the Access-Request/Accounting-Request) and Source IP of the request by looking up the local configuration and conveys the same to CGW for session setup.

**Command Changes**

**twan-profile**

Creates a Trusted Wireless Access Network (TWAN) profile and enters the TWAN Profile Configuration Mode for the current context. The TWAN profile contains information on the RADIUS client addresses (WLC) and access-type corresponding to the RADIUS clients.

```plaintext
configure
  context context_name
    [ no ] twan-profile twan_profile_name
  end
```

**access-type**

This command allows you to specify the access-type for the Radius client or specify a default access type for all Radius clients under a TWAN profile.

```plaintext
configure
  context context_name
    twan-profile twan_profile_name
      access-type [ client { ipv4/ipv6_address[/mask] } ] { eogre | pmip }
      no access-type { client { ipv4/ipv6_address[/mask] } | eogre | pmip }
    end
```

**radius**

This command allows you to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

```plaintext
configure
  context context_name
```
associate

With this release, the `twan-profile` keyword is introduced for this command to associate one or more TWAN profile with the current MRME service.

```plaintext
configure
    context context_name

    mrme-service mrme_service_name

    cmd variable

    [ no ] associate twan-profile twan_profile_name

end
```

radius client

From this release onwards, the `radius client` command in the MRME Configuration Mode has been deprecated and replaced with the `radius` command in the TWAN Profile Configuration Mode.

Notes:

- For backward compatibility, the CLI is still supported. A warning is displayed when legacy radius client is configured under MRME service.
- If MRME service already has legacy Radius client configured under it, the TWAN profile association is denied.
- If MRME service already has a TWAN profile association, the legacy radius client configuration is denied.

associate

With this release, the `dhcp-service` keyword is added to this command in the SaMOG Service Configuration Mode to associate a DHCPv4 service with the SaMOG service.

```plaintext
configure
    context context_name

    samog-service samog_service_name

    [ no ] associate dhcp-service dhcp_service

end
```

Notes:
For the Ethernet over GRE (EoGRE) feature to function, a DHCPv4 service must be associated with the SaMOG service.

**virtual-mac**

Configures the virtual MAC address for this APN profile to use as the default gateway’s MAC address for the user equipment (UE). This command is specific to SaMOG and introduced in support of the EoGRE feature.

```
configure

apn-profile profile_name

[ no ] virtual-mac mac_address

end
```

**Performance Indicator Changes**

**show mrme-service { name | all }**

With this release, the Radius clients under MRME service display the TWAN profile name with which they are associated.

- Twan-Profile Name

**show samog-service { all | name <service-name> }**

With this release, the output for this command has been extended to show the associated DHCP service which acts as a DHCP server for the EoGRE feature.

- Associated DHCP service

**show sub all**

With this release, the output for this command has been modified to show the access-type as samog-eogre/samog-pmip.

- (r) - samog-pmip
- (+) - samog-eogre

**show sub samog-only full**

With this release, the output for this command has been modified to show the following fields in support of the SaMOG EoGRE feature:

- Access Type : samog-eogre
- CGW Subscriber Info:
  - UE default-gw-addr
  - VLAN ID
  - UE VMAC Address
show sub full

With this release, the output for this command has been modified to show the following fields in support of the SaMOG EoGRE feature:

- Access Type: samog-eogre
- UE def-gw-addr
- UE MAC Address
- AP MAC
- SSID

show dhcp statistics

With this release, the command output has been extended to show the statistics of associated DHCP service as well. The additional statistics are exactly similar to the output of `show dhcp statistics dhcp-service dhcp_service` command.

DHCP Service Stats:

- Session Stats:
  - Total Current:
    - DHCP Proxy
    - DHCP Relay Agent
    - DHCP Server
  - Total Setup:
    - DHCP Proxy
    - DHCP Relay Agent
    - DHCP Server
    - Total Released
  - Session Release Reasons: (dhcp-proxy)
    - Admin Releases
    - Bearer Call Terminated
    - Lease Exp Policy
    - Lease Renew Failure
    - IP Address mismatch
    - Lease time mismatch
    - Chaddr mismatch
    - Client-identifier mismatch
    - Other Reasons
  - Session Release Reasons: (dhcp-relay)
• Admin Releases
  • Bearer Call Terminated
  • Lease Timed-out
  • Other Reasons

• Session Release Reasons: (dhcp-local-server)
  • Admin Releases
  • Bearer Call Terminated
  • Lease Timed-out
  • Other Reasons

• Session Release Reasons: (dhcp-local-server)
  • Admin Releases
  • Bearer Call Terminated
  • Lease Timed-out
  • Other Reasons

• DHCP Messages
  • DISCOVER TX
  • DISCOVER retransmitted
  • DISCOVER RX
  • DISCOVER retrieved RX
  • DISCOVER relayed
  • DISCOVER retransmitted relayed
  • OFFER RX
  • OFFER Discarded
  • OFFER TX
  • OFFER relayed
  • REQUEST TX
  • REQUEST retransmitted
  • REQUEST RX
  • REQUEST renewal RX
  • REQUEST relayed
  • REQUEST renewing relayed
  • ACK RX
  • ACK for INFORM
  • ACK Renewing RX
• ACK TX
• ACK Renewing TX
• ACK relayed
• ACK renewing relayed
• NAK RX
• NAK for INFORM
• NAK TX
• NAK relayed
• DECLINE TX
• DECLINE RX
• DECLINE relayed
• RELEASE TX
• RELEASE RX
• RELEASE relayed
• RELEASE for relay call
• INFORM TX
• INFORM retransmitted
• INFORM RX
• INFORM relayed

• DHCP OFFER Discard Reasons
  • Parse error
  • Lease less than min
  • Lease greater than max
  • IP Validation failed
  • XID mismatch

• DHCP ACK Discard Reasons:
  • Parse error
  • XID mismatch

• DHCP DECLINE Reasons: (dhcp-proxy)
  • IP mismatch

• DHCP DISCOVER Discard Reasons:
  • Parse error

• DHCP REQUEST Discard Reasons:
  • Parse error
• Renewal Statistics: (dhcp-proxy)
  • IP Lease Renewals
  • Failed IP Lease Renewals
    • No reply from server
    • Server NAK
    • IP address mismatch
    • Lease mismatch

**show apn-profile full**

With this release, the output of this command has been modified to display virtual mac configuration details.

• Virtual MAC

**show configuration errors**

With this release, this command has been extended to show the missing DHCP configuration for EoGRE.

• Warning: DHCP service not configured for SAMOG service <samog1> in the context <samog>. EoGRE clients will not work.

**CSCug95440, CSCuj24323, CSCul39688, CSCul94593 - Local Breakout on SaMOG GW**

**Feature Changes**

**SaMOG Local Breakout Support**

With this release, SaMOG extends support for the Local Breakout (LBO) feature to enable subscribers to access the Internet without having to connect to the EPC core. The LBO feature is implemented by configuring a local PGW. All subscribers of a particular APN will be locally broken out and will not connect to PGW over the S2a interface. SaMOG performs IP allocation locally.

The APN provided by AAA is mapped to the locally configured PGW service IP. This eliminates the need for a DNS. The local PGW assigns the IP using a locally configured IP pool after receiving the subscriber information from AAA. Subscriber information is received from the SaMOG service to the local PGW service through a GTP tunnel. This tunnel is set up with in the same chassis.

The MRME service provides the following functionality:

• If the AAA server requests a local breakout support for the subscriber, MRME service communicates the same to CGW during call setup.

• If the AAA server does not provide any indication for a local breakout support, or if the AAA server requests support for both local breakout and EPC core connection, MRME service determines if a local breakout support is needed for a session by looking up the apn-profile at the local policy. The decision is communicated to CGW during call setup.
New SaMOG Local Breakout Diameter Attributes

Two new Diameter attributes: "DER-Flags" and "DEA-Flags" are included in the Diameter-EAP-Request (DER) and Diameter-EAP-Answer (DEA) messages to support the Local Breakout feature. These attributes are added under the AAA attribute "LTE_STa_Auth" in the RADIUS dictionary.

SaMOG Local Breakout License

In support of this feature, an optional SaMOG Local Breakout license has been introduced.

Important: For more information on the SaMOG Local Breakout license, contact your Cisco account representative.

Command Changes

associate

This command associates another service to the current CGW service.

With this release, the pgw-service keyword has been introduced to the CGW Service Configuration Mode in support of the LBO feature.

configure

    context context_name
    
    cgw-service cgw_service_name
    
    associate pgw-service pgw_service
    
    no associate pgw-service
    
    end

precedence

This command sets the order of precedence, the matching criteria and the association to an operator policy for subscribers meeting the match criteria.

With this release, the ssid keyword has been introduced to the LTE Subscriber Map Configuration Mode in support of the LBO feature.

configure

    lte-policy
    
    subscriber-map subscriber_map_name
    
    precedence number match-criteria imsi mcc mcc_num mnc mnc_num msin first
    start_range last end_range [ ssid id ] operator-policy-name policy_name
    
    precedence number match-criteria [ imsi mcc mcc_num mnc mnc_num ] [ service-plmnid id ] ssid id operator-policy-name policy_name
local-offload

With this release, this command has been introduced to enable or disable the SaMOG Local Break Out (LBO) feature.

configure

apn-profile profile_name

[ no ] local-offload

end

Notes:
- When enabled, LBO will be allowed for the UE connecting to the specified SSID, through which this APN profile is reached.

Performance Indicator Changes

show cgw-service all

With this release, the following fields have been added to the output of this command in support of the LBO feature:
- PGW service : pgw-ingress
  If the PGW service is not configured:
  - PGW service : n/a

show apn-profile full name <name>

With this release, the following fields have been added to the output of this command in support of the LBO feature:
- Local Offload : {Enabled | Disabled}

show subscribers samog-only full

With this release, the following fields have been added to the output of this command in support of the LBO feature:
- Network Access Mode : { Local Offload | EPC(GTPv1) | EPC(GTPv2) }

show samog-service statistics

With this release, the following fields have been added to the output of this command in support of the LBO feature:
- Network Access Mode Stats:
  - Local Offload
  - GTPv1
  - GTPv2
CSCug95458 - CDRs on CGW and SaMOG GW

Feature Changes

CDR Support on CGW and SaMOG

With this release, SaMOG supports generation of CDR files for offline charging. In Offline Charging, charging information is collected concurrently with resource usage. The charging information is then passed through a chain of logical charging functions, and the CDR files are generated by the network, which are then transferred to the network operator's Billing Domain.

As 3GPP specifications does not define a CDR format for SaMOG, the SGW CDR and SGSN CDR record formats are used to define the CDR format for SaMOG 4G/3G subscribers. The record format can be selected using a CLI command under the GTPP Group Configuration Mode for SAMOG mixed license. For SAMOG 3G license only SGSN record type can be used. By default, for an SaMOG mixed license, the SGW record type is used, and for an SaMOG 3G license, the SGSN record type is used.

Previous Behavior: In previous releases, offline charging (CDR generation) was not supported on SaMOG.

New Behavior: With this release, offline charging (CDR generation) is now supported.

Customer Impact:

- Offline charging (CDR) generation is supported for SaMOG.
- Accounting policy can be configured for SaMOG CDR.
- Accounting mode and charging char are displayed in the CLI output.
- Accounting policy is displayed in the CLI output.

Command Changes

associate accounting-policy

With this release, this command has been introduced to associates the APN with specific pre-configured policies configured in the same context for SaMOG charging.

configure

    apn-profile profile_name

    associate accounting-policy policy_name

    remove associate accounting-policy

end

Notes:

- The accounting policy if configured under the APN profile takes priority over the accounting poilcy configured under the call control profile.

accounting context
With this release, this command has been introduced to define the name of the accounting context and associate a GTPP group with the current APN profile.

```plaintext
configure

apn-profile profile_name

  accounting context context_name gtpp group group_name

  remove accounting context

end
```

Notes:
- Even if an accounting context is also specified in a call control profile, the priority is given to the accounting context of the APN profile.

**accounting mode**

With this release, this command command has been introduced to define the mode of accounting to be performed for this SaMOG APN profile.

```plaintext
configure

apn-profile profile_name

  accounting mode { gtpp | none }

  [ default | remove ] accounting mode

end
```

Notes:
- **default**: Resets the accounting mode to GTPP.
- **remove**: Removes the accounting mode from the current profile’s configuration.
- Even if an accounting mode is also specified in a call control profile, the priority is given to the accounting mode of the APN profile.

**associate**

This command associates various MME-specific lists and databases with this call control profile. On an SGSN, this command can be used to associate some of these MME-related items to GPRS and/or SGSN services in support of S4 functionality. For SaMOG, this command can be used to associate various SGW/SGSN CDR triggers for the call control profile.

With this release,

```plaintext
configure

call-control-profile profile_name

  associate accounting-policy policy_name
```
remove associate accounting-policy

end

Notes:
- If no policy is configured, triggers based on the call control profile will not be generated, and the accounting policy in the SaMOG service context will be used.

gtpp attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented. Many keywords are also applicable to S-GW and P-GW CDRs.

With this release, the record-type keyword has been introduced for selection of the CDR type for the SaMOG offline charging feature.

configure

context context_name

gtpp group group_name

gtpp attribute record-type { sgsnprecord | sgwrecord }

no gtpp attribute record-type

end

Notes:
- Default: sgwrecord
- For an SaMOG 3G license, this keyword will not be available. However, sgsnprecord type will be used as the default record type.

Performance Indicator Changes

show call-control-profile full name <name>

With this release, the following fields have been added to the output of this command in support of the SaMOG offline charging feature:
- Accounting Mode (SGW/SaMOG)
- Accounting Policy (SaMOG) : <name>

show subscriber samog-only full all

With this release, the following fields have been added to the output of this command in support of the SaMOG offline charging feature:
- Accounting mode: GTPP
- Charging id
- Charging chars
show apn-profile full all

With this release, the following fields have been added to the output of this command in support of the SaMOG offline charging feature:

- Accounting Context Name (SaMOG) : <acct-context>
- Accounting GTPP Group Name (SaMOG) : <gtpp-group-name>
- Accounting Mode (SaMOG) : Gtpp
- Accounting Policy (SaMOG) : <policy-name>

show gtppp group name <name>

With this release, the following fields have been added to the output of this command in support of the SaMOG offline charging feature:

- Record-Type (SaMOG) : SGSNPDPRECORD/sgwrec (only for SAMOG mixed license)

CSCug95483, CSCuj80861 - SaMOG support for 3G subscribers

Feature Changes

SaMOG Support for 3G Subscribers

This feature enables the use of SaMOG gateway to service 3G subscribers by anchoring GTPv1 WiFi sessions to the GGSN of existing 3G networks. Billing and other 3G services like DPI are available for the subscriber attached to the WiFi session. On the data plane, SAMOG accepts L3 WiFi packets, encapsulates them into GTP tunnels, and forwards them to GGSN. These packets are then decapsulated in the downlink direction by SAMOG and forwarded to the WiFi network.

The AAA server is selected based on the local policy configuration that contains the serving PLMN (derived from NAI) of the subscriber. The configuration also indicates the authentication method (RADIUS or STa) for that AAA server. The call type (3G or 4G) depends on the subscriber profile information received from the AAA server.

SaMOG used in an operator's WLAN offload scheme typically follow the models outlined below:

- **3G only Packet Core (Pre-release 8 Mobile Packet Core (MPC))**: The network nodes in this model are not Release 8 complaint. MRME uses the Radius interface towards AAA Server for authentication and fetches the 3G specific attributes of the authenticated user such as IMSI, MSISDN, APN from the Radius Access-Accept Message from the AAA Server.

- **Overlay 3G/4G network (Release 8 Complaint Evolved Packet Core (EPC) Nodes)**: This is a deployment model where EPC nodes and 3G MPC coexist. Assuming that the 3GPP AAA Server is Release 8 compliant, 3G subscribers are authenticated using the STa interface. As a 4G network can support an STa interface, Radius-based authentication is used only for 3G subscribers.

**Important**: As 3GPP specifications do not provide guidance for receiving 3G QoS parameters on STa interface or supporting a GTPv1 call with STa authentication, this feature for 3G/GTPv1 support with STa authentication is a proprietary solution until the 3GPP specifications are updated to accommodate the same.

License Requirements
With this release, two SaMOG base licenses will be made available for operators with different network model requirements:

- An SaMOG 3G-only license for operators running a 3G only deployment model. With this license, operators can setup 3G (GTPv1) calls through SaMOG. A Diameter based authentication will not be available.
- An SaMOG 3G/4G license for operators running a 4G, or 4G/3G mixed mode deployment model. With this license, operators can setup a 3G or 4G call based on the serving PLMN and the subscription of the subscriber.

**Important:** The aforementioned licenses are mutually exclusive and cannot be used together on SaMOG. For more information on SaMOG licenses, contact your Cisco account representative.

### Command Changes

**authenticate context**

With this release, this command has been introduced to specify the authentication group, context, and type of authentication for the AAA server.

```configure
  call-control-profile profile_name
    authenticate context context_name [ aaa-group aaa_group_name ] [ auth-type { diameter | radius } ]
    remove authenticate context [ aaa-group ]
  end
```

Notes:

- Default (SaMOG 3G license): radius
- Default (SaMOG Mixed Mode license): diameter
- The `auth-type { diameter | radius }` keyword is available only if the SaMOG Mixed Mode license is configured.

**dns-mrme**

With this release, this command has been introduced to configure the DNS client context and DNS query type used for the PGW/GGSN resolution for MRME.

```configure
  call-control-profile profile_name
    dns-mrme { context context_name [ query-type { a-aaa | snaptr } ] | query-type { a-aaa | snaptr } }
    no dns-mrme context
    default dns-mrme query-type
```
Notes:

- The `default dns-mrme query-type` command is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.

- The default dns-context is configured under the MRME Service Configuration Mode. If no DNS context is configured under the MRME Service Configuration Mode, the DNS context will be used as the context for the MRME service.

**mobility-protocol**

With this release, this command has been introduced to configure the default GTP version to be used for setting up a call when the AAA server forwards an IP address directly.

```plaintext
configure
  call-control-profile profile_name
    mobility-protocol { GTPv1 | GTPv2 }
    default mobility-protocol
  end
```

Notes:

- Default (SaMOG 3G license): GTPv1
  - Default (SaMOG Mixed Mode license): GTPv2
- If mobility protocol is also configured in the APN Profile Configuration Mode, the value configured here will be overridden with the configured value in the APN profile.

**mobility-protocol**

With this release, this command has been introduced to configure the default GTP version to be used for setting up a call when the AAA server forwards an IP address directly.

```plaintext
configure
  apn-profile profile_name
    mobility-protocol { GTPv1 | GTPv2 }
    no mobility-protocol
  end
```

Notes:

- This command is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.
- If mobility protocol is also configured under the Call Control Profile Configuration Mode, the value configured here will override the configured value in the Call Control profile.
• By default, all APN profiles will use the mobility protocol configured under the Call Control Profile Configuration Mode.

twan

With this release, this command has been introduced to configure the APN profile with the default gateway address and mask to be sent in the DHCP offer and PBA messages.

```
configure
  apn-profile profile_name
    [ no ] twan default-gateway ipv4/ipv6_address/mask
  end
```

Notes:
• A maximum of 16 IP addresses and subnet masks can be configured (in separate lines) for each APN profile.

associate

This command associates another service to this CGW service.

With this release, the `sgtp-service` command has been introduced.

```
configure
  context context_name
    cgw-service cgw_service_name
      associate sgtp-service sgtp_service [ context context_name ]
      no associate sgtp-service cmd variable
    end
```

Notes:
• `context`: Defines the context in which the SGTP service was created. If no context is specified, the current context will be used.

Performance Indicator Changes

show apn-profile full all

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

• MRME Mobility Protocol: {GTPv1 | GTPv2}
• TWAN Default Gateway (s):
  • Default Gateway1
  • Default Gateway2
show call-control-profile full all

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

- Call Control Profile Name = <cc-profile name>
- MRME Authentication Type : {RADIUS | DIAMETER}
- MRME DNS Query Type : {A-AAAA | SNAPTR}
- MRME DNS Context Name : <context name>
- MRME Mobility Protocol: {GTPv1 | GTPv2}

show samog-service statistics

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

- PGW/GGSN Selection Stats
  - IP Address
  - Hostname
  - SNAPTR Procedure
    - Success
    - Failure
  - APN FQDN
    - SNAPTR Procedure
    - A/AAA Procedure

- Network Access Mode Stats:
  - GTPv1
  - GTPv2

show subscribers samog-only full all

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

- IMSI
- PLMN
- Call-Control Profile
- Current AAA Server Details
- AAA Auth context
- AAA Auth group
- AAA Auth type
SaMOG Enhancements for 16.0

- DNS Context
- Configured Mobility Protocol: { GTPv1 | GTPv2 }
  - Network Access Mode: { Local Offload | EPC(GTPv1) | EPC(GTPv2) }

**show cgw-service all**

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

- SGTP Service: <service name> (or n/a of not configured)
- SGTP Service context: <context name> (or n/a of not configured)

**show subscriber all**

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

- (/) - GTPv1 (For SAMOG)
- (!) - GTPv2 (For SAMOG)

**show subscriber samog-only full**

With this release, the output of this command has been modified to show the network-type as GTPv1/GTPv2, in addition to new fields for control and datapath.

- Network Type: GTPv1
- CGW Subscriber Info:
  - ggsn c-addr
  - ggsn u-addr
  - cgw gn c-addr
  - cgw gn u-addr
  - ggsn c-teid
  - ggsn u-teid
  - cgw gn c-teid
  - cgw gn u-teid
- Bearer QoS:
  - alloc/retention priority
  - delay class
  - reliability class
  - peak throughput (oct/s)
  - mean throughput (oct/h)
  - precedence class
• traffic class
• delivery order
• Source stats Descriptor
• Transfer Delay
• Negotiated MBR for up (bps)
• Negotiated MBR for down (bps)
• Negotiated GBR for up (bps)
• Negotiated GBR for up (bps)

**show subscriber full all**

With this release, output of this command has been modified to show the network-type as GTPv1/GTPv2

• Network Type: { GTPv1 | GTPv2 }

**show samog-service statistics**

With this release, the following fields have been added to the output of this command for SaMOG’s support for 3G Subscribers:

• GTPv1 PDNs:
  • Active
  • Setup
  • Released
  • Rejected

• GTPv2 PDNs:
  • Active
  • Setup
  • Released
  • Rejected

• PDNs Released By Reason:
  • GGSN Ini

• Gn-U Total Data Statistics:
  • Uplink:
    • Total Pkts
    • Total Bytes
    • Dropped Pkts
    • Dropped Bytes
  • Downlink:
    • Total Pkts
CSCuh75537 - Congestion Control Threshold and TCA Alerts

Feature Changes

SaMOG Congestion Control and Threshold Crossing Alerts (TCA) Support

With this release, SaMOG enhances on the StarOS framework to provide congestion control policies and threshold crossing alerts to ensure smooth performance of the SaMOG service and prevent congestion. This feature enables you to set policies and thresholds, and specify how the system should react in the event of a heavy load condition. The StarOS congestion control framework monitors the system performance and invokes configured policies in the event of a degraded performance to handle it.

Congestion control monitors the following resources:

- Licensing utilization
- Maximum sessions per service utilization
- Demux message queue utilization
- Demux message queue wait time
- Port Rx specific utilization
- Port Tx specific utilization
- Averate transmit port Tx utilization
- Process CPU utilization
- System CPU utilization
- System memory utilization

The behavior of system under high load or overload conditions can be specified using Congestion control.

The TCA feature monitors a variety of internal resources and user traffic events. The threshold values for the monitored resources and events can be configured, and the system generates an alarm when the threshold is exceeded.

Command Changes

```
congestion-control policy

This command configures congestion control policies.

With this release, the samog-service keyword has been introduced to support SaMOG’s Congestion Control.

configure

    congestion-control policy samog-service action { drop | none | reject }

end
```
threshold per-service-samog-sessions

With this release, this command has been introduced to configure alarm or alert thresholds for the number of S2a Mobility over GTP (SaMOG) sessions per SaMOG service in the system.

```
configure

threshold per-service-samog-sessions high_thresh [ clear low_thresh ]
end

threshold poll per-service-samog-sessions

With this release, this command has been introduced to configure the polling interval in seconds over which to count the number of S2a Mobility over GTP (SaMOG) contexts per SaMOG service in the system.

```
configure

threshold poll per-service-samog-sessions interval duration
end
```

Performance Indicator Changes

**show samog-service statistics**

With this release, the following field has been introduced to support SaMOG’s Congestion Control Threshold:

- Congestion control policy applied

CSCuh83409, CSCuh83390, CSCul94616, CSCul94628 - Session Recovery support on SaMOG

Feature Changes

**SaMOG Session Recovery Support**

With this release, SaMOG has the ability to recover fully created sessions in the event of process level or card level failures. This feature supports the following types of session recovery:

- **Task level recovery**: SaMOG sessions are recovered when a Session Manager task serving the session is terminated due to a software error.

- **Card level recovery**: SaMOG sessions are recovered when the entire PSC/DPC card hosting the Session Manager fails, and all the tasks running on that card have to be recovered.

When the Session Recovery feature is enabled using the CLI, the Session Manager maintains a backup of the session critical information with the AAA Manager that has the same instance number. A paired AAA Manager with the same instance number as the Session Manager is started on a different PSC/DPC card. When a failure is detected, the Call Recovery Record (CRR) that contains the backed up information is fetched from the AAA Manager, and the sessions are re-created on the recovered Session Manager.
This feature requires a minimum of four PSCs (3 active and 1 standby). As the SaMOG session recovery feature makes use of the existing StarOS IPSG framework, new fields are added to the IPSG session recovery record to recover attributes specific to the SaMOG session (For example: GRE end point address, SaMOG EGTPC information, etc).

**SaMOG Session Recovery License**

In support of this feature, two optional SaMOG session recovery licenses have been introduced for an SaMOG 4G/3G deployment model, and SaMOG 3G only deployment model.

**Important:** For more information on SaMOG session recovery licenses, contact your Cisco account representative.

**CSCun71453 - [SaMOG-3G] 3gpp2 attributes needs to be removed from radius server dict**

**Feature Changes**

**3GPP2 RADIUS Attributes Removed from custom70 Dictionary for SaMOG**

With this release, the RADIUS dictionary "custom70" for SaMOG is updated to include only two RADIUS accounting attributes and three Authentication groups - standard, ThreeGPP, and Starent-VSA1.

The ThreeGPP2 set of attributes are removed from custom70 as these attributes are not used by SaMOG, but still being parsed in the Access request messages.

**CSCuo29010 - [SaMOG-GW] Support for Sequence Number Bit unset default with PMIP GRE**

**Feature Changes**

**GRE Sequence Number Validation**

With this release, in order to address SaMOG from automatically validating the PMIPv6 GRE sequence number in the data packets, a new configuration option has been introduced to enable or disable sequence number validation when required.

**Command Changes**

gre sequence-numbers

With this release, this command has been introduced to enable or disable the inclusion of sequence number bit and sequence number value in the GRE encapsulation header

```
configure

context context_name
```

**Release Change Reference, StarOS Release 16**
cgw-service cgw_service_name

[ no ] gre sequence-numbers

end

Notes:

- Use the no keyword to disable the inclusion of sequence number bit and sequence number value in the GRE encapsulation header.
- By default, this configuration is disabled.

Performance Indicator Changes

show cgw-service all

With this release, the following field has been introduced to indicate if the configuration for the GRE Sequence number bit is enabled or disabled:

- GRE Sequence Numbers
Chapter 22
SecGW Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from SecGW in StarOS 16 software releases.
SecGW Enhancements for 16.1

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

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

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

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

---

**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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**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
```

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

**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

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.

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 COngfiguration 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 the show wsg-service 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
SecGW Enhancements for 16.0

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

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

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

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

---

**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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCuf52257 – Support DHVPv4**

**Feature Changes**

**IP Address Allocation Method**

The default method for IPv4 address allocation is from a local pool. You also have the option of specifying a DHCPv4 proxy server.

**Previous Behavior:** IPv4 address allocation was solely handled via local pools.

**New Behavior:** You can now specify the use of a DHCPv4 server for allocating IP addresses.
Command Changes

dhcp { context-name context_name | service-name srvc_name }

This is a new command in a wsg-service configuration that allows you to specify a DHCPv4 proxy server for allocating IP addresses. You must specify both the context associated with the DHCPv4 service, as well as the name of the service. This will be the DHCPv4 service used if you configure the IP address allocation method to dhcp-proxy.

configure

    context wsg_context

        ip address alloc-method dhcp-proxy

        dhcp context-name dhcpv4_srvc_context

        dhcp service-name dhcpv4_service

    end

Notes:
- Only one DHCPv4 service can be configured.
- You must restart the WSG service for these settings to be effective. You restart the service by unbinding and binding the IP address to the service context.

ip address alloc-method { dhcp-proxy | local }

dhcp-proxy is a new keyword in this command. It specifies the use of a DHCPv4 service for allocating IPv4 addresses.

configure

    context wsg_context

        ip address alloc-method dhcp-proxy

        ip address alloc-methods dhcp-proxy

    end

Notes:
- The DHCPv4 service that will be used must be specified via the dhcp context-name and dhcp service-name commands.
- You must restart the WSG service for this setting to be effective. You restart the service by unbinding and binding the IP address to the service context.
CSCug99134 - RRI For Remote Access

Feature Changes

RRI Support for RAS IPSec

Security Gateway (SecGW) now supports Reverse Route Injection (RRI) for Remote Access Service (RAS) IPSec deployment mode.

RRI injects routes in the reverse direction onto the ASR 9000 VSM (IOS-XR blade) so that clear traffic can be routed to the correct interface on the target VSM. The OneP (ConnectedApps [CA]) library provides the necessary API calls to CA clients to communicate to the oneP server (running on IOS-XR).

The RRI feature is used in conjunction with the StarOS SecGW to deal with Site-to-Site (S2S) IPSec SAs. RRI route transaction is initiated when a tunnel SA is being created.

For detailed information, see Security Gateway Administration Guide and QvPC-VSM System Administration Guide.

Command Changes

**ip rri-remote-access**

This new command configures RRI remote access mode parameters. This command is only required for Remote Access Service configurations.

```
configure
   context context_name
       ip rri-remote-access { ip_address | next-hop nexthop_address } interface interface_name [ vrf vrf_name ]
```

Notes:

- *ip_address* and *next_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 new 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 `next_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.

**rri-mode**

This new ConnectedApps Configuration mode command configures the supported RRI mode.

```
cfg rri-mode { both | none | ras | s2s }
```

Notes:
- `ras` = Remote Access Service
- `s2s` = site-to-site

**CSCui71288 – Bulk Stats support for 16.0 on SecGW**

**Performance Indicator Changes**

**wsg Schema**

The following bulk statistics have been added in support of the Security Gateway (SecGW):
- `wsg-current-sessions-total`
- `wsg-current-active-sessions`
- `wsg-current-dormant-sessions`
- `wsg-current-active-ipv4-sessions`
- `wsg-current-dormant-ipv4-sessions`
- `wsg-current-active-ipv6-sessions`
- `wsg-current-dormant-ipv6-sessions`
- `wsg-current-simple-ipv4-total`
- `wsg-current-simple-ipv6-total`
- `wsg-current-data-clients-total`
- `wsg-total-simple-ip-attempts`
- `wsg-total-simple-ip-successes`
- wsg-total-simple-ip-failures
- wsg-total-simple-ip-fallback-successes
- wsg-total-simple-ip-fallback-failures
- wsg-total-simple-ip-fallback-no-mobile-ip-req-rx
- wsg-total-simple-ip-fallback-not-allowed
- wsg-total-simple-ip-fallback-tagged-pool-address
- wsg-total-simple-ip-fallback-fail-misc-reasons
- wsg-total-setup-successes
- wsg-total-setup-attempts
- wsg-total-attempts-failed
- wsg-total-disconnected
- wsg-total-disconnected-locally
- wsg-total-disconnected-remotely
- wsg-total-simple-ip-ipv4-sessions
- wsg-total-disconnected-remotely-before-connect
- wsg-total-disconnected-remote-disc-ipsec
- wsg-total-disconnected-admin-disconnect
- wsg-total-disconnected-idle-timeout
- wsg-total-disconnected-absolute-timeout
- wsg-total-disconnected-long-duration-timeout
- wsg-total-disconnected-session-setup-timeout
- wsg-total-disconnected-no-resource
- wsg-total-disconnected-auth-failure
- wsg-total-disconnected-flow-add-failure
- wsg-total-disconnected-invalid-dest-context
- wsg-total-disconnected-source-addr-violation
- wsg-total-disconnected-duplicate-request
- wsg-total-disconnected-mac-validation-failure
- wsg-total-disconnected-addr-assign-failure
- wsg-total-disconnected-misc-reasons
- wsg-total-eap-server-total-received
- wsg-total-eap-server-challenge-received
- wsg-total-eap-server-success-received
- wsg-total-eap-server-failure-received
• wsg-total-eap-mobile-total-received
• wsg-total-sent-to-eap-server
• wsg-total-initial-requests-sent-to-eap-server
• wsg-total-eap-server-requests-forwarded
• wsg-total-eap-mobile-discarded
• wsg-total-eap-server-discarded
• wsg-total-packets-sent
• wsg-total-bytes-sent
• wsg-total-packets-rcvd
• wsg-total-bytes-rcvd
• wsg-total-packets-violations

For additional information on these bulk statistics, see the Statistics and Counters Reference.

**CSCum95936 - Document SecGW HA support in inter-chassis and intra-chassis mode**

**Feature Changes**

**SecGW Support for HA Intrachassis and Interchassis HA Configurations**

The following user documents describe high availability (HA) configurations for QvPC-VSM (ICSR-SRP) and ASR 9000 VSM (IOS-XR):

- **16.0 QvPC-VSM System Administration Guide**
- **16.0 Security Gateway Administration Guide**
Chapter 23
SGSN Changes in Release 16

This chapter identifies features and functionality added to, modified for, or deprecated from SGSN in StarOS 16 software releases.
SGSN Enhancements for 16.5

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 *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.

**CSCus80817 - RAB-SetupOrModify message should not include some fields in case of Modi**

**Feature Changes**

**Configurable RANAP IE in RAB Assignment Request**

According to 3GPP 25.413 Section 8.2.2: “For each RAB requested to be modified, the message may contain:

- RAB ID (mandatory);
- NAS Synchronisation Indicator;
- RAB parameters;
- Transport Layer Information;
- User Plane Information.

At a RAB modification, it is only possible to include information elements (IEs), other than the RAB ID and possibly the NAS Synchronisation Indicator, in the RAB ASSIGNMENT REQUEST message when a previously set value for
another IE is requested to be modified, for example the Transport Layer Information IE or the User Plane Information IE.

**Previous Behavior:** "Data Volume Reporting Indication IE" and "PDP Type Information IE" in RAB Assignment Request modification are optional, per 3GPP specifications, and the SGSN was implementing the option by including these IEs. This behavior was not configurable by the operator and some RNCs rejected RAB Assignment Requests which included either of these IEs.

**New Behavior:** With this change, the SGSN can send a request for modification to include a RANAP IE: "Data Volume Reporting Indication IE" or "PDP Type Information IE". New keywords have been added to the existing CLI `rab-modify-procedure normal-modify` to allow the operator to enable or disable sending RANAP information elements "Data Volume Reporting Indication IE" or "PDP Type Information IE" for the RAB Assignment Request modification.

**Command Changes**

```
rab-modify-procedure
```

Two new keywords filters `pdp-type-info-ie` and `data-vol-report-ind-ie` provide the operator with the option to enable or disable the sending of either "PDP Type Information IE" or "Data Volume Reporting Indication IE" in the request for modification of the RAB Assignment Request procedure. RAB Assignment Request modification is configured per RNC under IuPS-Service configuration mode.

```
configure
  context context_name
    iups-service iups_service_name
      rnc id rnc_id
        default rab-modify-procedure
        no rab-modify-procedure normal-modify [ data-vol-report-ind-ie | pdp-type-info-ie ]
    end
```

Notes:

- `normal-modify` selects the normal modification procedure for RAB assignment. Either one of two IE options can be included:
  - `data-vol-report-ind-ie` sends the “Data Volume Reporting Indication IE” as part of the modification request of the RAB Assignment Request procedure.
  - `pdp-type-info-ie` sends the "PDP Type Information IE" as part of the modification request of the RAB Assignment Request procedure.

- The command can be repeated to configure first one IE and then the second IE

- `default` prefix added to the command, resets the configuration to use `release-an-establish`, the SGSN’s default RAB Assignment modification procedure.
• no prefix added to the command has a different effect depending if a keyword option is included:
  • no rab-modify-procedure normal-modify disables a previously configured normal modify procedure and sets the configuration to use the default RAB Assignment modification procedure (i.e.: release-an-establish).
  • no rab-modify-procedure normal-modify data-vol-report-ind-ie changes the configuration to disable sending "Data Volume Reporting Indication IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (i.e.: normal-modify).
  • no rab-modify-procedure normal-modify pdp-type-info-ie changes the configuration to disable sending "PDP Type Information IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (i.e.: normal-modify).

Performance Indicator Changes

show configuration verbose

Two new fields have been added to indicate if IEs have never been enabled in the configuration:
  • no pdp-type-info-ie
  • no data-vol-report-ind-ie

New fields have been added to indicate if the IEs have been enabled:
  • rab-modify-procedure normal-modify pdp-type-info-ie
  • rab-modify-procedure normal-modify data-vol-report-ind-ie

Display the IEs are disabled. Note that ‘normal modify’ remains enabled:
  • no rab-modify-procedure normal-modify pdp-type-info-ie
  • no rab-modify-procedure normal-modify data-vol-report-ind-ie

The following is a sample of a possible display that shows the IEs enabled for RNC 250, the IEs have been disabled for RNC 235, and the default modification procedure is configured for RNC 257:

[local]asr5000# show configuration verbose
config
..............
iups-service iups1
rnc id 250
default direct-tunnel
default rab-asymmetry-indicator
rab-modify-procedure normal-modify pdp-type-info-ie
rab-modify-procedure normal-modify data-vol-report-ind-ie
ranap signalling-indication-ie rab-assignment-request relocation-request

rnc id 235

default direct-tunnel
default rab-asymmetry-indicator
rab-modify-procedure normal-modify
no rab-modify-procedure normal-modify pdp-type-info-ie
no rab-modify-procedure normal-modify data-vol-report-ind-ie
ranap signalling-indication-ie rab-assignment-request relocation-request

rnc id 257

show iups-service

Two new fields have been added to the ‘Rab Modify Procedure’ section of the output of this command to indicate if these two IEs have been configured for sending. The following indicates that PDP Type Information IE *is enabled* and that Data Volume Report Indication *is not enabled*:

- **PDP Type Information** : IE is included in RAB Modify
- **Data Volume Report Indication** : IE is not included in RAB Modify
SGSN Enhancements for 16.4

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 *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

---

**CSCur07639 - Multiple SESSMGR crash of same kind after upgrade to 16.2.0**

**Feature Changes**

**Handling 2G Power-off Detach Requests**

- **Previous Behavior:** During Inter-RAT at 2G, a 2G power-off detach request received from different RAI is always posted to 3G.
- **New Behavior:** During Inter-RAT from 3G to 2G, a 2G power-off detach request received from different RAI is processed by 2G.
- **Customer Impact:** Session Manager crashes do not occur in the above mentioned scenario.
CSCur57064 - Intra-SRNS SGSN to send ULI to GGSN, with valid PLMN, LAC, SAC

Feature Changes

ULI contains valid SAI information with PLMN, LAC and SAC

**Previous Behavior:** During Intra-SRNS, the SGSN does not include ULI information until the location information is updated by the MS in the UPCQ.

**New Behavior:** During Intra-SRNS, the SGSN now includes the "LOCATION TYPE" as SAI with a valid LAC and SAC in the ULI field of UPCQ.

**Customer Impact:** The SGSN updates the User Location Information of the MS via UPCQ during Intra-SRNS based on the availability, this information can be used by the operator for billing.

CSCur57085 - Inter-SRNS SGSN to send ULI to GGSN, with valid LAC and SAC=0

Feature Changes

ULI to GGSN contains valid LAC and SAC

**Previous Behavior:** During Intra-SRNS, the SGSN does not include ULI information until the location information is updated by the MS in the UPCQ.

**New Behavior:** During Intra-SRNS, the SGSN now includes LOCATION TYPE as SAI with a valid LAC and "SAC = 0" in the ULI field of initial UPCQ.

**Customer Impact:** The SGSN updates the User Location Information of the MS via UPCQ during Intra-SRNS based on the availability, this information can be used by the operator for billing.

CSCur74184 - Global CN-ID should be sent in DirectInformationTransfer RIM with Iuflex

Feature Changes

Including Global CN-ID in RANAP-RIM messages

When Iu-flex is activated, some RNCs may expect RIM information, issued by the SGSN, to include the Global CN-ID.

**Previous Behavior:** The SGSN does not include the Global CN-ID IE in the RANAP Direct Information Transfer message to the RNC.

**New Behavior:** When an RNC is configured as "pooled" as part of the SGSN’s IuPS Service configuration, then the SGSN includes the configured core network ID as the Global CN-ID IE in the RANAP Direct Information Transfer RIM messages towards the RNC.
CSCus52926 - SM Cause codes behavior Change after REL16.0 upgrade

Feature Changes

DNS Failure and DNS Timeout Cause Codes Updated

**Previous Behavior:** Both DNS failure and DNS timeout reject activation with Cause Code “(31) Activation rejected, unspecified”.

**New Behavior:** The Cause Codes for DNS failure and DNS timeout have been updated as follows:

- DNS timeout : (34) Service option temporarily out of order
- DNS failure : (27) Missing or unknown APN
SGSN Enhancements for 16.3

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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

---

**CSCup77395 - Assert - sn_dp_utran_process_purge_req_evt()**

**Feature Changes**

**Intra SGSN SRNS Aborted**

Intra SGSN SRNS are aborted at the PMM level if there are no active RABs.

**Previous Behavior:** Intra SGSN SRNS continues even if there are no active RAB at the SM level.

**New Behavior:** Intra SGSN SRNS is aborted if there are no RABs at the SM level.
CSCuq42759 - Handle 2g attach request with same Random-TLLI

Feature Changes

Additional NSEI Check for Attach Requests

**Previous Behavior:** The SGSN drops the Attach Request received with the Random-TLLI which is already in use.

**New Behavior:** The SGSN can now process the ATTACH-REQUEST message received with the Random-TLLI which is already in use as long as this request comes from a different NSEI. If this feature enhancement is configured, only one ATTACH is processed by SGSN with the same Random-TLLI. A new CLI keyword `only-on-same-nsei` is included in the command `gmm-message attach-with-tlli-in-use` under the SGSN global configuration mode. By enabling this configuration the SGSN can process the ATTACH-REQUEST message from different MS using the TLLI which was already existing in the SGSN and used by other MS to Attach. If the second attach arrives from the same MS and same Random-TLLI which was used earlier to attach it will be processed by the SGSN after an additional check to ensure this attach is coming from a different NSEI. This feature enhancement is disabled by default.

Command Changes

`gmm-message attach-with-tlli-in-use`

A new optional keyword `only-on-same-nsei` is introduced in the command `gmm-message attach-with-tlli-in-use` under the SGSN global configuration mode. If this keyword is configured the SGSN can discard/drop the ATTACH-REQUEST message received with the Random-TLLI which is already in use by additionally validating NSEI. Attach gets processed if the attach is coming from different NSEI. This keyword is disabled by default.

```plaintext
configure
  sgsn-global
    [ default ] gmm-message attach-with-tlli-in-use { discard-message [only-on-same-nsei] }
end
```

CSCuq43024 - SGSN write corrupted APN to its HLR cache after sending error to HLR

Feature Changes

Subscription Data Updated to the Database

**Previous Behavior:** The subscription data received from ISD is stored in a cache allocated by the SGSN before it is updated in the db. The information in the cache is updated in the db after a response is sent to the ISD. If the ISD is rejected with an error message, this cache is not cleared. The cache holds the partial data from the ISD and this partial data gets incorrectly updated in the db.

**New Behavior:** The issue is now resolved and only valid data is updated in the db.
CSCuq96834 - [Smoke2] UBR should not be rejected in this scenario

Feature Changes

A Default EPS Bearer is a Non-GBR Bearer

**Previous Behavior:** The Update Bearer Request is honoured if there is a change of default bearer to be a GBR bearer.

**New Behavior:** As per 3GPP TS 24.301 “A default EPS bearer is a non-GBR bearer”. If in an Update Bearer Request there is a request for the default bearer to be a GBR bearer then the Update Bearer Request is rejected.
SGSN Enhancements for 16.2

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
- GTPPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

CSCty13075 - PGW & SGW local address fallback-for-dns not working

**Feature Changes**

**Support for PGW and SGW Fallback for DNS Address**

**Previous Behavior**: The pgw-address configured under the apn-profile is treated as the local address when address-resolution-mode is configured as local. This address is always used instead of doing DNS Query. The SGW address configured under tai-mgmt-object in lte-policy is used for local address instead of doing DNS query.

**New Behavior**: The locally configured pgw-address will be treated as local or fallback-for-dns address based on configured address-resolution-mode under apn-profile. The SGW address configured under tai-mgmt-object in lte-policy will be treated as local or fallback-for-dns address based on configured sgw-address-resolution-mode (configured as local or fallback for dns). Activation is not rejected after PGW and SGW DNS Failure, if fallback-for-dns address is configured.
Command Changes

sgw-address-resolution-mode

This command is introduced to specify the address resolution mode of the SGW address(s) configured in the LTE Tracking Area Identifiers Management object for the TAI database. This command is applicable only for S4-SGSN.

configure
lte-policy
tai-mgmt-db db_name
tai-mgmt-obj obj_name
  sgw-address-resolution-mode { fallback-for-dns | local }
end

Notes:
- This command is used to specify the DNS query or local address resolution for this LTE TAI Management Object. The addresses will be valid only for lac and rac defined under tai-mgmt-object.
- By default the option fallback-for-dns is enabled.

address-resolution-mode

This command identifies the address resolution mode for an APN profile. This command is now supported for S4-SGSN. In releases prior to 16.2, this command was supported only for Gn- SGSN.

configure
apn-profile profile_name
  address-resolution-mode { fallback-for-dns | local }
  default address-resolution-mode
end

Notes:
- The keyword fallback-for-dns instructs the system to try DNS resolution. If the DNS query fails, the SGSN uses the locally configured addresses, if they have been configured. The pgw-address configured under apn-profile will be treated as fallback for dns address and will used only after DNS failure.
- This address will be used on DNS SNAPTR Failure except on Service parameter mismatch.
- If pgw-address-resolution-mode fallback-for-dns is not configured then the gateway-address will be treated as fallback for DNS address and UE will fallback to Gn-SGSN, if GPRS-Subscription is available.
CSCud55490, CSCup57547 - sm cause ‘Network Failure’ should not be sent in Pri/Sec Act. rej.

Feature Changes

Gn-SGSN SM Cause Code Changes

The change of behavior involves the SGSN sending a different SM cause code in Activate Reject for the identified scenarios; a cause code deemed more appropriate as the problem could be a temporary condition related to the GGSN not being reachable.

**Previous Behavior:** SM cause code sent in specific scenario - please refer to table below.

**New Behavior:** Different SM cause codes to be sent for the specified scenarios - please refer to table below

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old Code</th>
<th>New Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPC Response Timeout</td>
<td>activation rejected, unspecified(31)</td>
<td>service option temporarily out of order(34)</td>
</tr>
<tr>
<td>DNS Response Failure</td>
<td>missing or unknown APN(27)</td>
<td>activation rejected, unspecified(31)</td>
</tr>
<tr>
<td>CPC Response Failure with GTP cause &quot;System Failure&quot;</td>
<td>activation rejected, unspecified(31)</td>
<td>activation rejected by GGSN, Serving GW or PDN GW(30)</td>
</tr>
<tr>
<td>UPC Failure Response with GTP cause &quot;System Failure&quot; for Direct Tunnel UPCQ</td>
<td>activation rejected, unspecified(31)</td>
<td>activation rejected by GGSN, Serving GW or PDN GW(30)</td>
</tr>
</tbody>
</table>

CSCuj33259 - Attach not processed when ISRAU is in progress

Feature Changes

Handling of foreign PTMSI

**Previous Behavior:** If foreign PTMSI attach arrives when the GTP response is in pending state, the attach is not being honored.

**New Behavior:** If foreign PTMSI attach arrives when the GTP response is in pending state, an Identity request will be triggered towards the MS to obtain the IMSI.
CSCuo62141, CSCuo79732, CSCuo56933 - Remove SGSN Application code for Fast Path

Feature Changes

NPU FastPath Feature Not Supported

**Previous Behavior:** The SGSN supports the NPU FastPath feature.

**New Behavior:** The SGSN no longer supports the NPU FastPath feature. All the configuration commands and performance indicators related to the NPU FastPath feature are deprecated to support this change. The FastPath feature is not supported by any product from this release onwards.

Command Changes

**gtpu fast-path**

This command under the Call Control Configuration Profile enables or disables the NPU FastPath feature, NPU FastPath feature is no longer supported therefore this command is deprecated from this software release.

**clear sgsn-fast-path statistics all**

This command clears information related to NPU FastPath feature, this command is deprecated as NPU FastPath feature is no longer supported.

**show sgsn-fast-path statistics all**

This command displays information related to SGSN FastPath, the command is now deprecated as the FastPath feature is not supported from this software release.

Performance Indicator Changes

**show subscribers { sgsn-only | gprs-only } full all**

The following counter is deprecated from this software release:

- Fast Path

**show subscribers sgsn-only summary**

The following counter is deprecated from this software release:

- PDP ctxs with fast path

**show call-control-profile full name**

The following counter is deprecated from this software release:

- GTPU Fast Path
CSCuo86321- Issue with show subscriber and clear subscriber

Feature Changes

Evaluation of Idle time

**Previous Behavior:** The evaluation of idle time in show subscriber and clear subscriber CLI commands is based on MM signalling.

**New Behavior:** The evaluation of idle time in show subscriber and clear subscriber CLI commands is now based on data session idle time of the subscriber.

**Customer Impact:** The show subscriber and clear subscriber CLI commands with idle time will now work on data session idle time.

CSCuo87321- Notify PGW of modified QoS after negotiation with RNC

Feature Changes

Notify PGW of Modified QoS After Negotiation With RNC

**Previous Behavior:** During PDP context activation if the RNC downgrades the QoS in RAB Assignment Response, the S4-SGSN rejects the PDP with cause "Insufficient Resources". The 3GPP standards does not permit QoS renegotiation by RAN in EPC. The S4-SGSN is considered as an EPC Node and when it cannot allocate the PCRF-assigned QoS due to RAN or UE capabilities, it rejects the PDP Creation Request. The S4-SGSN supports local QoS capping (up to UE/RNC capabilities) to at-least allow PDP creation in this scenario, however this behavior is not permissible as it may lead to potential overcharging due to difference in maximum-bit-rates as enforced by PGW and as allowed by RAN.

**New Behavior:** The issue is resolved by informing capped QoS to PGW/PCRF using the Modify Bearer Command to modify the APN-AMBR at the PGW. A new CLI option `inform-pgw` is provided for the command `qos-modification` under the SGSN Service configuration command to enable or disable sending of Modify Bearer Command to the PGW. By default this option is disabled. When this option is enabled, the S4-SGSN triggers a Modify Bearer Command if QoS is downgraded by the RNC in RAB Assignment Procedure. To avoid looping of messages between S4-SGSN and PGW, The PCRF should be configured to "NOT" upgrade QoS when RAT-Type is 3G.

Command Changes

**qos-modification**

The `qos-modification` command under the SGSN Service Configuration mode provides the operator with the flexibility to control RAB setup and negotiations based on the RNC. If the keyword `allow-s4-rab-negotiation` is specified as a part of the configuration and if the S4 interface is used for PDP activation then the SGSN locally accepts what the RNC sends as QoS in the RAB Assignment Response and sends that QoS in the Activate Response. A new keyword `inform-pgw` is included as a part of the `allow-s4-rab-negotiation` CLI option. This CLI option is used to enable or disable sending of Modify Bearer Command to the PGW. By default this option is disabled. When this option is enabled, the S4-SGSN triggers a Modify Bearer Command if QoS is downgraded by the RNC in RAB Assignment Procedure. The PCRF should be configured to “NOT” upgrade QoS when RAT-Type is 3G.
SGSN Changes in Release 16

SGSN Enhancements for 16.2

CSCup49664 - [Intracer] Require 1-to-1 mapping for ipms-suppress and no ipms-suppress

Feature Changes

Handling of IPMS Suppress Command

Previous Behavior: The command `ipms-suppress` is configured to suppress or allow the IPMS-event reporting to Intracer for the specified RAT. In the current implementation at a time only one service (either gprs or umts service) related ipms event reporting to the Intracer server (IPMS server) can be suppressed using the CLI command, provided there is a valid IPMS-context and server address.

When the command `no ipms-suppress [gprs | umts]` is configured then regardless of the service provided the suppression enabled on the service (configured through `ipms-suppress [gprs | umts]`) will be disabled. There is no one-to-one mapping of the `ipms-suppress` and `no ipms-suppress` commands.

New Behavior: The implementation of the `ipms-suppress` command is now changed, ipms suppression can be enabled on both the services (GPRS and UMTS service) at the same time. This provides independent control on the suppression of ipms-events from the GPRS and UMTS services.

Customer Impact: The customer can experience improved CLI control for better handling of the traffic or congestion over the network.

CSCup94785, CSCuq34454 - QOS management for uplink data messages in 2G

Feature Changes

ARP-RP Mapping for Radio Priority in Messages

Previous Behavior: Radio priority was hardcoded to 4 irrespective of ARP values received by the SGSN from either a GGSN or an HLR. No mapping CLI existed for ARP and RP values in the SGSN configuration so radio priority of 4 was sent in the following downlink signaling messages:

- Activate PDP Accept.
- Modify PDP Request during network initiated PDP modification procedure.
- Modify PDP Accept during MS initiated PDP modification procedure provided the ARP has been changed by the network.
New Behavior: New configuration commands available in this release

- First, create profiles for mapping ARP to RP values, and
- Second, associate the mapping with SGSN (3G) and GPRS (2G) services.

Using the ARP to RP mapping, the SGSN can choose a preferred radio priority according to the ARP values sent by the GGSN and HLR. As well, these mappings will be used by corresponding 2G and/or 3G services to choose the radio priority value while triggering messages (such as those listed below) towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.
- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

Command Changes

`qos-arp-rp-map-profile`

This new command, in the SGSN Global configuration mode, creates an ARP-RP mapping profile.

```
configure
sgsn-global

qos-arp-rp-map-profile arp_profile_name

no qos-arp-rp-map-profile arp_profile_name

end
```

Notes:

- `arp_profile_name` - Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode.
- `no qos-arp-rp-map-profile` - Removes the profile definition from the configuration.

`arp`

When the ARP-RP mapping profile is created, default ARP-RP mapping is automatically included (see default values in the Notes section below). This `arp` command, in the ARP-RP mapping profile configuration mode, modifies the ARP-RP mapping for the profile.

```
configure
sgsn-global

qos-arp-rp-map-profile arp_profile_name

arp arp_value radio-priority rp_value

end
```

Notes:
• **arp_value** - Defines the allocation retention priority. Enter an integer from 1 to 3.

• **rp_value** - Defines the radio priority. Enter an integer from 1 to 4.

Default ARP-RP mapping would be

- ARP1 RP4
- ARP2 RP4
- ARP3 RP4

• Use the `show sgsn-mode` command to display the ARP-RP profile and configuration.

### sm radio-priority

The `radio-priority` keyword is new in the `sm` commands in both the GPRS-Service and SGSN-Service configuration modes. This new keyword is used to associate an ARP-RP mapping profile with a 2G and/or a 3G service.

**configure**

```plaintext
context context_name

gprs-service service_name

  sm radio-priority from-arp arp_profile_name

no sm radio-priority from-arp arp_profile_name

end
```

**Notes:**

• This example illustrates the GPRS Service configuration mode, but either GPRS or SGSN Service configuration modes could be entered. The command sequent would have to be repeated, once for each type of service, to associate the ARP-RP profile with both types of services.

• **no sm radio-priority from-arp** - This command will remove the association from the configuration.

• Use the `show configuration` command to display the association.
SGSN Enhancements for 16.1

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

---

**CSCtn15437, CSCuo37725 - InTracer Support of SGSN - New requirement**

### Feature Changes

**Intracer Support For 2G Calls**

The IPMS (Intelligent Packet Monitoring System) solution provides a framework for operators to analyze and investigate call related events for various platforms. The signaling messages related to 2G calls on SGSN are traced through the IPMS. These include the message exchanges between SGSN and other peer entities like GGSN, HLR, EIR and BSC.

A client server mechanism is implemented, where the IPMS client runs on the SGSN and copies the signaling packets related to a 2G subscriber and then ships them to the IPMS server. This data can be used by operators in numerous ways including debugging. Some identities like the IMSI, MSISDN, IMEI, APN, PDP addresses that are sent to the IPMS server as and when they are learnt by the SGSN as standalone messages (TLVs) without any PDU. For example, during a PTMSI attach procedure after the identity response from MS, the SGSN learns about the subscriber's IMSI and...
communicates this identity with the IPMS server in the form a standalone IPMS message with IMSI TLV in it. The different identities of MS are learned by SGSN during a call in several signaling message.

Intracer support for 2G calls re-uses the same framework implemented for 3G calls in the previous release. An increase in the call-processing time is observed as the activities like duplicating the signaling PDU, generating the TLVs, constructing the IPMS event and packet, and shipping it to IPMS server are done on every signaling message.

**Command Changes**

**ipms-suppress**

The new command `ipms-suppress` is configured to suppress or allow the IPMS-event reporting to Intracer for the specified RAT. This CLI command helps the operator to change the IPMS-event reporting and manage network load or congestion on the fly.

```plaintext
configure
  sgsn-global
    ipms-suppress [gprs | umts]
    no ipms-suppress [gprs | umts]
  end
```

Notes:

- At a time only service (either gprs or umts service) related ipms event reporting to the Intracer server (IPMS server) can be suppressed using the CLI command, provided there is a valid IPMS-context and server address.
- When `no ipms-suppress [gprs | umts]` is configured then regardless of the service provided the suppression enabled on the service (configured through `ipms-suppress [gprs | umts]`) will be disabled. There is no one-to-one mapping of the `ipms-suppress` and `no ipms-suppress`.

  For example, if ipms-suppress on gprs is configured using the command `ipms-suppress gprs`. To remove ipms suppress, either of the commands `no ipms-suppress gprs` or `no ipms-suppress umts` can be used. However the command `no ipms-suppress gprs` is recommended in such a scenario.
- By default the IPMS event reporting will be done by both the services, provided there is a valid IPMS-context and IPMS-server configured.

**Performance Indicator Changes**

**show ipms status**

The show command `show ipms status [all | server address]` is executed to verify Intracer support for 2G calls, on executing the command the following parameters are displayed:

- BSSGP msg
- LLC msg
- 2G GMM/SM msg
CSCuj62285 - IP tcp mss settings on sgsn

Feature Changes

Making TCP MSS Configurable

**Previous Behavior:** The SGSN transparently passed the maximum segment size (MSS for TCP uplink/downlink traffic) in TCP SYN (and SYN-ACK) messages between UE and the server. In cases where the MSS value exchanged between UE and server is 1460 or more, with the addition of the GTP header, the packets often would be fragmented, which resulted in packets being dropped by network nodes that could not handle fragmentation.

**New Behavior:** To avoid fragmentation, the SGSN can now be configured to modify/overwrite the TCP MSS value exchanged between the UE and the server (for both 2G and 3G uplink/downlink traffic) if the requested value is more than the SGSN's locally configured value.

Command Changes

```
tcp-maximum-segment-size
```

This new command in the Call Control Profile configuration mode enables the operator to define a maximum segment size (MSS), that will be used to overwrite received TCP MSS values in uplink/downlink packets between UE to the server.

```
call-control-profile profile_name
    tcp-maximum-segment-size size
    remove tcp-maximum-segment-size
end
```

Notes:

- `size` - is the maximum number of octets for a segment, value range is 1 to 1460.
- `remove` - as part of the command, returns the MSS to the SGSN’s default of 1460 octets.
- An additional Yes/No prompt is included due to the high impact of the MSS configuration.

CSCun89389 - [16.0] Discrepancy in modify bearer req in rau from pre r7 and r7 rnc

Feature Changes

Delete Bearer Command Behavior

**Previous Behavior:** Consider the following scenario:

1. ISRAU in 3G from pre-release 7 RNC (No SGW change).
2. Context response with one default and dedicated bearer with APNAMBR as 20 Mbps and Bearer QoS 18 Mbps.
3. Authentication and Security procedures are completed.
4. Modify bearer request with context to be modified for default bearer and context to be removed for dedicated bearer.

The dedicated bearer is sent as “bearer to be removed” and PDP status is sent as Inactive in RAU accept. Delete Bearer Command was not sent to SGW after MBR response received.

New Behavior: The Delete Bearer command will be triggered whenever the GBR bearer is sent as “bearer to be removed” in Create Session Request / Modify Bearer Request.

CSCuo62754 - Assertion failure at sess/sgsn/sgsn-app/db/sgsn_db_pmm.c:1880

Feature Changes

Ready Timer During Attach/RAU

Previous Behavior: The Ready timer can expiry during ongoing Attach/RAU procedures.

New Behavior: Fix ensures that ready timer will not expire during ongoing Attach/RAU procedures.

CSCuo94954 - QvPC-SI platform support

Feature Changes

QvPC-SI platform support qualified on SGSN

SGSN Functionality on the QvPC-SI Platform

All 2G and 3G SGSN features and functions provided on the ASR 5000 and ASR 5500 for IP interfaces are now fully supported on the QvPC-SI platform, with the exception of FastPath and Narrowband SS7.

Previous Behavior: The QvPC-SI platform support on SGSN was not qualified in earlier software releases.

New Behavior: From this release onwards the QvPC-SI platform support on SGSN is qualified.

Customer Impact: QvPC-SI support for SGSN available for deployment post qualification.

Command Changes

Commands Not Supported by SGSN on ASR 5500

The QvPC-SI platform does not support either a Frame Relay or an ATM line card or Narrowband SS7 functionality, the following commands and/or keywords are not supported by the SGSN on the QvPC-SI platform:

- all commands in the ATM Port configuration mode
- all commands in the BITS Port configuration mode
- aps command, Card configuration mode
- sdh and sonet keywords of the framing command, Card configuration mode.
• header-type command, Card configuration mode
• initial-el-framing command, Card configuration mode
• service-type command, Card configuration mode
• all commands in the Channelized Port configuration mode
• all commands in the DLCI configuration mode
• fr filter for the nse keyword of the sgsn op command in the Exec mode
• dlci-utilization keyword for the show linecard command in the Exec mode
• fr-config keyword for the show network-service-entity command in the Exec mode
• peer-nsei and frame-relay keywords for the network-service-entity command in the Global configuration mode
• port atm command in the Global configuration mode
• port channelized command in the Global configuration mode
• mtp2-aerm-emergency-threshold command in the Link configuration mode
• mtp2-aerm-normal-threshold command in the Link configuration mode
• mtp2-eim-decrement command in the Link configuration mode
• mtp2-eim-increment command in the Link configuration mode
• mtp2-eim-threshold command in the Link configuration mode
• mtp2-error-correction command in the Link configuration mode
• mtp2-lssu-len command in the Link configuration mode
• mtp2-max-outstand-frames command in the Link configuration mode
• mtp2-suerm-threshold command in the Link configuration mode
• mtp3-msg-size command in the Link configuration mode
• sscf-nni-n1 command in the Link configuration mode
• sscop-max-cc command in the Link configuration mode
• sscop-max-pd command in the Link configuration mode
• sscop-max-stat command in the Link configuration mode
• timeout command in the Link configuration mode
• link-type keyword for the link command in the Linkset configuration mode
• all commands in the Network Service Entity - Peer NSEI configuration mode
• all commands in the NSVC configuration mode
• all commands in the PVC configuration mode
SGSN Enhancements for 16.0

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

---

**CSCtr31994 - [S4-SGSN] RIM message should be supported over S16 and S3 interface**

**Feature Changes**

**RIM over S3 and S16 Interfaces**

RAN Information Management (RIM) procedures facilitate the exchange of information between two BSC/RNC in support of Network Assisted Cell Change (NACC) across cells which are not part of the same BSC/RNC. Network assisted cell change improves the user experience during cell re-selection by reducing service outage duration.

**Previous Behavior:** The SGSN currently supports RIM over GTPv1.

**New Behavior:** In an MPC/EPC network, NACC is needed for transfer of radio context to target nodes during CSFB so that the CSFB call handovers are quick. For the S4-SGSN, RIM and NACC support now extend to the S3 and S16 interfaces using GTPv2 protocol by default. This functionality requires the SGSN S3/S4 license.
Use existing CLI to enable this functionality, use the `ran-information-management` commands in both the RNC configuration mode and the SGSN Global configuration mode. Use of GTPv2 is determined by configuring the EGTP service and use of GTPv1 is determined by configuring the SGTP service and then associating the EGTP or SGTP service configuration with the SGSN service configuration and/or the GPRS service configuration.

Currently, eGTPv2 stats are not available for GTPv2 RIM messages.

**Customer Impact:** This feature enables faster handover, which is especially critical in CFSB scenarios for faster voice call setup.

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

### Feature Changes

#### 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.

```plaintext
call-control-profile ccprofile_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-network | uli }` selects the type of information element (IE) the PLMN information is added to.
- **use-common-plmn** instructs the SGSN to identify the Common PLMN for the shared network.
- **use-selected-plmn** instructs the SGSN to identify the Selected PLMN for the shared network.
- **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.

**CSCts57950, CSCud49814, CSCuj06828 - Configurable Cause code mapping**

**Feature Changes**

**Mapping Preferred GMM Cause Codes**

**Previous Behavior:** The operator can map a preferred GMM reject cause code for the SGSN to send to a UE in place of MAP cause ‘roaming not allowed’ for MAP failures and and map a preferred GMM reject cause code to be sent in a RAU Reject for inbound peer SGSN address resolution failures.

**New Behavior:** With this release, additional cause code mappings are allowed to:

- Mapping GSM-MAP cause code “unknown-subscriber” to GMM cause code “gprs-service-not-allowed” if a response message comes without diagnostic information.
- Mapping GSM-MAP cause code “unknown-subscriber” with diagnostic information indicating “gprs-subscription-unknown” to a preferred GMM cause code.
- Mapping GSM-MAP cause code “unknown-subscriber” with diagnostic information indicating “imsi-unknown” to a preferred GMM cause code.
- Override the GMM cause sent to the MS in a RAU Reject during context transfer failure.
- Override the cause sent in a Deactivate Request, to an MS, due to the GGSN becoming unreachable.
- Mapping an SM cause code for Deactivate PDP Requests during a path failure towards the GGSN.

**Command Changes**

```
local-cause-code-mapping map-cause-code
```

New keyword `unknown-subscriber` configures the SGSN to include a preferred GMM cause code, in Reject messages to the UE, in place of MAP failure cause 'unknown-subscriber' for MAP failures and inbound RAU context transfer failures. Optionally, the Operator can map a specific GMM cause code if the SGSN receives additional MAP failure diagnostic information.

```
configure

   call-control-profile profile_name

       local-cause-code-mapping map-cause-code { roaming-not-allowed gmm-cause-code gmm_cause | unknown-subscriber { gmm-cause-code gmm_cause | map-diag-info { gprs-subscription-unknown gmm-cause-code gmm_cause | imsi-unknown gmm-cause-code gmm_cause } } }

       remove local-cause-code-mapping map-cause-code { roaming-not-allowed | unknown-subscriber { gmm-cause-code | map-diag-info { gprs-subscription-unknown | imsi-unknown } } }

   end
```

Notes:

- `unknown-subscriber` Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE’s access request is rejected due to map cause ‘unknown-subscriber’.
- `gmm-cause-code gmm_cause` identifies the replacement GMM cause code; options include:
  - gprs-serv-and-non-gprs-serv-not-allowed
  - gprs-serv-not-allowed
  - gprs-serv-not-in-this-plmn
  - location-area-not-allowed
  - network-failure
  - no-suitable-cell-in-this-la
  - plmn-not-allowed
  - roaming-not-allowed-in-this-la
SGSN Changes in Release 16

- map-diag-info gprs-subscription-unknown gmm-cause-code gmm_cause identifies a replacement GMM cause code if additional ‘gprs-subscription-unknown’ diagnostic MAP failure information is received when the UE’s access request is rejected due to map cause ‘unknown-subscriber’.

- map-diag-infoimsi-unknown gmm-cause-code gmm_cause identifies a replacement GMM cause code if additional ‘imsi-unknown’ diagnostic MAP failure information is received when the UE’s access request is rejected due to map cause ‘unknown-subscriber’.

- remove erases the mapping configuration.

rau-inter

There are two new command actions for the rau-inter command:

1. The new keyword ctxt-xfer-failure configures a GMM failure cause code to be sent in a RAU Reject to the UE due to context transfer failures.
2. The remove command filter has been added to the rau-inter command to work with the new ctxt-xfer-failure keyword and the already present peer-sgsn-addr-resolution-failure keyword.

configure

call-control-profile profile_name

rau-inter ctxt-xfer-failure failure-code fail_code
remove rau-inter ctxt-xfer-failure
remove rau-inter peer-sgsn-addr-resolution-failure

end

Notes:

- remove is supported for both ctxt-xfer-failure and peer-sgsn-addr-resolution-failure to erase defined configurations.
- fail_code enter value from 2 to 111 to identify the TS 124.008 GMM failure cause code for the ctxt-xfer-failure keyword.

local-cause-code-mapping path-failure

This new command configures SM cause codes to override the default cause codes sent in Deactivate PDP Request due to GTPC path failure.

configure

call-control-profile profile_name

local-cause-code-mapping path-failure sm-cause-code { insufficient-resources | network-failure | reactivation-requested | regular-deactivation }
remove local-cause-code-mapping path-failure

end

Notes:
- remove returns the configuration to the default “Not Configured”

Performance Indicator Changes

show call-control-profile full

The following fields, added to the output of this show command, have been added to indicate the configuration status of all of the newly supported cause code changes. Values indicated below are only examples:

- RAU Inter- Failure Code For Peer Sgsn Address Resolution: <value>
- RAU Inter- Failure Code For Context Transfer: <value>
- Mapped GMM Cause code for MAP cause Unknown Subscriber: Gprs Serv Not Allowed (7)
- MAP cause Unknown Subscriber with Diag Info Gprs Subscription Unknown: Gprs Serv Not Allowed in this PLMN (14)
- MAP cause Unknown Subscriber with Diag Info Imsi Unknown : Location Area Not Allowed (12)

CSCtx38089 - [S4-SGSN] UE-AMBR over RANAP messages shall be supported

Feature Changes

UE AMBR IE in RANAP Messages

New Behavior: It is now possible for the operator to configure, per RNC, the SGSN to include UE AMBR IE when sending RAB Assignment Request and Relocation Request RANAP messages.

Related Issues: CSCty42425, CSCty42433, CSCue32234,

Command Changes

ranap ue-ambr-ie

This new command allows the operator to determine if the UE AMBR IE is to be included when the SGSN sends RANAP messages of the type RAB Assignment Request and Relocation Request. This functionality can be enabled per RNC basis.

configure

custom context_name

iups-service service_name

rnc id rnc_id

[ no ] ranap ue-ambr-ie

end

Notes:
Performance Indicator Changes

show iups-service

A new field has been added to the output of the show iups-service name service_name:

- UE Aggregate Maximum Bit Rate

CSCtx38779 - RFSP from subscription or local policy to be supported

Feature Changes

S4-SGSN Support for RFSP from Subscription Or Local Policy

SGSN supports sending of the RAT/Frequency Selection Priority (RFSP ID) from subscription or a local overridden value towards RNC BSC. The RNC/BSC use the subscribed RFSP ID or locally overridden value at the SGSN to choose the Radio frequency. RANAP Direct transfer Extension, RANAP Common ID Extension and DL-Unitdata message will be encoded with RFSP ID. RFSP ID is sent in Common ID message to RNC. RFSP ID is sent in DL-Unitdata PDU and PS handover related messages to BSC.  

Previous Behavior: RFSP ID IE is not included in outbound messages to the RNC or BSC.

New Behavior: RFSP ID IE will be included in RANAP Direct transfer Extension and Common ID extn messages to RNC/BSC. RFSP ID will also be send in BSSGP DL-UNITDATA message.

New CLI key word `eutran-ho-restricted` value is introduced in the command `rfsp-override` under Call-Control Configuration Profile to configure the value for RAT frequency selection priority when Handover to EUTRAN is restricted. This value overrides the RFSP ID value sent by the HLR/HSS in an EPS subscription.

A new CLI command `ranap rfsp-id-ie` is introduced under the IuPS Service configuration mode to enable or disable the inclusion of the Subscriber Profile ID for RA/T/Frequency priority IE in RANAP Direct transfer Extension and Common Id. Extension messages.

A new CLI command `bssgp-message dl-unitdata` is introduced under the SGSN Global Configuration mode to exclude or include RAT/Frequency Selection Priority (RFSP ID) in BSSGP DL-Unitdata messages to the BSC.

Customer Impact: RANAP Direct transfer Extension, RANAP Common ID Extension and DL-Unitdata message are encoded with RFSP ID.

Command Changes

`rfsp-override`

This command configures the RAT frequency selection priority override parameters for this call control profile. A new keyword `eutran-ho-restricted` value has been introduced to configure the value for RAT frequency selection priority when Handover to EUTRAN is restricted.

```
cfg
  call-control profile profile_name
```
**SGSN Changes in Release 16**

**SGSN Enhancements for 16.0**

```bash
rfsp-overide { default value | eutran-ho-restricted value | ue-val value new-val value + } remove rfsp-overide { default | eutran-ho-restricted | ue-val value }
exit

ranap rfsp-id-ie

This command is introduced to enable or disable the inclusion of the Subscriber Profile ID for RAT/Frequency priority IE in RANAP Direct transfer Extension and Common Id. Extension messages.

cfg
context <context_name>
iups_service <service_name>
rnc id rnc_id
    ranap rfsp-id-ie
    no ranap rfsp-id-ie
exit

bssgp-message dl-unitdata rfsp-id exclude

Configure this command to exclude or include RAT/Frequency Selection Priority (RFSP ID) in BSSGP DL-Unitdata messages to the BSC.

cfg
sgsn-global
    bssgp-message dl-unitdata rfsp-id exclude
    default bssgp-message dl-unitdata rfsp-id exclude
exit

**Performance Indicator Changes**

**show call-control profile**

The following new field is added in the show output to display the configured value for RAT frequency selection priority when Handover to EUTRAN is restricted:

- Rfsp-overide eutran-ho-restricted

**show subscribers sgsn-only full all**

The following new field is added in the show output to display the value of the RFSD Id. Used:

- RFSP Id in Use
show subscribers gprs-only full all

The following new field is added in the show output to display the value of the RFSD Id. Used:

- RFSP Id in Use

show iups-service name

The following new field is added in the show output to display if the Subscriber Profile ID for RAT/Frequency priority IE is included or not in the outbound RANAP Direct transfer Extension and Common Id Extension message:

- RFSP ID

show sgsn-mode

The following new field is added in the show output to display if the RFSP ID is either included or excluded in BSSGP DL-Unitdata messages to the BSC:

- DL Unitdata Tx

CSCty34288, CSCuh28109 - Need enhancement on map statistics as to why SAI / UGL fails

Command Changes

Performance Indicator Changes

show map statistics

Additional MAP statistics have been added to provide clarity for SAI and UGL failures:

- System Failure: UnExpected Data Value:
- Unknown Subscriber: Roaming Not Allowed:

show map statistics

Additional MAP statistics have been added to provide tracksuit failures:

- SData Missing: UnExpected Data Value:
- Un-identified Subscriber:

CSCty42425 - [S4-SGSN] APN-AMBR override from local config shall be supported in 3G

Feature Changes

Capping APN AMBR Based on Local Configuration
For 3G subscribers, the operator can now cap the subscribed APN AMBR value with a change to the local configuration. Or, the operator can set the prefer-cap type.

**Related Issues:** CSCtx38089, CSCty42433, and CSCue32234

**Command Changes**

**qos**

Two existing keywords in the *qos* command will be used by the SGSN for this feature:

The first keyword, `apn-ambr`, is newly supported by the SGSN to enable the operator to configure the aggregate maximum bit rate per APN (APN-AMBR). The SGSN can send the capped APN AMBR in response to a QoS change in an activation init Create Session Request or a Modify Bearer Command message.

The second keyword, `prefer-as-cap`, enables the operator to configure preferred uplink and downlink QoS cap values.

```plaintext
configure
  apn-profile profile_name
    qos apn-ambr max-ul max_ul_value max-dl max_dl_value
    remove qos apn-ambr
    qos prefer-as-cap { both-hlr-and-local | hlr-subscription | local }
    remove qos prefer-as-cap
  end
```

**Notes:**
- `max-ul` defines the maximum bit rate for uplink traffic; range 0 to 1410065408.
- `max-dl` defines the maximum bit rate for downlink traffic; range 0 to 1410065408.
- `both-hlr-and-local` instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.
- `hlr-subscription` instructs the SGSN to use the HLR subscription for QoS capping.
- `local` use the locally configured QoS bit rate for QoS capping.
- `remove` erases the configuration from the APN profile.

**Performance Indicator Changes**

**show apn-profile**

In support of the new ability to configure UE AMBR, new fields have been added to the output of the `show apn-profile full name profile_name`

- Quality of Service Capping <Enabled/Disabled>
  - Prefer Type <selection>
- QOS UE-AMBR <Enabled/Disabled>
  - MAX uplink <value>
  - MAX downlink <value>

CSCty42433 - [S4-SGSN] APN-AMBR override from local config shall be supported in 2G

Feature Changes

Capping APN AMBR Based on Local Configuration

For 2G subscribers, the operator can now cap the subscribed APN AMBR value with a change to the local configuration. Or, the operator can set the prefer-cap type.

Related Issues: CSCtx38089, CSCty42425, and CSCue32234

Command Changes

```
qos
```

Two keywords are newly supported in the `qos` command.

The first new keyword, `apn-ambr`, enables the operator to configure the aggregate maximum bit rate per APN (APN-AMBR). The SGSN will send the capped APN AMBR in the activation init Create Session Request, Modify Bearer Command in case of a QoS change.

The second new keyword, `prefer-as-cap`, enables the operator to configure preferred uplink and downlink QoS cap values.

```
configure

apn-profile profile_name

qos apn-ambr max-ul max_ul_value max-dl max_dl_value

remove qos apn-ambr

qos prefer-as-cap { both-hlr-and-local | hlr-subscription | local }

remove qos prefer-as-cap

end
```

Notes:

- `max-ul` defines the maximum bit rate for uplink traffic; range 0 to 1410065408.
- `max-dl` defines the maximum bit rate for downlink traffic; range 0 to 1410065408.
- `both-hlr-and-local` instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.
• **hlr-subscription**  
  instructs the SGSN to use the HLR subscription for QoS capping.

• **local**  
  use the locally configured QoS bit rate for QoS capping.

• **remove**  
  erases the configuration from the APN profile.

**Performance Indicator Changes**

**show apn-profile**

In support of the new ability to configure UE AMBR, new fields have been added to the output of the `show apn-profile full name profile_name`

- Quality of Service Capping <Enabled/Disabled>
  - Prefer Type <selection>
- QOS UE-AMBR <Enabled/Disabled>
  - MAX uplink <value>
  - MAX downlink <value>

**CSCty44479 - APN Restriction on S4-SGSN**

**Feature Changes**

**APN Restriction Extended to S4-SGSN**

**Previous Behavior:** The Gn-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.
SGSN Changes in Release 16

CSCtz55422 - SGSN should start dns query for default SGSN when nri based query fails / Fallback to RAI based query when NRI based query fails

Feature Changes

SGSN Support for RAI Based Query

Previous Behavior: A DNS query with NRI is performed for ISRAU, Identification and Suspend Requests. Failure of the NRI based DNS query results in failure of the ISRAU, Identification and Suspend Requests. The SGSN does not support a RAI based query when NRI based query fails.

New Behavior: A new CLI option rai-fqdn-fallback is provided in the peer-nri-length CLI under the Call Control Profile Configuration, which allows the operator to configure the SGSN's support to fallback on RAI based query when NRI based query fails.

Command Changes

peer-nri-length

A new keyword rai-fqdn-fallback has been included in the peer-nri-length command, this keyword is configured to support RAI based query when NRI based query fails. This keyword is disabled by default.

configure

    call-control profile profile_name

    peer-nri-length length [rai-fqdn-fallback]

    remove peer-nri-length [rai-fqdn-fallback]

    end

Notes:

- 2G Context Request and Identification Request messages are not supported.
- S4 support of this extensions for all applicable scenarios is not supported.

CSCtz56555 - SGSN Disable GTPv0 for specific set of APNs

Feature Changes

Disable GTPv0 Fallback to Prevent Unnecessary Signaling

Previous Behavior: By default, the SGSN supports GTPv0 fallback and uses either GTPv1 or GTPv0. After exhausting all configured retry attempts for GTPv1, the SGSN retries the GTP-C Request using GTPv0. This fallback is conditional and is done only when the GTP version of a GGSN is unknown during the first attempt at activating a PDP context with the GGSN.
New Behavior: With this release, it is now possible for the operator to disable the GTPv0 fallback for requests to GGSNs of specific APNs. This function is configured under the APN profile and is applicable for GGSNs corresponding to that APN. If GTPv1 only is enabled in the APN profile, then the SGSN does not attempt fallback to GTPv0 (towards GGSNs corresponding to that APN) after all GTPv1 retries have been attempted. If more than one GGSN address is returned by the DNS server during activation, then the SGSN attempts activation with the next GGSN after exhausting all the GTPv1 retry attempts. If only one GGSN address is returned, then the SGSN rejects the activation after exhausting all the configured GTPv1 retries.

Customer Impact: This change enables the operator to prevent unnecessary signaling on the Gn/Gp interface in networks where all the GGSNs support GTPv1. For example, if all the home GGSNs in an operator’s network support GTPv1, then the unnecessary GTPv0 fallback can be avoided by enabling this feature for the APNs associated with home GGSNs.

Command Changes

\texttt{gn-gtp-version}

The new command \texttt{gn-gtp-version} with its \texttt{v1-only} extension, in the APN profile configuration mode, enables the operator to prevent the SGSN from attempting GTPv0 Requests for GGSNs associated with specified APNs so that the SGSN tries activation with the next available GGSN if the current GGSN does not respond after the GTPv1 Request retries fail.

\texttt{configure}

\begin{verbatim}
  apn-profile profile_name

  gn-gtp-version v1-only

  [ remove ] gn-gtp-version v1-only

  end
\end{verbatim}

Notes:

- \texttt{remove} used with the command erases a previous GTPv1 configuration and returns the SGSN configuration to the default value of Both GTPv1 and GTPv0.

Performance Indicator Changes

\texttt{show apn-profile}

A new field has been added to the output to indicate the current configuration for use of GTPv1 only or GTPv1 and GTPv0 for fallback.

- Gn GTP Version

\textbf{CSCtz83032 - NRI Based DNS Query for Inter Pool 2G requests}

Feature Changes

NRI-FQDN based DNS resolution for non-local RAI (2G subscribers)
The SGSN now supports use of NRI-RAI based address resolution which includes both local lookup as well as DNS Query for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the BSC where the subscriber originally attached. This feature was formerly supported only for 3G subscribers and is now extended to 2G subscribers. The command enables the SGSN to perform address resolution for peer SGSN with an NRI when an unknown PTMSI (Attach or RAU) comes from an SGSN outside the pool. The SGSN uses NRI-RAI based address resolution for the non-local RAIs for 2G subscribers in place of RAI based address resolution.

This functionality is applicable in situations for either inter- or intra-PLMN when the SGSN has not chosen a local NRI value (configured with SGSN Service commands) other than local-pool-rai or nb-rai. This means the RAI (outside pool but intra-PLMN) NRI length configured here will be applicable even for intra-PLMN with differently configured NRI lengths (different from the local pool). This functionality is not applicable to call control profiles with an associated MSIN range as ceprofile selection is not IMSI-based.

**Previous Behavior:** For a 2G new SGSN subscriber, old SGSN RAI based local lookup and RAI based DNS query is performed. For non-pooling scenarios the address look up based on RAI is correct. However, for pooling scenarios the NRI/RAI based lookup and DNS query should not be performed.

**New Behavior:** For 2G New SGSN subscriber if the command peer-nri-length is configured, the local look up for address will be NRI/RAI based. If the address is not found locally, a NRI/RAI based DNS A-Query or SNAPTR is performed.

### Command Changes

**peer-nri-length**

This command enables the SGSN to use NRI-FQDN-based DNS resolution for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the BSC where the subscriber originally attached. This command was formerly supported only for 3G subscribers and is now extended to 2G subscribers. The command enables the SGSN to perform DNS query with an NRI when RAU comes from an SGSN outside the pool. The SGSN uses NRI-FQDN-based DNS resolution for the non-local RAIs for 2G subscribers in place of RAI-FQDN-based DNS resolution.

```bash
configure
call-control profile profile_name
  peer-nri-length length [rai-fqdn-fallback]
  remove peer-nri-length [rai-fqdn-fallback]
end
```

**Notes:**

Fall back to RAI based query when NRI based query fails is not supported in the following scenarios:
- 2G Context Request and Identification Request are not supported.
- S4 support of this extension for all applicable scenarios are not supported.
CSCub16134 - Paging Load throttling

Feature Changes

Paging Load Throttling

The Page Throttling feature limits the number of paging messages going out of the SGSN. It provides flexibility and control to the operator who can now reduce the number of paging messages going out from the SGSN based on the network conditions. In some of the customer locations, the amount of paging messages initiated from the SGSN is very high due to the bad radio conditions. A higher number of paging messages results in the consumption of bandwidth in the network. This feature provides a configurable rate-limit, in which the paging message gets throttled at:

- Global level for both 2G and 3G accesses
- NSE level for 2G only
- RNC level for 3G only

This feature improves the bandwidth consumption on the radio interface.

Command Changes

interface

The `interface` command is used to configure the mapping between the RNC Id and the RNC name. The operator can configure the paging RLF template either by RNC name or RNC identifier.

```shell
config
    sgsn-global
        interface-management
            [ no ] interface { gb peer-nsei | iu peer-rnc } { name <value> | id <value> }
        exit
```

Notes:

The `no` form of the command removes the mapping and other configuration associated for the RNC paging-RLF-template configuration from the SGSN and resets the behavior to default for that RNC.

Example configurations:

```shell
[local]SGSN1# configure
[local]SGSN1(config)# sgsn-global
[local]SGSN1(config-sgsn-global)# interface-management
[local]SGSN1(config-sgsn-interface-mgmt)# interface iu peer-rnc id 250 name bng_rnc1
[local]SGSN1(config-sgsn-interface-mgmt)# end
```
[local] SGSN1#

paging-rlf-template

This command allows the SGSN to associate an RLF template either at the global level, which limits the paging messages initiated across both 2G (NSE level) and 3G (RNC level) access, or at the per entity level, which can be at either the RNC level for 3G access or at the NSE level for 2G access.

config

sgsn-global

interface-management

[ no ] paging-rlf-template { template-name <template-name> } { gb peer-nsei | iu peer-rnc } { name <value> | id <value> }

exit

Notes:
If there is no RLF template associated for a particular NSE/RNC, then the paging load is limited based on the associated global RLF template (if present). If there is no global RLF template is associated, then rate limiting is not applied on the paging load.

[local] SGSN1(config)# sgsn-global
[local] SGSN1(config-sgsn-global)# interface-management
[local] SGSN1(config-sgsn-interface-mgmt)# paging-rlf-template template-name rlf1
[local] SGSN1(config-sgsn-interface-mgmt)# end
[local] SGSN1#
[local] SGSN1# configure
[local] SGSN1(config)# sgsn-global
[local] SGSN1(config-sgsn-global)# interface-management
[local] SGSN1(config-sgsn-interface-mgmt)# paging-rlf-template template-name rlf2
gb peer-nsei id 1
[local] SGSN1(config-sgsn-interface-mgmt)# end
[local] SGSN1#
[local] SGSN1# configure
[local] SGSN1(config)# sgsn-global
[local] SGSN1(config-sgsn-global)# interface-management
[local] SGSN1(config-sgsn-interface-mgmt)# paging-rlf-template template-name rlf2
iu peer-rnc name bng_rnc1
[local]SGSN1(config-sgsn-interface-mgmt)# end

[local]SGSN1#

For more information on the CLI command, see Command Line Interface Reference.

The RLF template can be configured under the global configuration mode which provides the option to configure the message rate, burst size, threshold, and delay tolerance for throttling or rate limiting. To configure the RLF template see the Interface Management section of the Command Line Interface Reference.

Performance Indicator Changes

show configuration

Listed below are the parameters added for the Page Throttling feature:

- paging-rlf-template template-name
- paging-rlf-template template-name gb peer-nsei id
- paging-rlf-template template-name iu peer-rnc id
- interface iu peer-rnc id rnc_id name name

show sgsn-mode interface-mgmt-status

Listed below are the parameters added for the Page Throttling feature:

- Global Paging RLF template
- Paging RLF Template

show gmm-sm statistics verbose

The following new statistics are added in the show gmm-sm statistics verbose status command to support the Page Throttling feature:

- 3G Page Throttling statistics
- PS-Page-Req sent by RLF
- Ret-PS-Page-Req sent by RLF
- PS-Page-Req dropped by RLF
- Ret-PS-Page-Req dropped by RLF
- PS-Page-Req dropped due to no memory
- 2G Page Throttling statistics
- Paging Request sent out by RLF
- Total-Page-Req sent
- Ret-Total-Page-Req sent
- Page-Requests-LA
- Ret-Page-Requests-LA
CSCub16201, CSCub48329 - Support for QoS Upgrade from GGSN/PCRF

Feature Changes

Support for QoS Upgrade from GGSN/PCRF

The SGSN negotiates the Requested QoS with Subscribed QoS from HLR (the HLR Subscribed QoS can be over-ridden by the local configuration). The SGSN includes this Negotiated QoS in Create PDP Context Request and Update PDP Context Request messages to the GGSN, the negotiate QoS is capped to the Subscribed QoS and cannot exceed it. The “Upgrade QoS Supported” flag is not set, and the GGSN cannot negotiate a QoS higher than that sent by the SGSN.

This feature enables the functionality, where the SGSN can set the “Upgrade QoS Supported” flag within the common flags IE in Tunnel management messages, Create PDP Context Request and Update PDP Context Request messages. The SGSN accepts the QoS from GGSN in Create PDP Context Response, Update PDP Context Request/Response messages as the Negotiated QoS for the PDP session.

In a 3G scenario, if QoS is downgraded by the RNC then SGSN sets the “No QoS negotiation” flag in the common Flags IE of the corresponding Update PDP Context Request. The “QoS upgrade supported” flag is not set.

A new configuration CLI is provided under the APN Profile configuration mode to support the QoS upgrade feature. If this CLI is configured, the SGSN sets the “Upgrade QoS Supported” bit in the Common Flags IE in Create PDP Context
Request and Update PDP Context Request. The SGSN accepts the QoS from the GGSN in Create PDP Context Response, Update PDP Context Request/Response as the Negotiated QoS for the PDP session.

Command Changes

\texttt{qos allow-upgrade access-type}

This command is used to configure support for QoS upgrade from GGSN/PCRF:

\begin{verbatim}
config
  apn-profile <profile_name>
    qos allow-upgrade access-type \{ gprs | umts \}[ prefer-as-cap subscription ]
    remove qos allow-upgrade access-type \{ gprs | umts \}
exit
\end{verbatim}

Notes:
- The “Upgrade QoS Supported” flag is now set in “Create PDP Context” and “Update PDP Context” messages sent by SGSN. The SGSN signals the availability of this functionality by use of the “Upgrade QoS Supported” bit within the Common Flags IE. The SGSN sets the “Upgrade QoS Supported” bit within the Common Flags IE to “1” within the “Create PDP Context” and “Update PDP Context”
- If keyword \texttt{prefer-as-cap subscription} is enabled, SGSN accepts a higher QoS in the Create/Update PDP Context Response than sent in Create/Update PDP Context Request, but negotiates and restricts the value within HLR/local subscribed QoS. If this keyword is disabled, the SGSN accepts the QoS in Create PDP Context Response and Update PDP Context Response as the Negotiated QoS (this QoS may be downgraded by the RNC in case of UMTS access).

For more information on the command, see the \textit{Command Line Interface Reference}.

Performance Indicator Changes

\texttt{show apn-profile full name}

The configuration can be verified by executing the show command \texttt{show apn-profile full name <apn_profile_name>}. The following parameters are displayed on executing the command:

- Allow QoS Upgrade from GGSN
- QoS Upgrade From GGSN (UMTS)
- Capped with Subscribed QoS
- QoS Upgrade From GGSN (GPRS)
- Capped with Subscribed QoS

For description of the fields listed above see the \textit{Statistics and Counters Reference}. 
CSCub16578 - SNAPTR Queries for GGSN selection

Feature Changes

S-NAPTR Query Support for GGSN Selection

**Previous Behavior:** S-NAPTR queries were only supported by the S4-SGSN for P-GW selection.

**New Behavior:** With this release, the SGSN supports S-NAPTR queries for GGSN selection for both EPC and non-EPC capable UE. Changes were made to the `apn-resolve-dns-query` command to support this new functionality - refer to the Command Line Interface Reference and see Command Changes indicated below.

By supporting S-NAPTR queries, it is possible for the Gn/Gp-SGSN to perform Topological Gateway Selection provided with feature enhancement CSCzn60387. Refer to CSCzn60387 for the command needed to configure the SGSN’s canonical name for the Gn/Gp-SGSN.

Command Changes

```
apn-resolve-dns-query

epc-ue and non-epc-ue are new keywords for APN configuration with the `apn-resolve-dns-query snaptr` command. This command now enables the operator to configure whether to use GGSN S-NAPTR queries applicable for both EPC-capable UEs and non-EPC-capable UEs.

configure

    apn-profile profile_name

    apn-resolve-dns-query snaptr [ epc-ue non-epc-ue ]

    remove apn-resolve-dns-query snaptr

    end
```

Notes:

- If neither of the new keywords are included, then S-NAPTR query is applicable to all UE, both EPC-capable UE and non-EPC capable UE.
- `epc-ue` - S-NAPTR queries applicable for EPC-capable UE.
- `non-epc-ue` - S-NAPTR queries applicable for non-EPC-capable UE.

CSCub34940 - Bypass APN remap functionality

Feature Changes

Bypassing APN Remap for Specific IMEI Ranges

**Previous Behavior:** If a local default APN configured in an IMEI profile could not be used, then any default APN configured under an operator policy was used.
Also, only the `apn-selection-default` CLI option, under the APN Remap Table configuration associated with an IMEI profile, was valid. Other CLI options such as `apn-remap` and `blank-apn` were not applicable when a remap table was associated with an IMEI profile.

**New Behavior:** An APN Remap Table associated with an IMEI profile overrides a remap table associated with an operator policy.

This means activation will be rejected if a local default APN configured, in an APN Remap Table associated with an IMEI profile, cannot be used. This will occur even if a valid local default APN is available in an APN Remap Table associated with an operator policy.

No changes or modifications have been made to the command line interface (CLI). The APN Remap Table CLI options will be applicable for an IMEI profile in the same manner as for the configuration of an APN profile.

**Customer Impact:**

**Important:** To achieve the previous default behavior, the operator will need to change the current APN Remap configuration as indicated in this behavior change statement.

Customers already using an APN Remap Table that is associated with an IMEI profile will have to change the existing configuration to achieve the previous behavior. For example, if an existing configuration forced all matching IMEI in a defined IMEI range to use xxx.net APN, the configuration needs to be changed to an APN Remap Table configuration similar to what is shown below: Old APN Remap Table associated with an IMEI profile:

```
apn-selection-default network-identifier xxx.net
```

For a configuration to accomplish the same remapping function, change the APN Remap Table associated with an IMEI profile to the following:

```
apn-remap network-identifier * new-ni xxx.net
```

**Sample Configuration**

The following sample configuration will enable the operator to bypass APN remapping for a specific IMEI range:

```
cfg
  operator-policy name OpPol1
    associate call-control-profile OpPol1CCprof1
    associate apn-remap-table RemapOpPol1
      imei-range first start_imei last ending_imei [ sv IMEI_sv ] imei-profile name IMEIprof1
    exit
  imei-profile name IMEIprof1
    associate apn-remap-table remapIMEIprof1
  exit
  apn-remap-table remapIMEIprof1
```
exit

apn-remap-table RemapOpPoll

apn-selection-default network-identifier NewAPN.net

end

CSCub46992, CSCub47023 - 3G-SGSN and 2G-SGSN on ASR5500

Feature Changes

SGSN Functionality on the ASR 5500 Platform

All 2G and 3G SGSN features and functions provided on the ASR 5000 for IP interfaces are now fully supported on the ASR 5500 platform, with the exception of FastPath and Narrowband SS7.

Command Changes

Commands Not Supported by SGSN on ASR 5500

Because the ASR 5500 does not support either a Frame Relay or an ATM line card or Narrowband SS7 functionality, the following commands and/or keywords are not supported by the SGSN on the ASR 5500 platform:

- all commands in the ATM Port configuration mode
- all commands in the BITS Port configuration mode
- aps command, Card configuration mode
- sdh and sonet keywords of the framing command, Card configuration mode.
- header-type command, Card configuration mode
- initial-e1-framing command, Card configuration mode
- service-type command, Card configuration mode
- all commands in the Channelized Port configuration mode
- all commands in the DLCI configuration mode
- fr filter for the nse keyword of the sgsn op command in the Exec mode
- dlci-utilization keyword for the show linecard command in the Exec mode
- fr-config keyword for the show network-service-entity command in the Exec mode
- peer-nsei and frame-relay keywords for the network-service-entity command in the Global configuration mode
- port atm command in the Global configuration mode
- port channelized command in the Global configuration mode
- mtp2-aerm-emergency-threshold command in the Link configuration mode
• mtp2-aerm-normal-threshold command in the Link configuration mode
• mtp2-eim-decrement command in the Link configuration mode
• mtp2-eim-increment command in the Link configuration mode
• mtp2-eim-threshold command in the Link configuration mode
• mtp2-error-correction command in the Link configuration mode
• mtp2-lssu-len command in the Link configuration mode
• mtp2-max-outstand-frames command in the Link configuration mode
• mtp2-suerm-threshold command in the Link configuration mode
• mtp3-msg-size command in the Link configuration mode
• sscf-nni-n1 command in the Link configuration mode
• sscop-max-cc command in the Link configuration mode
• sscop-max-pd command in the Link configuration mode
• sscop-max-stat command in the Link configuration mode
• timeout command in the Link configuration mode
• link-type keyword for the link command in the Linkset configuration mode
• all commands in the Network Service Entity - Peer NSEI configuration mode
• all commands in the NSVC configuration mode
• all commands in the PVC configuration mode

CSCub48101 - QoS based on PLMN and RAT

Feature Changes

Support For QoS Based On PLMN And RAT

SGSN support for QoS selection based on RAT type is introduced through this feature, this functionality improves the Operator Policy based QoS Control capabilities. Currently, the SGSN supports only PLMN based QoS selection. The Operator policy on SGSN allows the operators to control QoS for visiting subscribers (National or International roaming-in subscribers or MVNO subscribers) on an APN basis depending on the PLMN-ID or IMSI range. APN profiles are configured under the Operator Policy as either default for all APN or specific profiles for particular APN.

The following limitations are encountered when only PLMN based QoS selection is supported:

1. When co-locating MME and SGSN into the same node, separate Operator Policy can be configured for E-UTRAN on the MME and both GERAN/UTRAN on the SGSN but not for GERAN and UTRAN separately on the SGSN.
2. The Operator policy currently allows to 'allow' or 'restrict' access to the network based on zone-code (set of LA/SA for 2G/3G and TA for LTE) but does not allow restricting the QoS in specific area of the network based on zone-code.

To overcome the limitations listed above, Operator Policy based QoS Control capabilities are introduced based on RAT-Type or a combination of RAT-Type with PLMN-ID or IMSI range.
Command Changes

**associate quality-of-service-profile**

Use the following command to associate an APN profile with a QoS profile:

```plaintext
config

apn-profile <profile_name>

associate quality-of-service-profile <profile_name> access-type [ gprs | umts ]

remove associate quality-of-service-profile <profile_name> access-type [ gprs | umts ]

exit
```

Notes:

This command is used to associate the specified Quality of Service profile with the APN profile. The access-type must be configured as either `gprs` or `umts`.

**quality-of-service-profile**

Use the following commands under the new CLI configuration mode “Quality of Service Profile” to configure the QoS parameters:

- `apn-ambr max-ul mbr-up max-dl mbr-dwn`
- `remove apn-ambr`
- `[ remove ] class { background | conversational | interactive | streaming } [ qualif_option ]`
- `[ remove ] description description`
- `end`
- `exit`
- `prefer-as-cap [ both-subscription-and-local | subscription | local ]`
- `prefer-tc [ background | conversational | streaming | interactive ]`
- `remove prefer-tc`

Performance Indicator Changes

**show apn-profile full [all | name]**

The following parameters are introduced in the `show apn-profile full [ all | name ]`:

- Associated Quality of Service Profile Name (UMTS)
- Validity
- Associated Quality of Service Profile Name (GPRS)
show quality-of-service-profile [ all | full [ all | name ] | name ]

This new show command is introduced to support this feature. The following parameters are displayed on execution of this command:

- QoS Profile Name
- Description
- Preferred Traffic Class
- Quality of Service Capping
- Prefer Type
- Traffic Class
- Sdu delivery order
- Delivery Of Erroneous Sdus
- Max Bit Rate Uplink
- Max Bit Rate Downlink
- Allocation/Retention Priority
- Guaranteed Bit Rate Uplink
- Guaranteed Bit Rate Downlink
- Sdu Max Size
- Minimum Transfer delay
- Sdu Error Ratio
- Residual BE R
- QoS APN-AMBR
- Max uplink
- Max downlink

CSCub48124 - EIR Selection for roaming subscribers

Feature Changes

EIR Selection for Roaming Subscribers

The Equipment Identity Register (EIR), used for authentication and authorization during an Attach, is the carrier's IMEI(SV) database of the unique numbers allocated to each subscriber’s mobile station equipment (IMEI) and the manufacturer’s software version (SV). An IMEI(SV) can be in one of three lists in the EIR:

- white list - the subscriber equipment is permitted access
- black list - the subscriber equipment is not permitted access
- grey list - the subscriber equipment is being tracked for evaluation or other purposes

As part of this enhancement, the SGSN now creates and uses an EIR profile to define the parameters to:
- use a single EIR address for multiple EIRs,
- achieve the Check-IMEI-Request, and
- associate the EIR profile with a call control profile.

This makes it possible for the SGSN to select an EIR based on the PLMN into which the subscriber has roamed and reduce signalling back to home PLMNs for roamers.

**Command Changes**

**eir-profile**

eir-profile is a new command in the SGSN Global configuration mode. This command creates up to 16 instances of an EIR profile and provides access to the EIR profile configuration mode commands that define the parameters of the profile.

```
configure
sgsn-global

[ no ] eir-profile profile_name

[ no ] check-imei-every-n-events check_frequency | eir-address { isdn isdn_number | point-code point_code | include-imsi | map-include-imsi

end
```

Notes:
- **no eir-profile** deletes a profile from the SGSN global configuration.
- **no** with an EIR profile configuration command disables a previously set value.
- **check-imei-every-n-events** configures the frequency with which a 'check IMEI' message is sent to the EIR. When set, the SGSN skips sending the ‘check IMEI’ message for the first N-1 where IMDI/IMEISV is received. frequency must be an integer from 1 to 15. By default, ‘check IMEI’ message is sent for every event.
- **eir-address** identifies the EIR’s address as either an E.164 ISDN (up to 15 digits) or an SS7 point-code and includes the Source SSN (default of 149 for SGSN).
- **include-imsi** includes IMSI in TCAP message to enable inclusion of IMSI checking during the IMEI check procedure. By default the IMSI is not included.
- **map-include-imsi** includes IMSI in MAP message to enable inclusion of IMSI checking during the IMEI check procedure. By default the IMSI is not included.
- **show sgsn-mode** displays values configured for all EIR profiles.

**eir-profile**

eir-profile is a new command in the Call Control Profile configuration mode. This command identifies the EIR profile, created and configured in the SGSN Global configuration mode, to associate with the call control profile.

```
configure
```
call-control-profile profile_name

[ no ] eir-profile profile_name

end

Notes:
- no disassociates an EIR profile with the call control profile.
- The EIR parameters configured under the EIR profile associated with the call control profile take precedence over those configured in the MAP service.

CSCuc21648, CSCud69746, CSCud12642 - Support higher than 16 Mbps bit rate flag in 3G S4-SGSN

Feature Changes

S4-SGSN Support for “Higher Bit Rates than 16 Mbps” Flag

As per 3GPP R9 specifications, the SGSN can now be aware if the UE is capable of supporting extended R7 bit rates. The “higher bit rates than 16 Mbps” flag is used for this purpose. This flag is sent by the RNC in the Initial UE message or Re-location Complete message or by Peer S4-SGSN / MME in Forward Relocation Request / Context Response message. The SGSN also supports sending “higher Bit Rates than 16 Mbps flag” as part of MM Context in Context response/Forward Relocation request/identification request during Old ISRAU/SRNS handover procedures. The SGSN stores the UE capability in the MM-context. During PDP context activation, the per bearer bit rate or APN-AMBR is capped based on the flag's value. If the RNC is not 3GPP R9 compliant, the SGSN does not receive this flag. A new CLI keyword `ue-3gpp-compliance-unknown restrict-16mbps` is introduced under the sgsn-service to support this functionality. When the CLI is configured, the SGSN caps the APN-AMBR for non-GBR bearers to “16” Mbps and rejects activation of GBR bearers with GBR higher than “16” Mbps. If not, APN-AMBR and GBR higher than “16” Mbps are allowed.

Consider the scenarios where UE 3GPP compliance is not known and the CLI is configured to restrict bitrate to 16 Mbps or it is known that UE is not capable of supporting bitrates higher than 16Mbps; the Session Manager uses the flag to perform the following actions:

1. The APN-AMBR is restricted to “16” Mbps during PDP activation of non-GBR bearers, particularly the default bearer.
2. If the PGW upgrades the APN-AMBR in Create Session Response during non-GBR bearer activation, then the APN-AMBR is retained as “16” Mbps and same is indicated to the UE in an Activate Accept.
3. If the PGW upgrades APN-AMBR in Update Bearer Request for non-GBR bearer, then the APN-AMBR is restricted to “16” Mbps and only if the APN-AMBR changes, the PGW init bearer modification procedure is continued. In case APN-AMBR does not change, then Update Bearer Response is sent immediately.
4. For GBR bearers, Update Bearer Request with GBR/MBR higher than “16” Mbps is rejected with “No resources available”.
5. Activation of GBR bearers with MBR/GBR higher than “16” Mbps in Create Bearer Request is rejected with cause “No resources available”.
6. After S3 SRNS, Modify Bearer Command is initiated to modify the APN-AMBR to “16” Mbps for Non-GBR bearers having bitrates higher than 16 Mbps.
7. After S3 SRNS, GBR bearers having bitrates higher than “16” Mbps are de-activated.

Previous Behavior: The S4-SGSN did not restrict bitrate to “16” Mbps for UE's not capable of handling higher bitrates, the RNC had to downgrade the bitrates during RAB assignment procedure.
New Behavior: The S4-SGSN now restricts the bitrates to “16” Mbps for UE’s not capable of higher bitrates based on a flag received from the RNC or peer SGSN. This downgraded bitrate is sent in the Create Session Request during activation.

Customer Impact: The flag “Higher Than 16Mbps” RANAP IE was introduced in 3GPP R9 specifications. If RNC’s are not 3GPP R9 complaint or do not support sending of this flag, then the S4-SGSN action can now be overridden through the new CLI introduced under sgsn-service, otherwise the bearer activations may fail if the RNC downgrades the QoS, this is not allowed or the UE de-activates the bearer with cause “Qos not accepted”.

Command Changes

sm

A new CLI keyword `ue-3gpp-compliance-unknown restrict-16mbps` is introduced to support the “Higher Bit Rates than 16 Mbps” flag.

```
configure
  context context_name
    sgsn-service service_name
      sm { T3385-timeout time | T3386-timeout time | T3395-timeout time | guard-timer
           guard_seconds | ignore-asi | max-activ-retransmission number | max-deactiv-retransmission
           number | max-modf-retransmission number | ue-3gpp-compliance-unknown restrict-16mbps } 
      no sm { ignore-asi | ue-3gpp-compliance-unknown [restrict-16mbps] }
```

end

Notes:
- If this keyword is configured, the SGSN caps the APN-AMBR for non-GBR bearers to “16” Mbps and rejects the activation of GBR bearers with GBR higher than “16” Mbps.
- If the `no` form of this keyword is configured, the APN-AMBR and GBR higher than “16” Mbps are allowed.
- By default, the SGSN does not cap APN-AMBR or reject GBR bearer activation with bitrates higher than “16” Mbps.

Performance Indicator Changes

```
show sgsn-service name <service_name>
```

A new field with either 'Enabled' or 'Disabled' options has been added to the output of the command `show sgsn-service name <service_name>` to indicate whether or not the option to restrict bitrate to “16” Mbps when the UEs 3GPP compliance is not known has been configured, this option is disabled by default:
- Restrict Bitrate to 16 Mbps when UE 3GPP Compliance is Unknown

```
show subscribers sgsn-only full imsi <>
```

A new field is added to display the MM context value of the “higher bit rates than 16 Mbps” flag as either Allowed or Not Allowed or Unknown.
Higher Than 16 Mbps

CSCuc90461 - Support DSCP marking on SGSN Diameter interfaces (S6d & S13')

Feature Changes

Support For DSCP Marking on SGSN Diameter interfaces (S6d & S13')

**Previous Behavior:** DSCP marking is not supported for S6d and S13' interfaces.

**New Behavior:** The CLI command `dscp <value>` under the Diameter Endpoint Configuration mode is now supported for S6d and S13' interfaces on the SGSN.

**Customer Impact:** DSCP marking is now configurable on S6d and S13' interfaces.

CSCud12642 - [15.0]Support per RNC level bit rate capping at S4-SGSN

Feature Changes

**Bit Rate Capping per RNC on the S4-SGSN**

**Previous Behavior:** In StarOS R14.0 there was lack of clarity on how the S4-SGSN should support handovers from R7+ RNC to pre-R7 RNC. As a result, S4-SGSN did not support per-RNC bit rate capping although the Gn-SGSN does.

**New Behavior:** 3GPP TS 23.060 v11.3 version provides some clarity on how an S4-SGSN should handle per RNC / UE QoS capability based bit rate capping. In this release, the S4-SGSN functionality has been enhanced to support per RNC level bit rate capping.

The operator should use the existing CLI `release-compliance` command, in the RNC Configuration Mode, to set both MBR and GBR for uplink and downlink traffic.

**Customer Impact:**

With support for bit rate capping per RNC, the S4-SGSN:

- restricts the APN-AMBR to the RNC supported bit rate during PDP activation and modification of non-GBR bearers.
- rejects PDP activation and modification of GBR bearers having requested GBR greater than the RNC supported bit rate.
- deactivates GBR bearers having GBR bit rate greater than the RNC supported bit rates of the target RNC during inter RNC handovers. SGSN initiated dedicated bearer deactivation procedure will be triggered towards the S-GW and the P-GW to deactivate the bearers at the S-GW and the P-GW.
- restricts the APN-AMBR for non-GBR bearers to the RNC supported bit rates of the target RNC during inter-RNC handovers. The SGSN also initiates PDP modification procedures toward the UE after the completion of the handover procedure.
CSCud64147 - SGSN shall provide bulk statistics support for LCS-MAP counters

Performance Indicator Changes

SGSN Schema

New bulk statistics have been added for LCS. For details, refer to the Statistics and Counters Reference:

- map-sub-loc-rpt-req-tx
- map-sub-loc-rpt-rsp-rx
- map-sub-loc-rpt-err-rx
- map-sub-loc-rpt-timeouts-rx
- map-prov-sub-loc-req-rx
- map-prov-sub-loc-rsp-tx
- map-prov-sub-loc-err-tx

CSCud69746 - Support S4 interface for non EPC devices

Feature Changes

S4 Interface Support For Non-EPC devices

The S4 interface support has been extended to Non-EPC capable devices. This support was only available for EPC service capable devices or subscribers with EPS subscription. S4 interface support to Non-EPC devices allows more control on interface selection and ability to handle QoS and legacy UE related behavior issues.

To enable S4 support for Non-EPC devices, interface selection options during first PDP activation have been added, these options allow the following:

1. S4 interface selection based on UEs EPC capability alone.
2. S4 interface selection only for UEs that are EPC capable and those that have EPS subscription.
3. S4 interface selection for all UEs having EPS subscription.
4. An option to always select S4 interface.

When the S4 interface is used and a Non-E-UTRAN capable device requests for PDP de-activation of only the primary PDP without de-activating the associated secondary PDP’s (that is, without a teardown indicator), the SGSN deletes the associated secondary PDP contexts locally without informing UE.

When a Non-E-UTRAN capable UE activates a PDP context with Conversational or Streaming class (GBR bearers) and if Iu is released, the UE preserves the PDP with bit rate set to “0” kbps. However, when the S4-SGSN notices an Iu-Release, it has to de-activate the GBR bearers. Currently the S4-SGSN does not support the de-activation of GBR bearers. When S4-SGSN support for PDP context preservation procedures is added in a future release (for both EPC and Non-EPC devices), GBR bearers will be de-activated without informing the UE.
Command Changes

sgsn-core-nw-interface

The command `sgsn-core-nw-interface` in the Call-Control-Profile configuration is enhanced with keywords to support S4 interface selection:

```
config

    call-control-profile cc-profile name

    sgsn-core-nw-interface {gn | s4 [epc-ue {always | eps-subscribed} non-epc-ue {never | always | eps-subscribed}]}

    exit
```

Notes:

- When keywords or options are not selected with the selection of the S4 interface option, it implies that the SGSN will apply S4 interface always for both EPC and Non-EPC devices. This is also synonymous to the CLI command configured as `sgsn-core-nw-interface s4 epc-ue always non-epc-ue always`.
- To configure SGSN behavior supported in previous releases, the CLI is configured as `sgsn-core-nw-interface s4 epc-ue always non-epc-ue eps-subscribed`. This is also the default behavior when the CLI is not configured.

For more information on the CLI commands see the Command Line Interface Reference.

Performance Indicator Changes

show call-control-profile full name < >

This show command is updated with information about SGSN core network interface selection. The following new fields have been added:

- SGSN Core Network Interface Selection
- SGSN Core Network Interface Type
- S4 for EPC Capable Devices
- S4 for Non-EPC Capable Devices

The field **SGSN Core Network Interface Type** displays interface selected as either Gn or S4.

The field **S4 for EPC Capable Devices** displays the configuration as either Always or When EPS Subscription Available, based on the CLI configured in the command `sgsn-core-nw-interface` in the Call-Control Profile.

The field **S4 for Non-EPC Capable Devices** displays the configuration as Never or Always or When EPS Subscription Available, based on the CLI configured in the command `sgsn-core-nw-interface` in the Call-Control Profile.

show subscribers sgsn-only full imsi < >

This show command is updated to display the subscription type being used for primary PDP activation. The field **Subscription Type** is added to the show output. The subscription type is displayed as either EPS or GPRS.
SGSN Changes in Release 16

show subscribers gprs-only full imsi < >

This show command is updated to display the subscription type being used for primary PDP activation. The field Subscription Type is added to the show output. The subscription type is displayed as either EPS or GPRS.

CSCue32234 - [S4-SGSN] UE-AMBR override from local config shall be supported

Feature Changes

Capping UE AMBR Based on Local Configuration

The operator can now cap the subscribed UE AMBR value with a change of the local configuration. Or, the operator can set the prefer-cap type.

Related Issues: CSCtx38089

Command Changes

qos

ue-ambr is a newly supported keyword in the qos command. This keyword enables the operator to configure either the aggregate maximum bit rate stored on the UE (UE AMBR) or select the preferred uplink and downlink QoS cap values.

configure

    call-control-profile profile_name

        qos ue-ambr { max-ul max_ul_value max-dl max_dl_value | prefer-as-cap { both-hss-and-local minimum | local } }  
        remove qos ue-ambr 
        end

Notes:

- max-ul defines the maximum bit rate for uplink traffic; range 0 to 1410065408.
- max-dl defines the maximum bit rate for downlink traffic; range 0 to 1410065408.
- both-hss-and-local minimum use the lower of either the locally configured QoS bit rate or the Home Subscriber Server (HSS)-provided QoS bit rate.
- local use the locally configured QoS bit rate.
- remove erases the QoS UE Ambr configuration from the call control profile.

Performance Indicator Changes

show call-control-profile
In support of the new ability to configure UE AMBR, new fields have been added to the output of the `show call-control-profile full name profile_name`

- Qos
  - UE-AMBR <Enabled/Disabled>
    - MAX uplink <value>
    - MAX downlink <value>
  - Quality of Service Capping <Enabled/Disabled>
    - Prefer Type <selection>

**CSCue97071 - CLI to choose MCC, MNC coding in hex or dec for DNS FQDN**

**Feature Changes**

**Format Encoding of MNC and MCC in DNS Queries Enhanced**

**Previous Behavior:** In gprs-service and sgsn-service, the CLI `dns israu-mcc-mnc-encoding [hexadecimal | decimal]` was used to control hexadecimal format encoding for mcc and mnc in naptr and a-query. The procedures controlled by this CLI were RAU, Ptmsi-Attach and SUSPEND. Both NAPTR and A Query were controlled by same CLI command.

**New Behavior:** The CLI command `dns israu-mcc-mnc-encoding [hexadecimal | decimal]` has been deprecated and a new CLI command `dns mcc-mnc-encoding { rai-fqdn | apn-fqdn | rnc-fqdn | mmec-fqdn | tai-fqdn}* {a-query | snaptr-query }* { decimal | hexadecimal }` is introduced, all the procedures invoking DNS are controlled by this CLI. New keyword options `snaptr-query` and `a-Query` are provided to control different types of queries.

To ensure backward compatibility:

1. If the command `dns israu-mcc-mnc-encoding decimal` is executed, it will be auto converted to `dns mcc-mnc-encoding rai-fqdn a-query snaptr-query decimal`.
2. If the command `dns israu-mcc-mnc-encoding hexadecimal` is executed, it will be auto converted to `dns mcc-mnc-encoding rai-fqdn a-query snaptr-query hexadecimal`

**Customer Impact:** Customers can control DNS query for a particular type of procedure more effectively.

**Command Changes**

`dns mcc-mnc-encoding`

This new command has been introduced to configure encoding format for the MCC and MNC values in the DNS query.

configure

```
context context_name

sgsn-service service_name

dns mcc-mnc-encoding { apn-fqdn | mmec-fqdn | rai-fqdn | rnc-fqdn | tai-fqdn}* {a-query | snaptr-query }* { decimal | hexadecimal }
```
default dns mcc-mnc-encoding
end

Notes:
In order to provide effective control on DNS queries for particular type of procedures, existing CLI commands in GPRS and SGSN services have been deprecated and replaced with new enhanced commands. The command `dns israu-mcc-mnc-encoding [hexadecimal | decimal]` has been deprecated and this new CLI command is introduced. New keyword options `snaptr-query` and `a-Query` are provided to control different types of queries.

dns mcc-mnc-encoding
This new command has been introduced to configure encoding format for the MCC and MNC values in the DNS query.

configure

context context_name
gprs-service service_name
dns mcc-mnc-encoding { apn-fqdn | mmec-fqdn | rai-fqdn | rnc-fqdn | tai-fqdn }* { a-query | snaptr-query }* { decimal | hexadecimal }
default dns mcc-mnc-encoding
end

Notes:
In order to provide effective control on DNS queries for particular type of procedures, existing CLI commands in GPRS and SGSN services have been deprecated and replaced with new enhanced commands. The command `dns israu-mcc-mnc-encoding [hexadecimal | decimal]` has been deprecated and this new CLI command is introduced. New keyword options `snaptr-query` and `a-Query` are provided to control different types of queries.

Performance Indicator Changes

show sgsn service all

New counters have been introduced to display the encoding format for MCC and MNC values in the DNS query:
- MCC/MNC Encoding in DNS for RAI FQDN in A/AAAA Query
- MCC/MNC Encoding in DNS for RAI FQDN in SNAPTR Query
- MCC/MNC Encoding in DNS for APN FQDN in A/AAAA Query
- MCC/MNC Encoding in DNS for APN FQDN in SNAPTR Query
- MCC/MNC Encoding in DNS for RNC FQDN in A/AAAA Query
- MCC/MNC Encoding in DNS for RNC FQDN in SNAPTR Query
- MCC/MNC Encoding in DNS for MMEC FQDN in A/AAAA Query
- MCC/MNC Encoding in DNS for MMEC FQDN in SNAPTR Query
- MCC/MNC Encoding in DNS for TAI FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for TAI FQDN in SNAPTR Query

show gprs service all

New counters have been introduced to display the encoding format for MCC and MNC values in the DNS query:

• MCC/MNC Encoding in DNS for RAI FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for RAI FQDN in SNAPTR Query
• MCC/MNC Encoding in DNS for APN FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for APN FQDN in SNAPTR Query
• MCC/MNC Encoding in DNS for RNC FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for RNC FQDN in SNAPTR Query
• MCC/MNC Encoding in DNS for MMEC FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for MMEC FQDN in SNAPTR Query
• MCC/MNC Encoding in DNS for TAI FQDN in A/AAAA Query
• MCC/MNC Encoding in DNS for TAI FQDN in SNAPTR Query

CSCug56288, CSCun89857, CSCun41909 - EIR IMSI Field in IMEI Check

Feature Changes

IMSI Inclusion in the MAP-Check-IMEI Message

SGSN sends IMEI information to the EIR to validate the equipment used by the subscriber. The SGSN sends the IMEI and equipment information via the Gf interface over MAP in a CHECK_IMEI Request.

The operator can configure the SGSN to also send the IMSI parameter in the MAP_CHECK_IMEI message to the EIR to identify the subscriber using the equipment. Knowledge of the subscriber will cause the EIR to behave differently, in accordance with the user type - that is blacklisted, roamer and so on.

This support is only available in MAP Version 3 messages.

Command Changes

equipment-identity-register

A new optional keyword, map-include-imsi, enables the SGSN to include the IMSI in the MAP portion of the MAP_CHECK_IMEI message to the EIR to identify the subscriber using the equipment.

config

c context context_name

map-service service_name

equipment-identity-register { isdn E.164_num | point code pt_code } [ check-imei-every-n-events times | source-ssn ssn] [include-imsi | map-include-imsi]
no equipment-identity-register { isdn E.164_num | point code pt_code }
[include-imsi | map-include-imsi]
end

Where:
- **include-imsi** keyword enables the inclusion of IMSI checking during the IMEI check procedure. By default this function is not included.
- **map-include-imsi** keyword enables the inclusion of IMSI parameter in the CHECK_IMEI Request. By default, IMSI is not included in the CHECK_IMEI Request.
- **no** included in the command phrase, disables the specified operation.

### Performance Indicator Changes

**show map-service**

A new field has been added to the `show map-service` output to indicate if sending the IMSI in the MAP_CHECK_IMEI message has been enabled in the SGSN configuration:

- MAP CHECK IMEI MAP Include IMSI :

### CSCug97812 - Lock Peer-Server Point/Process (PSP)

#### Feature Changes

**SGSN Support for Peer-Server Blocking**

The validity of SCTP redundancy has to be tested by simulating fail overs when new RNCs/STPs have to be commissioned. Peer-Server Blocking support has been added to prevent any issues during commissioning of new RNCs/STPs.

The Peer Server Blocking feature provides the following functionalities:

1. The SCTP association can be either brought up or down in order to test the redundancy of the same.
2. The PSPs can be brought down without removing the configuration.
3. The SGSN supports a new configuration command under the psp-instance to block/unblock peer endpoint and this configuration is pushed to the Link Manager to achieve peer-server blocking.
4. The SGSN sends a SCTP Shutdown to the remote endpoint and marks the endpoint as LOCKED when the PSP is configured as blocked and if the PSP is in ESTABLISHED state.
5. The SGSN initiates a SCTP INIT when a blocked PSP is un-blocked and if the SGSN is a client and is asp-associated.
6. The SGSN replies with an ABORT when the peer sends INIT in LOCKED state.
7. The SGSN marks the remote endpoint as LOCKED when the PSP is configured as blocked and if the PSP is in a CLOSED state.
8. The PSP state is recovered in case of Link Manager death and no messages are initiated after recovery if the PSP is in locked state.

**Previous Behavior:** Control for locking PSP was not supported.

**New Behavior:** The SGSN now supports control for bringing down and locking PSPs. A new CLI has been added for supporting Peer-Server blocking.
Command Changes

**shutdown**

A new CLI command `shutdown` is added under the PSP instance configuration mode to bring down and lock the SCTP association.

```
config

ss7-routing-domain routing_domain_id variant variant_type

peer-server id id

psp_instance psp_instance

[ no ] shutdown

exit
```

Notes:

- On configuring `shutdown`, the PSP is brought down via a SCTP Shutdown procedure (if association is already ESTABLISHED) or Abort (any other association state) and it is marked LOCKED. The SGSN does not initiate any messages towards the peer and any message from the peer will be responded with a SCTP Abort, when the PSP is in a LOCKED state.
- On configuring `no shutdown`, the PSP is marked unlocked and the SGSN initiates an association establishment towards the peer. This is the default configuration for a PSP. The default is `no shutdown`.
- Listed below are the error codes added to support the Peer-Server blocking feature:
  - Once the CLI is configured if the operator tries to re-configure the same CLI again, a CLI failure is displayed. This suppresses the Link Manager error logs while trying to push same configuration twice.
    
    The error code displayed is:
    
    **Failure: PSP: Re-configuring same value**
  
  - During an ongoing shutdown procedure if the command `no shutdown` is executed, the execution of the command will be unsuccessful and a CLI failure error message is displayed.
    
    The error code displayed is:
    
    **Cannot unlock PSP during ongoing shutdown procedure**

    This ensures that the shutdown procedure is graceful. The command `no shutdown` can be configured only when there is no ongoing shutdown procedure.

**CSCuh31686 - Authentication vector management in S4 SGSN**

Feature Changes

**Authentication Vector Management in the SGSN**
The SGSN provides a mechanism to define the number of authentication vectors (AVs) that can be requested from the HSS by the SGSN in an Authentication Info Request (AIR) message. New vectors are fetched when no more vectors are available.

As well, it is possible to configure a minimum (low watermark) threshold value (number of unused vectors present) and when the current number of unused vectors falls below this value, new vectors will be fetched. This low watermark is set with the `min-unused-auth-vectors` in the call control profile.

**Previous Behavior:** Prior to Release 16, the maximum configurable number of authentication vectors to be retrieved from HSS is 3.

**New Behavior:** The new maximum configurable number of authentication vectors to be retrieved from the HSS is 5.

**Customer Impact:** The management of authentication vectors is key in order to maintain service accessibility and delivery when there is a problem on the Gr / S6a or S6d interface (for example: link failure, DRF failure, HSS failure).

### Command Changes

**auth-request**

The value range for the `num-auth-vectors` keyword of this command has been extended from 3 to 5.

```
configure

context context_name

    hss-peer-service service_name

    auth-request num-auth-vectors num

    default auth-request num-auth-vectors

end
```

**Notes:**

- `num` must be an integer from 1 to 5.
- `default` returns the minimum AV configuration to 1.

### CSCuh57775 - Common Routing Area for 2G and 3G

**Feature Changes**

**Common Routing Area for 2G and 3G**

If the RA is configured in both 2G and 3G, the SGSN now supports paging in both the RATs. In previous releases common Routing Area across 2G and 3G was not supported completely. Paging was done only in the last known RAT and power-off detach from other RAT was not supported.

With the introduction of this feature, the following enhancements have been made:

1. If paging has to be done in RA which is common across the RATs, the SGSN supports paging initiation in both the RATs.
2. The SGSN accepts power-off detach from the common RA.
3. If the MS is in STANDBY or PMM-IDLE state and a downlink packet arrives at the SGSN, paging is done. This is applicable for both A/Gb and Iu modes.

GPRS detach (power-off) may be initiated by the MS, but as the request is received in switched off mode the core network does not send a Detach Accept. When the Routing Area is shared across (Iu/Gb), the Detach Request is accepted at any of the modes and the subscriber details are cleared.

**Previous Behavior:** Paging is not done in both the RATs for a subscriber in common RA.

**New Behavior:** A new CLI command `common-ra-paging` is introduced in the SGSN Global configuration mode, this command has to be configured to enable paging in both the RATs for subscriber in common RA.

**Command Changes**

`common-ra-paging`

This command enables support for the new feature:

```
config
sgsn-global
  no common-ra-paging
exit
```

Notes:

This command enables paging across common Routing Area (RA) for 2G and 3G. For more information on this command see the *Command Line Interface Reference*.

**Performance Indicator Changes**

**SGSN Schema**

The following statistics are included in the SGSN Schema in support of this feature:

- common-ra-3g-page-req-same-rat
- common-ra-2g-page-req-same-rat
- common-ra-3g-page-req-ret-same-rat
- common-ra-2g-page-req-ret-same-rat
- common-ra-3g-page-req-other-rat
- common-ra-2g-page-req-other-rat
- common-ra-3g-page-req-ret-other-rat
- common-ra-2g-page-req-ret-other-rat
- common-ra-3g-page-rsp-same-rat
- common-ra-2g-page-rsp-same-rat
- common-ra-3g-page-rsp-attach-other-rat
- common-ra-2g-page-rsp-attach-other-rat
• common-ra-3g-page-rsp-rau-other-rat
• common-ra-2g-page-rsp-rau-other-rat
• common-ra-3g-page-rsp-power-off-other-rat
• common-ra-2g-page-rsp-power-off-other-rat
• common-ra-3g-page-timeout-other-rat
• common-ra-2g-page-timeout-other-rat
• common-ra-3g-page-stop
• common-ra-2g-page-stop
• common-ra-3g-attach-other-rat
• common-ra-2g-attach-other-rat
• common-ra-3g-rau-other-rat
• common-ra-2g-rau-other-rat
• common-ra-3g-power-off-other-rat
• common-ra-2g-power-off-other-rat

**show sgsn-mode**

The following new parameter indicates if common Routing Area paging is “Enabled” or “Disabled”:

• Common RA Paging

**show gmm-sm statistics**

The following new parameters are added to this show command to display the statistics for this feature:

**Paging Statistics**

• Total-CRA-Page-Req-Same-RAT
• 3G-PS-CRA-Page-Req
• Total-CRA-Page-Ret-Same-RAT
• 3G-PS-CRA-Page-Ret-Req-in-2G
• Total-CRA-Page-Req-Other-RAT
• 3G-PS-CRA-Page-Req-in-2G
• Total-CRA-Page-Ret-Other-RAT
• 3G-PS-CRA-Page-Ret-Req
• Total-CRA-Page-Rsp-Same-RAT
• 3G-PS-CRA-Page-Rsp
• Total-CRA-Page-Rsp-Other-RAT
• 3G-PS-CRA-Attach-from-2G
• 3G-PS-CRA-RAU-from-2G
- 3G-PS-CRA-Power-Off-from-2G
- Total-CRA-Page-TO-Other-RAT
- 3G-PS-CRA-Timeout-in-2G
- Total-CRA-Page-Stop
- 3G-PS-CRA-Page-Stop
- 2G-PS-CRA-Page-in-3G
- 2G-PS-CRA-Page-Ret-Req-in-3G
- 2G-PS-CRA-Page-Req
- 2G-PS-CRA-Page-Ret-Req
- 2G-PS-CRA-Page-Rsp
- 2G-PS-CRA-Attach-from-3G
- 2G-PS-CRA-RAU-from-3G
- 2G-PS-CRA-Power-Off-from-3G
- 2G-PS-CRA-Timeout-in-3G
- 2G-PS-CRA-Page-Stop

Non-Paging Statistics
- 3G-CRA-Attach
- 3G-CRA-RAU
- 3G-CRA-Power-Off
- 2G-CRA-Attach
- 2G-CRA-RAU
- 2G-CRA-Power-Off

CSCui71700 - Inclusion of CC17 and CC25 for RANAP redirection

Feature Changes

Redirection Indication Cause Codes for MOCN

The Cisco SGSN supports both 2G and 3G MOCN network sharing.

**Previous Behavior:** In network sharing scenarios, Redirection Complete IE was sent if an Attach or RAU was rejected with GMM cause code #17 - Network Failure when the SGSN receives MAP error “System Failure” or “Unexpected Data” value from the HLR.

**New Behavior:** As part of 3GPP Release-11, cause code #17 (network failure) and cause code #25 (not authorized for this CSG) have been added for redirection indication for network sharing cases. Cause code #25 is relevant only for 3G MOCN, and cause code #17 is applicable for both GERAN and UMTS MOCN cases.
Now, in both 2G and 3G network sharing scenarios, for roaming subscribers the Redirection Indication IE will be sent if an Attach or RAU is rejected with GMM cause code #17 - Network Failure when the SGSN receives MAP error for “System Failure” or “Unexpected Data” value from the HLR.

For 3G network operators, the operators have a new CLI to disable this new behavior.

**Customer Impact:** The HPLMN operator may accept Update Location from one sharing VPLMN operator but reject Update Location with cause code #17 from another sharing VPLMN operator. Previously, as soon as one sharing VPLMN operator receives MAP reject with cause #17, all sharing VPLMN operators stopped registering the subscriber. With the new behavior, VPLMN operators using shared networks should be able to accept registrations that are not accepted for the other sharing operators.

### Command Changes

**network-sharing**

For roaming subscribers in 3G MOCN only, the new keyword `stop-redirect-reject-cause` enables the operator to disable the new behavior and stop sending redirection indication RANAP Reject messages when reject is due to GMM cause #17 (network failure) related to System Failure or Unexpected Data value MAP error from the HLR. So the operator would change to send redirection complete.

```plaintext
configure

    context context_name

    iups-service service_name

    network-sharing stop-redirect-reject-cause network-failure

    { default | no } network-sharing stop-redirect-reject-cause

end
```

**Notes:**

- `default` enables the sending of redirect indication in Attach Reject or RAU Reject if reject is due to GMM cause 'network failure' which resulted from one of the MAP errors unexpected data value or system failure.
- `no` disables this configuration and instructs the SGSN to follow default behavior.

### Performance Indicator Changes

**SGSN Schema**

The following new bulk statistic variables have been introduced under the SGSN schema to track redirection as a cause for network failure:

- `redir-attach-rej-gprs-nf`
- `redir-attach-rej-comb-nf`
- `redir-periodic-rau-nf`
- `redir-rau-gprs-intra-sgsn-rej-nf`
- `redir-rau-comb-intra-sgsn-rej-nf`
• redir-rau-gprs-inter-sgsn-rej-nf
• redir-rau-comb-inter-sgsn-rej-nf
• redir-rau-gprs-inter-rat-nf
• redir-rau-comb-inter-rat-nf
• redir-rau-gprs-inter-serv-nf
• redir-rau-comb-inter-serv-nf
• 2g-attach-redir-ind-nw-failure
• 2g-rau-redir-ind-nw-failure
• redir-attach-rej-gprs-ncil
• redir-attach-rej-comb-ncil
• redir-periodic-rau-ncil
• redir-rau-gprs-intra-sgsn-rej-ncil
• redir-rau-comb-intra-sgsn-rej-ncil
• redir-rau-gprs-inter-sgsn-rej-ncil
• redir-rau-comb-inter-sgsn-rej-ncil
• redir-rau-gprs-inter-rat-ncil
• redir-rau-comb-inter-rat-ncil
• redir-rau-gprs-inter-serv-ncil
• redir-rau-comb-inter-serv-ncil

show gmm-sm statistics verbose

Under the subheading ‘Total Redirection Indications Sent’ for both the display headings ‘GPRS MOCN Attach Statistics’ and ‘GPRS MOCN RAU Statistics’, a single counter has been added

• Network failure

New counters have been added to peg the number of 3G Attach Rejects or RAU Rejects sent with Redirection Indication set due to network failure.

• Network Failure:
  • Tot-Attach-Rej:
    • Attach-Gprs:
    • Attach-Comb:
  • Tot-Rau-Rej:
    • Rau-Periodic:
    • Rau-Intra-SGSN:
    • Rau-Comb-Intra-SGSN:
    • Rau-Inter-SGSN:
• Rau-Comb-Inter-SGSN:
• Rau-Inter-Rat:
• Rau-Comb-Inter-Rat:
• Rau-Inter-Serv:
• Rau-Comb-Inter-Serv:
• Tot-Serv-Rej:

CSCuj70597 - Support ‘Homogenous Support of IMS Voice over PS Sessions’ indication in ULR message

Feature Changes

Support for “Homogenous Support of IMS Voice over PS Sessions” Indication in ULR Message

**Previous Behavior:** The “Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions” AVP is not sent in Update-Location-Request (ULR) message towards the HSS.

**New Behavior:** The “Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions” AVP is now included in Update-Location-Request (ULR) message towards the HSS. The AVP sent in the ULR message can be seen in the monitor-protocol. Currently SGSN always sends the value of the AVP “Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions” set to “Not_Allowed” in ULR command to HSS.

**Customer Impact:** The AVP “Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions” can now be seen in the ULR message.

CSCuj70624 - Support Terminating-Access Domain Selection (T-ADS) data retrieval

Feature Changes

Support for Terminating-Access Domain Selection (T-ADS) Data Retrieval

**Previous Behavior:** SGSN does not support indication of T-ADS Data Retrieval in ULR message towards the HSS on S6d Interface. Support for T-ADS Data Retrieval via IDR/IDA procedures on S6d Interface is required.

**New Behavior:** SGSN now supports indication of T-ADS Data Retrieval in supported features AVP of ULR message towards the HSS on S6d Interface. T-ADS data retrieval in IDR/IDA is supported.
CSCuj76698 - Message aggregation between linkmgr/gbmgr to sessmgr should be automated

Feature Changes

Controlling Aggregation of LinkMgr and GbMgr Messages

Previous Behavior: Aggregation was static.

New Behavior: Aggregation of messages from LinkMgr and GbMgr to the SessMgr is now automated and is CLI configurable.

Command Changes

aggregate-ipc-msg

New auto-num-msgs keyword enables automated aggregation of messages sent from LinkMgr or GbMgr to the SessMgr.

configure

sgsn-global

    aggregate-ipc-msg { gbmgr | linkmgr | sessmgr } { auto-num-msgs | flush-frequency
        frequency | num-msgs number_msgs } default aggregate-ipc-msg { gbmgr | linkmgr |
        sessmgr }

end

Notes:

- auto-num-msgs enables automated aggregation. Can be set per manager type along with flush frequency but is mutually exclusive with the num-msgs parameter. By default, this function is disabled.
- default resets the selected manager configuration to default values.

CSCuI04175 - S4-SGSN to support R11 agreed CR to avoid SRVCC race condition

Command Changes

apn-type

New command in the APN profile can identify the type of APN as an IMS APN.

configure

    apn-profile profile_name
apn-type ims

remove apn-type ims

end

Notes:

- **apn-type ims** identifies the APN as an IMS APN. This enables the SGSN to delay sending Modify Bearer Request to the S-GW until after receiving the Forward Relocation Complete Ack from the peer during SRNS procedure. By default this identification is disabled.
- **remove** erases this identification configuration from the APN profile and resets to the default.

**CSCul66952 - 2G/3G new counter to measure failure for IMSI identity request.**

**Feature Changes**

**Counters for T3370 timer Modified**

**Previous Behavior:** The T3370 timer has one counter each for 2G and 3G services to indicate the total number of times the T3370 timer timed-out for the service.

**New Behavior:** The T3370 timer has been segregated into following counters based on Identity Type:

- 3G-T3370-Expiry-IMSI
- 2G-T3370-Expiry-IMSI
- 3G-T3370-Expiry-IMEI
- 2G-T3370-Expiry-IMEI
- 3G-T3370-Expiry-IMEISV
- 2G-T3370-Expiry-IMEISV
- 3G-T3370-Expiry-TMSI
- 2G-T3370-Expiry-TMSI
- 3G-T3370-Expiry-Other
- 2G-T3370-Expiry-Other

**Performance Indicator Changes**

**SGSN Schema**

The following T3370 timer bulk statistics are deprecated:

- 3G-T3370-Expiry
- 2G-T3370-Expiry

The following T3370 timer bulk statistics are included, these bulk statistics are identity based:

- 3G-T3370-Expiry-IMSI
• 2G-T3370-Expiry-IMSI
• 3G-T3370-Expiry-IMEI
• 2G-T3370-Expiry-IMEI
• 3G-T3370-Expiry-IMEISV
• 2G-T3370-Expiry-IMEISV
• 3G-T3370-Expiry-TMSI
• 2G-T3370-Expiry-TMSI
• 3G-T3370-Expiry-Other
• 2G-T3370-Expiry-Other

**show gmm-sm statistics**

The following T3370 timer counters are deprecated:

• 3G-T3370-Expiry
• 2G-T3370-Expiry

The following T3370 timer counters are included, these counters are identity based:

• 3G-T3370-Expiry-IMSI
• 2G-T3370-Expiry-IMSI
• 3G-T3370-Expiry-IMEI
• 2G-T3370-Expiry-IMEI
• 3G-T3370-Expiry-IMEISV
• 2G-T3370-Expiry-IMEISV
• 3G-T3370-Expiry-TMSI
• 2G-T3370-Expiry-TMSI
• 3G-T3370-Expiry-Other
• 2G-T3370-Expiry-Other

**CSCum52817 - Do Not establish RAB even if ASI bit is set**

**Feature Changes**

**Ignoring ASI bit when Establishing RAB during RAU-based Handover**

**Previous and Current Behavior:** By default, the SGSN uses the ASI bit in SGSN Context Response to establish RAB during a RAU-based handover.

**New Behavior:** The operator can modify the SGSN service configuration to override the default behavior and configure the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers, and to ignore establishing a RAB for any PDPs.
**Important:** The new CLI will not modify the default behavior for an S4 interface.

**Customer Impact:** Signaling reduction.

**Command Changes**

**sm**

A new CLI keyword `ignore-asi` enables the operator to modify the SGSN service default configuration and instructs the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers over Gn interfaces.

```plaintext
configure
  context context_name
    sgsn-service service_name
      sm ignore-asi
      no sm ignore-asi variable
  end
```

**Notes:**

- Configuring this keyword will be ignored for S4 interfaces.
- `no` disables this new functionality to ignore the ASI bit and returns the SGSN service configuration to use the ASI bit for RAB establishment.

**Performance Indicator Changes**

**show sgsn-service name**

A new field in the `show sgsn-service` output display indicates if the ‘ignore ASI’ functionality has been enabled.

- Ignore ASI bit received from peer SGSN during RAU: Enabled / Disabled

**CSCum53036 - SGW/PGW host names can be displayed in show sub sgsn-only full o/p**

**Performance Indicator Changes**

**show sub [ gprs-only | sgsn-only ] full**

As part of the Topology-based S-GW Selection enhancement (CSCzn60387), now S-GW hostname and P-GW hostname will be displayed in the show output. Following are display fields with sample values:

- **SGW HostName:** topon.s4.sgw.div.bng.kar.3gppnetwork.org
• **PGW HostName**: topon.s5.pgw.div.bng.kar.3gppnetwork.org

**CSCum56947 - Configuration to enable sending extended MBR for UL/DL**

**Feature Changes**

**SGSN Support For Sending Extended Bits Bi-directionally**

**Previous Behavior**: Support for sending extended bitrates in both uplink and downlink directions is absent.

**New Behavior**: Extended bitrates are included in both uplink and downlink direction when the negotiated bitrate indicates that extended bitrates should be included in one direction. A new CLI `ranap bidirectional-always ext-mbr-ie` is added under the RNC Configuration mode to enable sending extended bitrates bi-directionally.

**Command Changes**

```plaintext
ranap bidirectional-always ext-mbr-ie
```

This command enables or disables sending of extended bitrates bi-directionally. When this command is enabled, the specified extended bitrates (MBR or GBR) are included bi-directionally (uplink and downlink directions) in the RAB Assignment Request even if the negotiated bitrate indicates that extended bitrates should be included in one direction.

```plaintext
configure

custom context context_name

    iups-service service_name

         rnc id rnc_id

             ranap bidirectional-always ext-mbr-ie [ext-gbr-ie]

             no ranap bidirectional-always

         end
```

**Notes:**

- When this command is configured, if the maximum bitrate for either uplink or downlink directions indicates that extended bitrates should be included (that is, the maximum bitrate negotiated value exceeds “16” Mbps in either uplink or downlink direction), then the maximum bitrate extended IE is included in both uplink and downlink directions. If in one direction (uplink or downlink) the negotiated value does not exceed “16” Mbps then extended maximum bitrate is sent as “16000001”.

- The keyword `ext-gbr-ie` is included to enable sending of Extended Guaranteed Bitrates IE.

- The `no` form of the command disables sending of both extended MBR and GBR bi-directionally.
CSCum56967 - Security Issue - Encryption on SGSN level

Feature Changes

Failure Action for Random IOV-UI Negotiation Failure

**Previous Behavior:** The SGSN falls back to un-encrypted mode whenever the XID negotiation for Random IOV-UI between the MS and the SGSN fails. This is irrespective of any ciphering algorithm configured.

In order to preserve the connection, the SGSN falls back to default encryption parameters whenever it fails to decipher an encrypted frame that is sent by the MS.

As a result of the above behavior, the MS users could be exposed to passive interception attacks, channel hijacking, or denial of service attacks.

**New Behavior:** In accordance with the 3GPP specification, once the encryption has been started, neither the MS nor the network shall go to an un-ciphered session. Thus, the SGSN’s default behavior to fallback to default IOV-UI is now changed to always reject the call.

In some situations of XID negotiation failure, the SGSN will respond as outlined in either CSCun09183 or CSCun13033.

Command Changes

```
llc random-value-in iov-ui
```

New configuration options, `negotiation-failure-action { fallback-to-default iovui | reject }`, enable the operator to specify the desired failure action to be performed whenever the random IOV-UI negotiation fails. The operator has the option to either

- (a) reject the call whenever the deciphering fails due to the random IOV-UI negotiation failure (thus avoiding a security breach), or
- (b) to fall back to the default IOV-UI.

```
configure

context context_name

gprs-service service_name

llc random-value-in iov-ui [ negotiation-failure-action { fallback-to-default iovui | reject } ]

  default llc random-value-in iov-ui

end
```

Notes:

- **default** resets the SGSN configuration so that all calls are rejected whenever the deciphering fails due to failure of the XID negotiation for random IOV-UI.
- **reject** returns the SGSN to the default configuration to reject all calls when random IOV-UI negotiation fails.
• fallback-to-default iovui allows the operator to return to the previous behavior where the SGSN falls back to un-encrypted mode whenever the XID negotiation for random IOV-UI negotiation fails.

Performance Indicator Changes

show session disconnect-reasons verbose

If configured for ‘Reject’, a new disconnect reason tracks the number of calls cleared due to the new default behavior to reject any call when random IOV-UI negotiation fails.

• sgsn-iovui-negotiation-failure(556)

show gprs-service name

Configuration of this feature can be viewed in the output display of both the show configuration and the show gprs-service with a new display field

• Random IOVUI negotiation failure action:

CSCum69971 - Modify pdp context reject cause different in 2g and 3g for same scenario

Feature Changes

Correct Reject Cause to UE

Previous Behavior: The SGSN sent “Insufficient Resources” to the UE in the Reject message in response to receiving GTP_SERVICE_NOT_SUPPORTED cause code from the GGSN in UPCR.

New Behavior: In UPCR, if the GGSN rejects the request with GTP_SERVICE_NOT_SUPPORTED cause code, then the SGSN sends “service option not supported” to the UE in the Reject message.

This message to the UE more accurately reflects the rejection condition.

CSCum69981 - change in ‘prefer subscription-interface’ in cc profile is not working

Feature Changes

Clarify ‘Preferred Subscription Interface’ Value Display

Previous Behavior: “Preferred Subscription Interface” field displayed the value configured using prefer subscription-interface { hss | hlr } command when both MAP and HSS service configuration were associated to a call control profile. When only one service was present (either MAP or HSS) or when remove prefer subscription-interface command was executed, the displayed value for the “Preferred Subscription Interface” field displayed the service on which the call would proceed.
New Behavior: “Preferred Subscription Interface” field always displays the value configured using the `prefer subscription-interface { hss | hlr }` command, even if there is only one service associated under the call control profile. If the `remove prefer subscription-interface` command is executed, then a value for the “Preferred Subscription Interface” field is not be displayed.

**CSCum94531 - Handle negative scenarios in MAP**

**Feature Changes**

**Behavior Changes to Handle Various MAP Scenarios**

**Previous Behavior:**
- When the subscriber was registered with the HSS, then received MAP ISDs and DSDs were processed.
- Received MAP standalone ISDs containing EPS Subscription Data, with an APN Configuration Profile containing an EPS Data List of Length 0 or of value NULL, were accepted and processed.
- Received MAP standalone ISDs containing GPRS Subscription Data, with a GPRS Data List of Length 0 or of value NULL, were accepted and processed.

**New Behavior:**
- When the subscriber is registered with the HSS, then received MAP standalone ISDs and DSDs are dropped.
- Received MAP standalone ISDs containing EPS Subscription Data, with an APN Configuration Profile containing an EPS Data List of Length 0 or of value NULL, will not be processed and an error with cause “Data Missing” will be returned.
- Received MAP standalone ISDs containing GPRS Subscription Data, with a GPRS Data List of Length 0 or of value NULL, will not be processed and an error with cause “Data Missing” will be returned.

**CSCun09183 - SGSN should not cleanup the subscriber when XID exchange times out**

**Feature Changes**

**Subscriber Moves to STANDBY for XID Negotiation Failure**

**Previous Behavior:** As a result of XID for random IOV-UI negotiation failure during intra-RAU or standalone authentication for SMS, the SGSN clears the subscriber.

**New Behavior:** Now, when XID for random IOV-UI negotiation failure occurs during intra-RAU or standalone authentication for SMS, the SGSN moves the subscriber to STANDBY and marks the XID negotiation as a failure.

In some situations of XID negotiation failure, the SGSN will respond as outlined in CSCun13033.
CSCun13033 - Detach request is not triggered in following scenario

Feature Changes

Changes to handling of failures of XID negotiation for random IOV-UI are also incorporated into related issues CSCum56967 and CSCun09183.

Responses to XID Negotiation Failure

**Previous Behavior:** SGSN clears the subscriber based on the configured negotiation failure action if the previous XID negotiation for random IOV-UI fails upon receiving any uplink packets whether ciphered or un-ciphered.

**New Behavior:** The SGSN manner of handling failure of XID negotiation for random IOV-UI has been modified, so that now the SGSN:

- Initiates XID for new random IOV-UI negotiation:
  1. with the MS is in STANDBY state, any uplink packet (in either ciphered or un-ciphered mode, except Attach / Intra-RAU) from the MS which results in CELL-UPDATE, READY TIMER START and RADIO STATUS READY causes an event indication to the application.

- Initiates Detach:
  1. with the MS is in STANDBY state, any uplink activity causes the SGSN to initiate a new XID exchange, which if it fails or aborts due to the reception of SUSPEND, RADIO-STATUS and READY-TIMER expiry, results in the SGSN initiating Detach.
  2. when PAGING is ongoing, any Page response from the MS results in the SGSN initiating Detach.
  3. during OLD_SGSN ISRAU, when any uplink data comes before T3 tunnel timer expiry then the SGSN initiates Detach.

- Handles Messages:
  1. Attach and intra-RAU (from both local and non-local TLLI or from both the same and different RA) will be processed in any state.

- Moves to STANDBY state:
  1. MS is moved to STAND-BY state if the XID exchange failed due to any of the following cases suspend, radio status, BVC block, BVC reset, ready timer expiry, no response received for XID exchange during INTRA-RAU/Standalone Authentication for SMS.
  2. XID is ongoing in READY state and if the MS moves to either 3G or to the peer-SGSN then the subscriber is moved to STANDBY state.

Also, all the uplink packets received from the MS (like ACTIVATE, ACTIVATE SECONDARY PDP, DE-ACTIVATE, MODIFY, SMS) will be dropped and the XID message will be retried whenever the XID is ongoing in READY STATE. Whenever the SGSN initiates the XID in READY state, it informs the GTP to stop forwarding the data if any is received for that MS. Upon the reception of XID response in READY state, GTP will be informed to start forwarding the data queued, if there is any.
CSCun22601 - In GPRS-Service ‘No GMM IMPLICITE-DETACH-INDICATION’ should be Added

Feature Changes

IDT and T3323-timeout Configuration Coordination

**Previous Behavior:** Configuration of GMM T3323-timeout in the GPRS service was allowed even if implicit-detach-timeout (IDT) under the `gmm` command in the GPRS service is not configured.

**New Behavior:** SGSN behavior has been modified so that configuration of GMM T3323-timeout in the SGSN service is not allowed if implicit-detach-timeout under `gmm` in GPRS service is not configured.

**Customer Impact:** Adjustment for T3323 and IDT should be done properly, and if IDT is not configured, then configuration of T3323 is not permitted. If attempted the SGSN generates an error message.

CSCun69966 - Need support to clear RLF context level statistics by RLF framework

Feature Changes

Support to Clear RLF Context Level Statistics

**Previous Behavior:** RLF context level statistics by RLF framework cannot be cleared.

**New Behavior:** A new CLI command `clear sgsn rlf-context-stats sessmgr { all | instance <instance_value> } [ peer-nsei-id <NSE_identifier> | peer-rnc-id <RNC_identifier> ] [ | { grep grep_options | more } ]` is introduced to clear the Paging throttle RLF context statistics.

Command Changes

`clear sgsn rlf-context-stats`

A new CLI command is introduced to clear the RLF context level statistics.

`exec`

```
clear sgsn rlf-context-stats sessmgr { all | instance <instance_value> } [ peer-nsei-id <NSE_identifier> | peer-rnc-id <RNC_identifier> ] [ | { grep grep_options | more } ]
```

**Notes:**

- This command can be configured to clear the Paging throttle RLF context statistics for:
  - All the Session Managers.
  - The specified Session Manager.
  - The specified Peer NSEI.
• The specified Peer RNC.
• The keyword `sessmgr` is a mandatory keyword. Specifying the `peer-nsei-id` or `peer-rnc-id` is optional. When the `peer-nsei-id` or `peer-rnc-id` is not specified the global statistics are cleared. If the Session Manager instance is specified, the RLF context statistics for that Session Manager are cleared. If the keyword `all` is configured the RLF statistics for all the Session Managers are cleared.

CSCzn60387 - [S4-SGSN] S4-SGSN shall support topology based SGW selection

Feature Changes

Topological Gateway Selection for the S4-SGSN

During primary PDP context activation for a UE in an EPC network, the SGSN does P-GW selection first for the given APN and then the SGSN selects the S-GW for the RAI FQDN.

Topology-based S-GW / P-GW selection is a mechanism defined by 3GPP TS 29.303 to choose a gateway based on the geographical (topological) proximity of the P-GW to the S-GW. The two being co-located would have the highest priority. Topology-based selection is not allowed for roamers connected to HPLMN access points (Home Routed Scenario).

DNS S-NAPTR returns a candidate list of GW nodes for each of the DNS queries. 3GPP TS 29.303 provides an algorithm to feed these candidate lists and choose the topologically closer nodes among them.

The SGSN’s Topology-based GW Selection feature supports two levels of sorting, first level is degree and second level is order/priority, where order is for NAPTR records and priority is for SRV Records. Degree has the highest preference.

When enabled with the new call control profile CLI (see below), the S4-SGSN can use topological selection of a GW during any of the following call flows for 2G, 3G, or both:

• First Primary Activation
• Subsequent Primary Activation
• INTRA RAU
• INTRA SRNS
• NEW INTER SGSN RAU
• NEW INTER SGSN SRNS
• IRAT

With this release, the Gn/Gp-SGSN now supports S-NAPTR-based DNS query (see CSCub16578). The Gn/Gp-SGSN can perform Topological Gateway Selection by using the DNS query to select a topologically closer GGSN or a co-located PGW.

For more details about this feature, refer to the Topology-based Gateway Selection feature section in the SGSN Administration Guide.

Customer Impact: Selecting a co-located or topologically-close gateway (GW) node results in lower latency and prevents unnecessary traversal of the packets in the network.
Command Changes

gw-selection

The `gw-selection` command in the call control profile configuration mode is new for the SGSN. This command configures the parameters controlling the gateway selection process for both the Gn/Gp-SGSN and the S4-SGSN.

```plaintext
call-control-profile profile_name

gw-selection { { co-location | pgw weight | sgw weight | topology } [ weight [ prefer { pgw | sgw } ] ] }

remove gw-selection { co-location | pgw | sgw | topology }

end
```

Notes:
- **co-location** enables the SGSN to select topologically closer P-GW and S-GW nodes, irrespective of the ‘topon’ or ‘topoff’ prefix being present in the hostname received in the results of the DNS query.
- **pgw weight** enables the SGSN to apply load balancing during selection of P-GW nodes.
- **sgw weight** enables the SGSN to apply load balancing during selection of S-GW nodes.
- **topology** enables the SGSN to select topologically closer P-GW and S-GW nodes, only when ‘topon’ prefix is present in the hostname received as part of the DNS query results.
- **weight** enables load balancing during selection of a node. When topology is applicable, **weight** instructs the SGSN to apply weight-based selection only on node pairs with the same degree and order.
- **prefer** instructs the SGSN to consider weight values for preferred GW type (P-GW or S-GW) during the first primary activation.
- **remove** erases the GW selection configuration from the call control profile.

For command usage information, see the `gw-selection` information in the *Call-Control Profile Configuration Mode* section of the *Command Line Reference*.

canonical-node-name

In order for the Gn/Gp-SGSN to support Topological Gateway Selection, the SGSN’s canonical node name must be defined in the SGSN’s configuration. (This is not needed for the S4-SGSN).

```plaintext
sgsn-global

canonical-node-name canonical_node_name

no canonical-node-name canonical_node_name

end
```

Notes:
CSCzn60731 - Ignoring PDP Inactivity configuration for one or more IMEIs

Feature Changes

SGSN support to Ignore PDP Data Inactivity

The SGSN supports options to configure PDP Data Inactivity detection duration and actions to be performed on timeout under the APN-Profile. The following configurable actions are supported under APN-Profile in case of PDP Data Inactivity detection in the PDP context:

1. De-activate all PDPs of the subscriber
2. De-activate all PDPs of the bundle (all linked PDPs)
3. Detach the subscriber. This action is triggered when:
   - Data in-activity is detected for all PDPs
   - Data in-activity is detected for any of the PDPs

On the Detection of the PDP Data Inactivity, depending on the configuration option the SGSN either de-activates the PDP or detaches the subscriber.

A new CLI `ignore-pdp-data-inactivity` is added to provide an option under the IMEI-Profile to ignore PDP Data Inactivity configuration for one or more IMEIs. On configuring this CLI, the SGSN ignores the application of in-activity configuration (configured in the APN-Profile) for a specified set of IMEIs.

Command Changes

`ignore-pdp-data-inactivity`

A new CLI `ignore-pdp-data-inactivity` is added to provide an option under the IMEI-Profile to ignore PDP Data Inactivity configuration for one or more IMEIs. On configuring this CLI, the SGSN ignores the application of in-activity configuration (configured in the APN-Profile) for a specified set of IMEI's.

```plaintext
configure

imei-profile profile_name

ignore-pdp-data-inactivity

remove ignore-pdp-data-inactivity

end
```

Performance Indicator Changes

`show imei-profile full name <imei-profile name>`
A new field with either 'Enabled' or 'Disabled' options has been added to the output of the command `show imei-profile full name <imei-profile name>` to indicate whether or not ignore PDP data inactivity functionality has been configured:

- Ignore PDP Data Inactivity
This chapter identifies features and functionality added to, modified for, or deprecated from S-GW in StarOS 16 software releases.
S-GW Enhancements for 16.5

There are no S-GW enhancements for this release.
S-GW Enhancements for 16.4

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

---

CSCup48554, CSCuq10884 - SGW should allow partial context Replacement

**Applicable Products:** S-GW

**Feature Changes**

**Partial Context Replacement Support on the S-GW**

As per existing requirements, a SGW accepts an incoming Create Session Request message colliding with an existing PDN connection context only if is received with the TEID 0 in the GTP-C header.

This can result in a failure to establish a PDN connection or move a PDN connection to a new SGW, in those error scenarios where a UE context already exists in both the MME/SGSN and SGW, and where a new Create Session Request is received by the SGW with a non-zero TEID which collides with an existing PDN connection context in the SGW. It does not help that the SGW rejects the Create Session Request if it collides with an existing PDN connection...
and the received TEID is not zero, because if the MME sends a Create Session Request (IMSI, EPS Bearer Id), this is already an indication that no corresponding PDN connection exists yet in the MME for that tuple.

To resolve this issue, the SGW now accepts a Create Session Request with a non-zero TEID colliding with an existing PDN connection and then clears the existing PDN connection in the following scenarios:

1. ISR is active on the UE.
2. Any procedure such as Create Bearer Request is pending on the UE.
3. Procedure is anything other than “UE Requested PDN Connection.”

This feature is enabled and embedded by default.

**Previous Behavior:** SGW accepts an incoming Create Session Request message colliding with an existing PDN connection context only if is received with the TEID 0 in the GTP-C header.

**New Behavior:** The SGW now accepts a Create Session Request with a non-zero TEID colliding with an existing PDN connection and then clears the existing PDN connection.

**Customer Impact:** This benefits customers because in pre-16.4.x releases there was no way for the MME and SGW to come back in synchronization. This feature allows partial context replacement and thus brings the MME and S-GW back in synchronization again.

### Performance Indicator Changes

**show egtpc statistics mme-address mme-address verbose**

The output of this command has been enhanced to provide statistics related to the Partial Context Replacement feature.

- Partial Context Replacement Statistics:
  - Additional PDN Connection Context Replacement:
S-GW Enhancements for 16.3

There are no S-GW enhancements in this release.
S-GW Enhancements for 16.2

This section identifies all of the S-GW enhancements included in this release:

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

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

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

---

**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

---

CSCuo09385 - S-GW session recovery not working post unplanned Demux MIO swover

**Applicable Products**: S-GW

**Feature Changes**

**Modification to Demux Manager**

The fix to CSCuo09385 has resulted in a behavior change.

**Previous Behavior**: The following CLI commands output the manager instance ID in sequence beginning with 1:

- `show task resources facility egtpinmgr all`
- `show task resources facility egtpegmgr all`
• `show task resources facility gtpumgr all`

**New Behavior:** The demux manager instance id will be the VPN-ID of a specific context. The VPN-ID can be obtained by using the `show context` command in Exec Mode.
S-GW Enhancements for 16.1

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

---

CSCuj86237 - Inaccurate SGW session stats on standby ASR

**Applicable Products**: S-GW

**Feature Changes**

**Correction to Inaccurate S-GW Session Statistics on Standby S-GW**

A behavior change has been introduced as part of the fix for CSCuj86237.

**Previous Behavior**: Previously, the system incremented active and setup counters on a standby S-GW for S-GW service statistics when they should only be incremented on the Active S-GW. Similarly, active, setup and release counters were incremented on standby the Standby S-GW for S-GW statistics and the S-GW sent these incremented counters in bulk statistics.

**New Behavior**: The software has been modified so that the Standby S-GW does not increment setup, release counters for S-GW service statistics and S-GW statistics. They will be incremented only when the Standby S-GW becomes
Active. Active counts are incremented on the Standby S-GW but in bulk statistics the S-GW sends active counters as 0 (zero), while the setup and release counts may be non-zero. Bulk statistics setup and release counters will reflect counts when this S-GW was last in the Active state.

**Customer Impact:** Previously, for a single call the customer would receive double the actual counter total Active and Standby statistics were added together. The counters now are incremented on the currently Active S-GW only, so the counter total is correct.

**CSCul24516 - show sub subsystem stats incorrect**

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

**Feature Changes**

**Enhancements to S-GW for RAT Based Counters**

The S-GW software has been enhanced to provide more granularity for RAT based counters for the various types of subscribers on the S-GW. Specifically, these counters are implemented for more visibility into 2G/3G calls via the S4-SGSN.

**Performance Indicator Changes**

**S-GW Schema**

The S-GW bulk statistics schema has been enhanced with the following to support the RAT based counters:

- ssessstat-totcur-ue-eutran
- ssessstat-totcur-ue-utran
- ssessstat-totcur-ue-geran
- ssessstat-totcur-ue-other
- ssessstat-totcur-pdn-eutran
- ssessstat-totcur-pdn-utran
- ssessstat-totcur-pdn-geran
- ssessstat-totcur-pdn-other

**SAEGW Schema**

The SAEGW bulk statistics schema has been enhanced with the following to support the RAT based counters:

- sgw-sessstat-totcur-ue-eutran
- sgw-sessstat-totcur-ue-utran
- sgw-sessstat-totcur-ue-geran
- sgw-sessstat-totcur-ue-other
- sgw-sessstat-totcur-pdn-eutran
- sgw-sessstat-totcur-pdn-utran
- sgw-sessstat-totcur-pdn-geran
- sgw-sessstat-totcur-pdn-other

**show subscriber sgw-only summary**

The output of this command has been enhanced to provide various PDN RAT Type counters for 4G and non-4G subscribers:

- Total Subscribers by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - OTHER

- Total PDNs by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - OTHER

**show subscriber sgw service statistics all**

The output of this command has been enhanced to provide current session counts based on RAT type.

- Current Subscribers by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - OTHER

- Current PDNs by RAT-Type
  - EUTRAN
  - UTRAN
  - GERAN
  - OTHER

**CSCuo09385 - SGW session recovery not working post unplanned Demux MIO swover**

Applicable Products: S-GW
Feature Changes

Behavior Change Due to Implementation of Fix for CSCuo09385

A behavior change was implemented as part of the fix for CSCuo09385.

**Previous Behavior:** The following CLI commands output the demux manager instance ID in numerical order beginning with 1 as the first instance:

- `show task resources facility egtpinmgr all`
- `show task resources facility egtpegmgr all`
- `show task resources facility gtpumgr all`

**New Behavior:** The demux manager instance ID now will be the VPN-ID of the given context. The VPN-ID can be obtained by using the `show context` command. Note that change in the demuxmgr instance does not affect any functionality.
S-GW Enhancements for 16.0

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

---

**CSCug83805 - InTracer Support: Auto and more simultaneous traces - S-GW**

**Feature Changes**

**InTracer Support for Auto-next-call and More Configurable Traces on the S-GW**

The system 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

**CSCuh25810 - SGW Session Idle Timer**

**Feature Changes**

**S-GW Session Idle Timer**

A session idle timer has been implemented on the S-GW to remove stale session in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down those sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

This feature is supported only for Pure S calls on the SAE-GW.

**Important:** The session idle timer feature will not work if the Fast Data Path feature is enabled.

**Command Changes**

```plaintext
timeout idle
```

This new command has been added to SGW Service Configuration Mode to tear down SGW sessions that remain idle for longer than the configured time limit.

```plaintext
configure
context context_name
sgw-service sgw_service_name
    timeout idle dur_seconds
no timeout idle
default timeout idle
end
```

**Notes:**

- `idle` `dur_seconds` specifies the time limit, in seconds, after which the SGW session will be torn down. Valid entries are from 0 to 4294967295.
- `no` disables the SGW session idle timer.
- `default` returns the SGW session idle timer to the default value of 0 (disabled).

**Performance Indicator Changes**

```plaintext
show sgw-service name
```
This command has been enhanced to indicate if the SessionIdle Timer feature is enabled on the S-GW.

- Idle timeout: 0...n secs/(n/a)

**show sgw-service statistics all**

This command has been enhanced to indicate if the Session Idle Timer feature is enabled on the S-GW:

- Released:
  - Idle timeout: 0...n secs
  - Idle timeout: (n/a)

**CSCuh35193 - SGW ASSERT removal**

**Feature Changes**

**Enhanced Validity Checks in S-GW APIs**

To more fully support EGTPC Assert removal activity, the S-GW software has been enhanced to return specific failure reasons in such cases and the S-GW will help clean up the particular CLP locally.

**S-GW Schema**

To support EGTPC Assert removal activity, the following bulkstats have been added to the S-GW schema:

- lcl-cleanup-bearer-not-in-same-state
- lcl-cleanup-bearer-not-in-correct-state
- lcl-cleanup-dup-data-teid
- lcl-cleanup-remote-addr-not-compatible
- lcl-cleanup-bad-peer
- lcl-cleanup-bearer_ctxt-missing

**Performance Indicator Changes**

**show sgw-service statistics all verbose**

The following statistics have been added to this command to indicate specific reasons for EGTPC Assert removal activity:

- Local Call Cleanup Cause Statistics
  - Bearer Not In Same State
  - Bearer Not in Correct State
  - Duplicate Data Teid
  - Remote Addr Not Compatible
- Bad Peer
- Bearer Missing Context

**CSCuh71727, CSCui42572 - Error response handling at SGW**

**Feature Changes**

**Improved Error Response Handling at the S-GW**

The software has been enhanced to improve error response handling at the S-GW when an erroneous message is received by EGTPC from a peer. On receiving a bad response from the peer, instead of dropping the message while doing validation, EGTPC informs the S-GW about the bad response received. The S-GW uses this notification from EGTPC that a bad response is received to send a proper response to the other peer. This will reduce load on the S-GW due to retransmissions. This also helps in capturing statistics based on the correct cause code.

**Previous Behavior:** When an erroneous response message is received by the S-GW EGTPC service from a peer, it is dropped while performing validation. After all retries of the request message, the EGTPC service then informs the other peer that there was no response from the peer.

**New Behavior:** If error-response-handling is enabled, and EGTPC receives the first error response, it now sends back *Invalid reply from remote peer* in the response message to the other peer.

**Customer Impact:** There will be no request message retries if the error response is received.

**Command Changes**

```
gtpc error-response-handling
```

The new command `gtpc error-response-handling` has been added to *EGTP Service Configuration Mode*. This command controls error response handling at the S-GW when an erroneous message is received by EGTPC from a peer.

```
context context_name

egtp-service egtp_service_name

  gtpc error-response-handling
  no gtpc error-response-handling

end
```

**Notes:**

- If this command is enabled in the egtp-service then on receiving a bad response from the peer instead of dropping the message while doing validation EGTPC informs the S-GW about the bad response received. The S-GW uses this notification from EGTPC that a bad response is received to send a proper response to the other peer.
- **no** disables the Error Response handling feature. The default setting is disabled.
CSCui04167 - PGW LORC mechanism for subscriber billing

Feature Changes

Overcharging Protection on the S-GW

Consider the following scenario:

1. When a subscriber has an active session and loses coverage or when the subscriber is Idle, the P-GW is not aware of the subscriber state.
2. If there is valid Downlink Data for the subscriber, the P-GW forwards the data to the S-GW and counts the data towards appropriate Rf and Gy records.
3. In scenarios when the subscriber loses RF coverage or when the subscriber is not reached via paging, the data is dropped at the S-GW and causes an overcharge to users.

The software has been enhanced so that the P-GW stops billing of the data in such scenarios. The S-GW notifies the P-GW of the subscriber state about when to pause and resume charging of the subscriber, this will reduce the overcharging of the subscriber.

**Customer Impact:** Huge reduction in overcharging by the P-GW in the above scenarios. This feature is supported only for Pure S calls on the SAE-GW.

Command Changes

```plaintext
gtpc private-extension overcharge-protection
```

The new command `gtpc private-extension overcharge-protection` has been added to *EGTP Service Configuration Mode*. This command controls whether the PDU will contain Overcharge-protection related data in the Indication IE or private extension. An Overcharge-protection license is required to use enable this feature.

```plaintext
configure

context context_name

egtp-service egtp_service_name

    gtpc private-extension overcharge-protection

    no gtpc private-extension overcharge-protection

end
```

Notes:

- `no` disables private extension overcharge protection. If this option is not enabled in the egtp-service, then by default the EGTPC layer will encode/decode overcharge-protection related data in the Indication information element. The default setting is disabled.
- If this command is enabled in the egtp-service then EGTPC will encode/decode overcharge-protection related data in/from the private extension instead of the Indication information element.

**Important:** An Overcharge-protection license is required to enable this feature. In addition, overcharge protection must be configured in *APN Profile Configuration Mode* using the `overcharge-protection` command to use this feature.
Performance Indicator Changes

show egtp-service name

This command has been enhanced to list the private-extension overcharge-protection setting on the S-GW, if configured.

- GTPC Private Extension
  - Overcharging Protection (Seconds): Enabled or Disabled

CSCui04214 - Dedicated bearer timeout action

Feature Changes

Dedicated Bearer Timeout Support on the S-GW

Important: For this release, this feature is Lab/Trial Quality only.

The S-GW has been enhanced to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value.

Customer Impact: Operators now can configure a bearer inactivity timeout for GBR and non-GBR bearers for more efficient use of system resources. This feature is supported only for Pure S calls on the SAE-GW.

Command Changes

timeout bearer-inactivity

The new command timeout bearer-inactivity supports a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions.

configure

apn-profile apn_profile_name

    timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { total bytes | uplink bytes | downlink bytes } | exclude-default-bearer

    remove timeout bearer-inactivity [ gbr | non-gbr ]

end

Notes:

- timeout: Specifies that a session time out value will be configured for this APN profile.
- bearer-inactivity: Specifies that the system will check for low activity for a bearer.
- gbr: Specifies that the system will check for low activity on a GBR bearer.
- non-gbr: Specifies that the system will check for low activity on a non-GBR bearer.
- **dur_seconds**: Specifies the timeout for the gbr or non-gbr bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).

- **volume-threshold**: Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.

- **total**: Specifies that the total of both uplink and downlink data will be used as a volume threshold. *bytes* must be a value from 1 to 4294967295.

- **uplink**: Specifies that an uplink data volume threshold will be used. *bytes* must be a value from 1 to 4294967295.

- **downlink**: Specifies that a downlink data volume threshold will be used. *bytes* must be a value from 1 to 4294967295.

- **exclude-default-bearer**: Specifies that inactivity handling for the default bearer will be excluded.

### Performance Indicator Changes

#### show apn-profile full name

This command has been enhanced to list bearer inactivity timeout settings, if configured.  
- **Bearer inactivity timeout:**
  - Exclude default bearer : Yes/No
  - GBR:
    - Timeout (Seconds) : *seconds*
    - Threshold (Bytes) : *bytes*
    - Direction : Downlink/Uplink/Bi-directional
  - non-GBR:
    - Timeout (Seconds) : *seconds*
    - Threshold (Bytes) : *bytes*
    - Direction : Downlink/Uplink/Bi-directional

#### show sgw-service-statistics all verbose

This command has been enhanced to list bearer inactivity timeout settings, if configured.  
- **Inactivity timeout:**
  - QCI 1: : *seconds*
  - QCI 2: : *seconds*
  - QCI 3: : *seconds*
  - QCI 4: : *seconds*
  - QCI 5: : *seconds*
  - QCI 6: : *seconds*
  - QCI 7: : *seconds*
• QCI 8: seconds
• QC9 1: seconds
• Non-Std QCI: seconds

S-GW Schema

To support Dedicated Bearer Timeout Support on the S-GW, the following bulkstats have been added to the S-GW schema:

- totepsbearrel-dedrsn-inactivity-timeout
- totepsbearrel-dedrsn-inactivity-timeout-qci1
- totepsbearrel-dedrsn-inactivity-timeout-qci2
- totepsbearrel-dedrsn-inactivity-timeout-qci3
- totepsbearrel-dedrsn-inactivity-timeout-qci4
- totepsbearrel-dedrsn-inactivity-timeout-qci5
- totepsbearrel-dedrsn-inactivity-timeout-qci6
- totepsbearrel-dedrsn-inactivity-timeout-qci7
- totepsbearrel-dedrsn-inactivity-timeout-qci8
- totepsbearrel-dedrsn-inactivity-timeout-qci9
- totepsbearrel-dedrsn-inactivity-timeout-qci-other

CSCui21603 - SGW Honor ingress & egress DSCP & Support DSCP marking @ APN profile

Feature Changes

Support for Honoring DSCP Ingress and Egress and DSCP Marking at the APN Profile

This feature will provide an operator with a configuration to set the DSCP value per APN profile, so different APNs can have different DSCP markings as per QOS requirements for traffic carried by the APN. In addition, the qci-qos mapping table is updated with the addition of a copy-outer for copying the DSCP value coming in the encapsulation header from the S1u interface to the S5 interface and vice-versa.

This feature is supported only for Pure S calls on the SAE-GW.

Previous Behavior:

1. The qci-qos mapping table was previously fetched from service.
2. The DSCP value in the encapsulated header was not getting relayed from s1-s5 and vice versa. Instead, a value of 0 (zero) was sent in the encapsulation header.

New Behavior:

1. The qci-qos-mapping table will be fetched from the APN profile first. If there is no association in the apn-profile for the qci-qos-mapping table then the service level configuration will be fetched for the qci-qos mapping table.
2. The DSCP value in the encapsulated header will be relayed from s1-s5 and vice versa using the `copy-outer` option in the `qci-qos-mapping` table.

**Command Changes**

`associate qci-qos-mapping`

The `qci-qos-mapping` keyword has been added to the `associate` command in APN Profile Configuration Mode to associate a QCI QOS mapping table with an APN profile.

```
configure
  apn-profile apn_profile_name
  associate qci-qos-mapping mapping_table_name
  remove associate qci-qos-mapping
end
```

Notes:
- `mapping_table_name` is the name of the QCI QOS mapping table that you want to associate with this APN profile.
- `remove` specifies that the association to the QCI QOS mapping table is to be deleted.

`qci`

The `copy-outer` keyword has been added to the `qci` command in *Global Configuration Mode*. Enabling this feature for copying the DSCP value coming in a data packet from S1u to the data packet sent on the S5 interface and vice-versa.

```
configure
  qci-qos-mapping mapping_table_name
    qci number downlink encaps-header copy-outer
    qci number uplink encaps-header copy-outer
end
```

Notes:
- `copy-outer` instructs the S-GW to copy the DSCP value coming in an encapsulation header from the S1u interface to the encapsulation header sent on the S5 interface and vice-versa.

**Performance Indicator Changes**

`show qci-qos mapping table name`

The output of this command has been enhanced to indicate if the `copy-outer` option is enabled for uplink and downlink in the QCI QOS table.
• uplink: user-datagram dscp-marking xxxx encaps-header copy-outer
• downlink: user-datagram dscp-marking xxxx encaps-header copy-outer

**show apn-profile full all**

The output of this command has been enhanced to indicate if a QCI QOS mapping table is associated with a given APN profile configuration.

- APN Profile Name
  - QCI-QOS mapping table :<QCI QOS table name>

**CSCui21610 - Dropped call counters granularity**

**Feature Changes**

**Increased Granularity for Bearer Released Reason and Drop Type**

The system has been enhanced to provide more detailed and granular output to report the reasons for dropped calls, specifically for IMS dropped calls/bearer/Qos Class Identifier (QCI).

**Customer Impact:** More granular reporting of dropped calls/ bearers counters is supported. This feature is especially useful for troubleshooting and tracking VoLTE field performance.

**Performance Indicator Changes**

**S-GW Schema**

The following bulkstats have been added to the S-GW schema to support increased granularity for bearer released reason and drop type.

- totepsbearrel-dedrsn-pgw
  - totepsbearrel-dedrsn-pgw-qci1
  - totepsbearrel-dedrsn-pgw-qci2
  - totepsbearrel-dedrsn-pgw-qci3
  - totepsbearrel-dedrsn-pgw-qci4
  - totepsbearrel-dedrsn-pgw-qci5
  - totepsbearrel-dedrsn-pgw-qci6
  - totepsbearrel-dedrsn-pgw-qci7
  - totepsbearrel-dedrsn-pgw-qci8
  - totepsbearrel-dedrsn-pgw-qci9
  - totepsbearrel-dedrsn-pgw-qci-other
- totepsbearrel-dedrsn-s1err
  - totepsbearrel-dedrsn-s1err-qci1
- totepsbearrel-dedrsn-s1err-qci2
- totepsbearrel-dedrsn-s1err-qci3
- totepsbearrel-dedrsn-s1err-qci4
- totepsbearrel-dedrsn-s1err-qci5
- totepsbearrel-dedrsn-s1err-qci6
- totepsbearrel-dedrsn-s1err-qci7
- totepsbearrel-dedrsn-s1err-qci8
- totepsbearrel-dedrsn-s1err-qci9
- totepsbearrel-dedrsn-s1err-qci-other

- totepsbearrel-dedrsns5err
  - totepsbearrel-dedrsn-s5err-qci1
  - totepsbearrel-dedrsn-s5err-qci2
  - totepsbearrel-dedrsn-s5err-qci3
  - totepsbearrel-dedrsn-s5err-qci4
  - totepsbearrel-dedrsn-s5err-qci5
  - totepsbearrel-dedrsn-s5err-qci6
  - totepsbearrel-dedrsn-s5err-qci7
  - totepsbearrel-dedrsn-s5err-qci8
  - totepsbearrel-dedrsn-s5err-qci9
  - totepsbearrel-dedrsn-s5err-qci-other

- totepsbearrel-dedrsn-s4err
  - totepsbearrel-dedrsn-s4err-qci1
  - totepsbearrel-dedrsn-s4err-qci2
  - totepsbearrel-dedrsn-s4err-qci3
  - totepsbearrel-dedrsn-s4err-qci4
  - totepsbearrel-dedrsn-s4err-qci5
  - totepsbearrel-dedrsn-s4err-qci6
  - totepsbearrel-dedrsn-s4err-qci7
  - totepsbearrel-dedrsn-s4err-qci8
  - totepsbearrel-dedrsn-s4err-qci9
  - totepsbearrel-dedrsn-s4err-qci-other

- totepsbearrel-dedrsn-s12err
  - totepsbearrel-dedrsn-s12err-qci1
  - totepsbearrel-dedrsn-s12err-qci2
- totepsbearrel-dedrsn-s12err-qci3
- totepsbearrel-dedrsn-s12err-qci4
- totepsbearrel-dedrsn-s12err-qci5
- totepsbearrel-dedrsn-s12err-qci6
- totepsbearrel-dedrsn-s12err-qci7
- totepsbearrel-dedrsn-s12err-qci8
- totepsbearrel-dedrsn-s12err-qci9
- totepsbearrel-dedrsn-s12err-qci-other

- totepsbearrel-dedrsn-local
  - totepsbearrel-dedrsn-local-qci1
  - totepsbearrel-dedrsn-local-qci2
  - totepsbearrel-dedrsn-local-qci3
  - totepsbearrel-dedrsn-local-qci4
  - totepsbearrel-dedrsn-local-qci5
  - totepsbearrel-dedrsn-local-qci6
  - totepsbearrel-dedrsn-local-qci7
  - totepsbearrel-dedrsn-local-qci8
  - totepsbearrel-dedrsn-local-qci9
  - totepsbearrel-dedrsn-local-qci-other

- totepsbearrel-dedrsn-pdn
  - totepsbearrel-dedrsn-pdn-qci1
  - totepsbearrel-dedrsn-pdn-qci2
  - totepsbearrel-dedrsn-pdn-qci3
  - totepsbearrel-dedrsn-pdn-qci4
  - totepsbearrel-dedrsn-pdn-qci5
  - totepsbearrel-dedrsn-pdn-qci6
  - totepsbearrel-dedrsn-pdn-qci7
  - totepsbearrel-dedrsn-pdn-qci8
  - totepsbearrel-dedrsn-pdn-qci9
  - totepsbearrel-dedrsn-pdn-qci-other

- totepsbearrel-dedrsn-pathfail-s1-u
  - totepsbearrel-dedrsn-pathfail-s1-u-qci1
  - totepsbearrel-dedrsn-pathfail-s1-u-qci2
  - totepsbearrel-dedrsn-pathfail-s1-u-qci3
• totepsbearrel-dedrsn-pathfail-s1-u-qci4
• totepsbearrel-dedrsn-pathfail-s1-u-qci5
• totepsbearrel-dedrsn-pathfail-s1-u-qci6
• totepsbearrel-dedrsn-pathfail-s1-u-qci7
• totepsbearrel-dedrsn-pathfail-s1-u-qci8
• totepsbearrel-dedrsn-pathfail-s1-u-qci9
• totepsbearrel-dedrsn-pathfail-s1-u-qci-other

• totepsbearrel-dedrsn-pathfail-s5-u
  • totepsbearrel-dedrsn-pathfail-s5-u-qci1
  • totepsbearrel-dedrsn-pathfail-s5-u-qci2
  • totepsbearrel-dedrsn-pathfail-s5-u-qci3
  • totepsbearrel-dedrsn-pathfail-s5-u-qci4
  • totepsbearrel-dedrsn-pathfail-s5-u-qci5
  • totepsbearrel-dedrsn-pathfail-s5-u-qci6
  • totepsbearrel-dedrsn-pathfail-s5-u-qci7
  • totepsbearrel-dedrsn-pathfail-s5-u-qci8
  • totepsbearrel-dedrsn-pathfail-s5-u-qci9
  • totepsbearrel-dedrsn-pathfail-s5-u-qci-other

• totepsbearrel-dedrsn-pathfail-s5
  • totepsbearrel-dedrsn-pathfail-s5-qci1
  • totepsbearrel-dedrsn-pathfail-s5-qci2
  • totepsbearrel-dedrsn-pathfail-s5-qci3
  • totepsbearrel-dedrsn-pathfail-s5-qci4
  • totepsbearrel-dedrsn-pathfail-s5-qci5
  • totepsbearrel-dedrsn-pathfail-s5-qci6
  • totepsbearrel-dedrsn-pathfail-s5-qci7
  • totepsbearrel-dedrsn-pathfail-s5-qci8
  • totepsbearrel-dedrsn-pathfail-s5-qci9
  • totepsbearrel-dedrsn-pathfail-s5-qci-other

• totepsbearrel-dedrsn-pathfail-s11
  • totepsbearrel-dedrsn-pathfail-s11-qci1
  • totepsbearrel-dedrsn-pathfail-s11-qci2
  • totepsbearrel-dedrsn-pathfail-s11-qci3
  • totepsbearrel-dedrsn-pathfail-s11-qci4
- totepsbearrel-dedrsn-pathfail-s11-qci5
- totepsbearrel-dedrsn-pathfail-s11-qci6
- totepsbearrel-dedrsn-pathfail-s11-qci7
- totepsbearrel-dedrsn-pathfail-s11-qci8
- totepsbearrel-dedrsn-pathfail-s11-qci9
- totepsbearrel-dedrsn-pathfail-s11-qci-other

- totepsbearrel-dedrsn-pathfail-s12
  - totepsbearrel-dedrsn-pathfail-s12-qci1
  - totepsbearrel-dedrsn-pathfail-s12-qci2
  - totepsbearrel-dedrsn-pathfail-s12-qci3
  - totepsbearrel-dedrsn-pathfail-s12-qci4
  - totepsbearrel-dedrsn-pathfail-s12-qci5
  - totepsbearrel-dedrsn-pathfail-s12-qci6
  - totepsbearrel-dedrsn-pathfail-s12-qci7
  - totepsbearrel-dedrsn-pathfail-s12-qci8
  - totepsbearrel-dedrsn-pathfail-s12-qci9
  - totepsbearrel-dedrsn-pathfail-s12-qci-other

- totepsbearrel-dedrsn-pathfail-s4-u
  - totepsbearrel-dedrsn-pathfail-s4-u-qci1
  - totepsbearrel-dedrsn-pathfail-s4-u-qci2
  - totepsbearrel-dedrsn-pathfail-s4-u-qci3
  - totepsbearrel-dedrsn-pathfail-s4-u-qci4
  - totepsbearrel-dedrsn-pathfail-s4-u-qci5
  - totepsbearrel-dedrsn-pathfail-s4-u-qci6
  - totepsbearrel-dedrsn-pathfail-s4-u-qci7
  - totepsbearrel-dedrsn-pathfail-s4-u-qci8
  - totepsbearrel-dedrsn-pathfail-s4-u-qci9
  - totepsbearrel-dedrsn-pathfail-s4-u-qci-other

- totepsbearrel-dedrsn-other
  - totepsbearrel-dedrsn-other-qci1
  - totepsbearrel-dedrsn-other-qci2
  - totepsbearrel-dedrsn-other-qci3
  - totepsbearrel-dedrsn-other-qci4
  - totepsbearrel-dedrsn-other-qci5
show sgw-service statistics all verbose

The following counters have been added to provide more granularity in dropped call counters by reason and Qos Class Identifier (QCI)

- PGW Ini:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- S1 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- S5 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
- QCI 4:
- QCI 5:
- QCI 6:
- QCI 7:
- QCI 8:
- QCI 9:
- Non-Std QCI:

- S4 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- S12 Error Ind:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- Local:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
- QCI 5:
- QCI 6:
- QCI 7:
- QCI 8:
- QCI 9:
- Non-Std QCI:

- PDN Down:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- Path Failure S1-U:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

- Path Failure S5-U
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
- QCI 6:
- QCI 7:
- QCI 8:
- QCI 9:
- Non-Std QCI:
  - Path Failure S5:
    - QCI 1:
    - QCI 2:
    - QCI 3:
    - QCI 4:
    - QCI 5:
    - QCI 6:
    - QCI 7:
    - QCI 8:
    - QCI 9:
    - Non-Std QCI:
  - Path Failure S11:
    - QCI 1:
    - QCI 2:
    - QCI 3:
    - QCI 4:
    - QCI 5:
    - QCI 6:
    - QCI 7:
    - QCI 8:
    - QCI 9:
    - Non-Std QCI:
  - Path Failure S4-U:
    - QCI 1:
    - QCI 2:
    - QCI 3:
    - QCI 4:
    - QCI 5:
    - QCI 6:
- QCI 7:
- QCI 8:
- QCI 9:
- Non-Std QCI:
- Path Failure S12:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:
- Other:
  - QCI 1:
  - QCI 2:
  - QCI 3:
  - QCI 4:
  - QCI 5:
  - QCI 6:
  - QCI 7:
  - QCI 8:
  - QCI 9:
  - Non-Std QCI:

**CSCui37794, CSCui47671 - ULI inclusion cond during Service Request procedure when ISR is active**

**Feature Changes**

**Support for Including ULI Inclusion Condition During Service Request when ISR is active.**

If Idle Mode Signaling Reduction (ISR) is active and the UE initiates a Service Request procedure then the MME and S4-SGSN are not in a position to decide whether the ULI has changed since it was last known. For example, when the
UE changes RAT type and performs a Service Request procedure in another RAT type. In this scenario, the MME/S4-SGSN always includes ULI in the MBR (if location reporting is enabled in P-GW). Since the ULI is received by the S-GW it will send an MBR to the P-GW even if the location info or RAT type has not changed since it was last known.

To remedy this situation, the software has been enhanced so that a new flag is introduced in the MBR. CLII is set to 1 by the MME/S4-SGSN if:

1. ISR is active and
2. Location info has changed.

The S-GW sends the ULI info in MBR to the P-GW if ISR is active and

1. RAT type is changed or
2. CLII flag is set.

**CSCui37806 - Suspend Notification/Acknowledge message in SGSN pool**

**Feature Changes**

**Support for Suspend Notification/Acknowledge Message in SGSN Pool Scenario**

The S-GW has been enhanced to add the IP address, Port number and Hop counter in the Suspend Notification message. This includes Suspend notification and acknowledge messages in the SGSN pool scenario to the UDP port number and IP address definition for GTPv2 messages. This enhancement ensures that the SGSN will not have to repeat sending the Suspend Notification message in a SGSN Pool scenario.

**CSCui37810, CSCui47711 - PGW restoration upon PGW failure w/o restart**

**Feature Changes**

**Support for New Cause Value in the S-GW**

The PGW Restart Notification may also be used to signal that the peer PGW has failed and not restarted. In this case, the P-GW Restart Notification now contains a new cause value, *PGW not responding*. While sending the PRN, the S-GW includes the cause with this new cause value depending on the echo response.

**CSCui47671 - ULI inclusion cond during Service Request procedure when ISR is active**

**Feature Changes**

**Support for Including ULI Inclusion Condition During Service Request when ISR is active.**

If ISR is active and the UE initiates a Service Request procedure then the MME/S4-SGSN are not in a position to decide whether the ULI has changed since it was last known. For example, when the UE changes RAT type and performs a Service Request procedure in another RAT type. In this scenario, the MME/S4-SGSN always includes ULI in the MBR (if location reporting is enabled in P-GW). Since the ULI is received by the S-GW it will send an MBR to the P-GW even if the location info or RAT type has not changed since it was last known.
To remedy this situation, the software has been enhanced so that a new flag is introduced in the MBR. CLII is set to 1 by MME/S4-sGSN if:

1. ISR is active and
2. Location info has changed.

The S-GW sends the ULI info in MBR to the P-GW if ISR is active and

1. RAT type is changed or
2. CLII flag is set.

**CSCui37800, CSCui47691 - Adding a Cause Value in Delete Session Request message**

**Feature Changes**

**Enhanced Cause Value Support in the S-GW**

*Network failure* is used by the SGSN or MME in the Delete Session Request to indicate that the message is sent due to a network problem. *QoS parameter mismatch* is used by the SGSN or MME in the Delete Session Request to indicate that the PDN connection can not be established due to a QoS parameter mismatch.

To ensure compliance and consistency, the SGW has been enhanced to also support the Cause Values *Network failure* and *QoS parameter mismatch*.

**CSCui70609 - [15.0]multi-access keyword under apn-profile to be concealed/removed**

**Feature Changes**

**multi-access Keyword Removed from APN Profile Configuration Mode**

The *multi-access* keyword is no longer required by the S-GW. As a result, it has been removed from *APN Profile Configuration Mode*.

**Previous Behavior:** *multi-access* keyword was available for use on the S-GW in *APN Profile Configuration Mode*.

**New Behavior:** *multi-access* keyword has been removed from *APN Profile Configuration Mode* on the S-GW.

**CSCui92670 - VOLTE: GTPU service to reserve bind addresses for VOLTE data bearers**

**Feature Changes**

**Preferential Treatment for VoLTE Calls on the S-GW**

The S-GW software has been enhanced to give preferential treatment for VoLTE calls, based on bearer traffic type.
Command Changes

**bind bearer-type**

The new `bearer-type` keyword in the `bind` command allows operators to give preferential treatment to VoLTE calls based on bearer traffic type.

```plaintext
configure
  context context_name
  gtpu-service service_name
  bind { ipv4-address ipv4_address [ bearer-type { non-ims-media | ims-media | all } ] }
end
```

Notes:
- `bearer-type` optionally configures the type of bearer to be associated with the bind address.
- `non-ims-media` configures the bind address for non-IMS calls only.
- `ims-media` configures the bind address for IMS media traffic only.
- `all` configures the bind address for all types of traffic. This is the default setting.

Performance Indicator Changes

**show gtpu-service all**

The output of this command has been enhanced to if bearer-type has been associated with the bind addresses.

- Address List:
  - `ipv4 or ipv6 address ims-media`
  - `ipv4 or ipv6 address non-ims-media`
  - `ipv4 or ipv6 address all`

CSCui95971, CSCuj13956 - Rel10 Compliance for SGW-CDRs

Feature Changes

**Release 10 Charging Compliance for S-GW CDRs**

To more fully comply with 3GPP Release 10, the following TLVs have been added to S-GW Call Detail Records (CDRs):
- IMSI Unauthenticated Flag
- Dynamic Address Flag extension
- S-GW Address IPv6
- Serving Node IPv6 Address
- P-GW Address IPv6

The new attributes are added to S-GW custom dictionaries CUSTOM24 and CUSTOM35.
Chapter 25
SNMP MIB Changes in Release 16

This chapter identifies SNMP MIB objects and alarms added to, modified for, or deprecated from StarOS 16 software releases.
SNMP MIB Object Changes for 16.5

This section provides information on SNMP MIB object changes in release 16.5.

**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 16.5.

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 16.5.

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 16.5.

The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes for 16.5

This section provides information on SNMP MIB alarm changes in release 16.5.

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 16.5.
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 16.5.
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 16.5.
The following alarms have been deprecated in this release:
None in this release.
SNMP MIB Conformance Changes for 16.5

This section provides information on SNMP MIB conformance changes in release 16.5.

---

**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 16.5.

The following list 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 16.5.

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 16.5.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 16.4

This section provides information on SNMP MIB object changes in release 16.4.

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 16.4.
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 16.4.
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 16.4.
The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 16.4

This section provides information on SNMP MIB alarm changes in release 16.4.

**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 16.4.
The following alarms are new in this release:

- starBGPPeerSessionIPv6Up
- starBGPPeerSessionIPv6Down

**Modified SNMP MIB Alarms**

This section identifies SNMP MIB alarms modified in release 16.4.
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 16.4.
The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 16.4

This section provides information on SNMP MIB conformance changes in release 16.4.

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 16.4.
The following list of conformances are new in this release:

- starBGPPeerSessionIPv6Up
- starBGPPeerSessionIPv6Down

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 16.4.
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 16.4.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 16.3

This section provides information on SNMP MIB object changes in release 16.3.

**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 16.3.

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 16.3.

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 16.3.

The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 16.3

This section provides information on SNMP MIB alarm changes in release 16.3.

**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 16.3.

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 16.3.

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 16.3.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 16.3

This section provides information on SNMP MIB conformance changes in release 16.3.

**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 16.3.

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 16.3.

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 16.3.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 16.2

This section provides information on SNMP MIB object changes in release 16.2.

**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 16.2.

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 16.2.

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 16.2.

The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes for 16.2

This section provides information on SNMP MIB alarm changes in release 16.2.

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 16.2.

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 16.2.

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 16.2.

The following alarms have been deprecated in this release:

None in this release.
SNMP MIB Conformance Changes for 16.2

This section provides information on SNMP MIB conformance changes in release 16.2.

### 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 16.2.

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 16.2.

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 16.2.

The following units of conformance have been deprecated in this release:

None in this release.
SNMP MIB Object Changes for 16.1

This section provides information on SNMP MIB object changes in release 16.1.

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 16.1.

The following objects are new in this release:

- starThreshPeriodInt
- starThreshDeviceNum
- starSLSServiceVpnName
- starSLSServiceServName
- starESMLCId
- starESMLCIpAddr1
- starESMLCIpAddr2
- starESMLCPortNum
- starSBCServiceVpnName
- starSBCServiceServName
- starPeerId
- starPeerIpAddr
- starPeerPortNum
- starBfdSrcAddressType
- starBfdSrcAddress
- starBfdDstAddressType
- starBfdDstAddress
- starBfdLocalDisc
- starBfdRemDisc
- starBfdSessDiagCode
- starSRPSwitchReason
- starHENBGWServiceTLRI
- starCBSServiceVpnName
- starIuBcSelfPortNum
Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 16.1.
The following objects have been modified in this release:

- starIuBcSelfIpAddr
- starIuBcPeerPortNum
- starIuBcPeerIpAddr
- starIuBcTcpConnCauseStr

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 16.1.
The following objects have been deprecated in this release:

None in this release.
SNMP MIB Alarm Changes for 16.1

This section provides information on SNMP MIB alarm changes in release 16.1.

**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 16.1.

The following alarms are new in this release:

- `starThreshFabricEGQDiscards`
- `starThreshClearFabricEGQDiscards`
- `starSLSServiceStart`
- `starSLSServiceStop`
- `starESMLCAssocDown`
- `starESMLCAssocUp`
- `starESMLCAllAssocDown`
- `starESMLCAllAssocDownClear`
- `starSBCServiceStart`
- `starSBCServiceStop`
- `starCBCAssocDown`
- `starCBCAssocUp`
- `starHENBGWMMEOverloadStart`
- `starHENBGWMMEOverloadStop`
- `starIuBcTcpConnDown`
- `starIuBcTcpConnUp`

### Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 16.1.

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 16.1.
The following alarms have been deprecated in this release:
None in this release.
SNMP MIB Conformance Changes for 16.1

This section provides information on SNMP MIB conformance changes in release 16.1.

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 16.1.

The following units of conformance are new in this release:

- starCBSServiceVpnName
- starIuBcSelfPortNum
- starIuBcSelfIpAddr
- starIuBcPeerPortNum
- starIuBcPeerIpAddr
- starIuBcTcpConnCauseStr
- starSLSServiceStart
- starSLSServiceStop
- starESMLCAssocDown
- starESMLCAssocUp
- starESMLCAllAssocDown
- starESMLCAllAssocDownClear
- starSBCServiceStart
- starSBCServiceStop
- starCBCAssocDown
- starCBCAssocUp
- starThreshFabricEGQDiscards
- starThreshClearFabricEGQDiscards
- starHENBGWMMEOverloadStart
- starHENBGWMMEOverloadStop
- starIuBcTcpConnDown
- starIuBcTcpConnUp
Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 16.1.
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 16.1.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 16.0

This section provides information on SNMP MIB object changes in release 16.0.

**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 16.0.

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 16.0.

The following objects have been modified in this release:

- `starVIMServiceInstanceId`
- `starScapNwId`
- `starIPMSServerAddr`
- `starCertSerialNumber`
- `starFileName`
- `starFTPservIpAddr`
- `starSDHSlot`
- `starSDHPort`
- `starSDHPathSlot`
- `starSDHPathPort`
- `starSDHPathNum`
- `starE1TribSlot`
- `starE1TribPort`
- `starE1TribPath`
- `starE1TribTug2`
- `starE1TribTu12`
- `starFractE1TribSlot`
- `starFractE1TribPort`
- starFractELTribPath
- starFractELTribTug2
- starFractELTribTu12
- starFractELTribBundNum
- starGPRSNsei
- starStorageSlot
- starStorageName
- starMMES1AssocENBID
- starMMES1AssocENBID
- starCscfSessCongestionResourceType
- starSmgrId
- starPeerAddressIpv6
- starLAGPartner
- starSGSServiceVpnName
- starSGSServiceServName
- starVLRName
- starVLRIpAddr1
- starVLRIpAddr2
- starVLRPortNum
- starCongestionType
- starCongestionActionProfileName
- starHENBGWServiceVpnName
- starHENBGWServiceServName
- starHENBGWServiceLogicalENBId
- starHENBGWServiceMMEservName
- starHENBGWServicePeerAddr
- starHENBGWServicePeerPort
- starChassisCrashList
- starL2TPLocalTunnelID
- starL2TPPeerTunnelID
- starNwReachName
- starNwReachSrvrAddr
- startChassisType
- starSlotNum
- starLogName
- starPowerNumber
- starCPUSlot
- starCPUNumber
- starNPUMgrNumber
- starTaskInstance
- starCongestionPolicy
- starCongestionResourceType
- starPTACConfig
- starPTACActive
- starInterfaceName
- starPCFAddress
- starPeerAddress
- starL3Address
- starUDPPortNum
- starBGPPeerIpAddress
- starContFiltCFFilename
- starContFiltCFErrorCode
- starFetchedFromAAAMgr
- starPriorToAudit
- starPassedAudits
- starCallsRecovered
- starAllCallLines
- starElapsedMs
- starCDRFilename
- starBLFilename
- starBLErrorCode
- starContFiltCFUpgradeFilename
- starContFiltCFUpgradeErrorCode
- starBLUpgradeFilename
- starBLUpgradeErrorCode
- starDynPkgFilename
- starDynCFErrorCode
- starDynPkgUpgradeFilename
• starDynCFUpgradeErrorCode

 Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 16.0.
The following objects have been deprecated in this release:
None in this release.
SNMP MIB Alarm Changes for 16.0

This section provides information on SNMP MIB alarm changes in release 16.0.

**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 16.0.

The following alarms are new in this release:

- starThreshMMESessions
- starThreshClearMMESessions
- starThreshMMEAuthFail
- starThreshClearMMEAuthFail
- starThreshMMEAttachFail
- starThreshClearMMEAttachFail
- starThreshPerServiceSAMOGSessions
- starThreshClearPerServiceSAMOGSessions
- starHENBGWMMESCTPAssocDestAddrDown
- starHENBGWMMESCTPAssocDestAddrUp
- starMRMEServiceStart
- starMRMEServiceStop

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 16.0.

The following alarms have been modified in this release:

- starSDHFractE1LMIUp
- starECSTotalDNSLearntIPv6Threshold
- starECSTotalDNSLearntIPv6Threshold
- starRMCPUOver
- starRMCPUOverClear
- starMMENewConnectionsDisallowed
- starMMENewConnectionsAllowed
Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 16.0.
The following alarms have been deprecated in this release:
None in this release.
SNMP MIB Conformance Changes for 16.0

This section provides information on SNMP MIB conformance changes in release 16.0.

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 16.0.

The following units of conformance are new in this release:

- starHENBGWServiceVpnName
- starHENBGWServiceServName
- starHENBGWServiceLogicalENBId
- starHENBGWServiceMMEServiceName
- starHENBGWServicePeerAddr
- starHENBGWServicePeerPort
- starHENBGWMMESCTPAssocDestAddrDown
- starHENBGWMMESCTPAssocDestAddrUp
- starMRMEServiceStart
- starMRMEServiceStop
- starThreshPerServiceSAMOGSessions
- starThreshClearPerServiceSAMOGSessions

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 16.0.

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 16.0.

The following units of conformance have been deprecated in this release:

None in this release.
Chapter 26
System Changes in Release 16

This chapter identifies ASR 5x00 and virtual platform system-level features and functionality added to, modified for, or deprecated from StarOS 16 software releases.
System and Platform Enhancements for 16.2

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.

CSCuh81020 - [Ares] ‘Boost’ EM (Exact Match) Flow enhancements: NPUMGR

**Applicable Products:** All (ASR 5500 only)

**Feature Changes**

**ASR 5500 NPU Enhancements**

NPU code changes improve exact match flow lookup behaviour in the ASR 5500.

CSCuo50178 - Need IPv6 support in crashd to send a full core file to crashlog server

**Applicable Products:** All

**Feature Changes**

**Send Full Core File to IPv6 Crashlog Server**

**Previous Behavior:** Crash log files could only be sent to an IPv4 server.

**New Behavior:** Crash log files can now be sent to an IPv6 server

**Customer Impact:** Interoperability

CSCuo50183 - Need IPv6 support in syslog/evlogd for logging events in syslogd server

**Applicable Products:** All
Feature Changes

IPv6 Support for syslog Servers

**Previous Behavior:** A syslog server at an IPv6 address could not be reached.

**New Behavior:** A syslog server at an IPv6 address can now be reached.

**CSCuo84086 - IPv6 support for NTP**

**Applicable Products:** All

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.

**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]

**CSCup68502 - Software version data should be consistent across prime network**

**Applicable Products:** All
Feature Changes

SNMP - New StarOS Version Numbering

Previous Behavior: SNMP GET requests inappropriately returned StarOS version information in the pre-16.1 format: <major>.<minor> (<build-number> in the entity table and other relevant MIB values.

New Behavior: SNMP GET requests now return version information in the new, 16.1+ format. For detailed information on the new format, see the System Administration Guide.

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

CSCuq28805 - ICSR failover resulted in loss of PCRF binding

Applicable Products: All products that support ICSR

Feature Changes

Handling of Interim Resource Messages During ICSR Upgrade

A new CLI command supports the proper handling of Interim Resource messages when upgrading to StarOS 16.1 or higher. If you do not enable this feature, an ICSR system may experience PCRF binding problems (5002 error code message) when performing an ICSR upgrade from previous StarOS versions.

Command Changes

handle-interim-resource-msg version-16.1

This new command enables proper SRP Interim Message handling in an ICSR configuration being upgraded to 16.1+. By default this feature is disabled to preserve compatibility with release versions prior to 16.1.

configure

   context  context_name

   service-redundancy-protocol variable
handle-interim-resource-msg version-16.1

end

Notes:

- `context_name` is the context designated for SRP.
System and Platform Enhancements for 16.1

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.

---

**CSCug23975 - VoLTE: Prioritized handling of VoLTE/Emergency calls**

**Applicable Products:** LTE

**Feature Changes**

**Prioritized Handling of for VoLTE/Emergency Calls**

If prioritized APN/ARP handling is enabled and if the APN/ARP received in CSReq matches any of the configured prioritized APN/ARP values, any valid CSReq will not be rejected because of congestion control.

In summary, prioritized calls will not be rejected due to congestion.

---

**CSCuh25721 - LAG CLI Enhancements**

**Applicable Products:** All (ASR 5x00 only)

**Feature Changes**

**LAG Statistics**

A `show` command and LAG bulkstat schema have been added in this release to provide Link Aggregation Group (LAG) statistics.

**Performance Indicator Changes**

**link-aggr Schema**

The link-aggr schema provides the following LAG statistics:

- group-index
- group-state
- group-no-ports
- group-no-masters
- group-active-master
- group-sys-mac
- group-sys-prio
- group-rx-bytes
- group-tx-bytes
- group-rx-unicast-frames
- group-tx-unicast-frames
- group-rx-multicast-frames
- group-tx-multicast-frames
- group-rx-broadcast-frames
- group-tx-broadcast-frames
- group-curr-util-rx
- group-curr-util-tx
- group-5min-util-rx
- group-5min-util-tx
- group-15min-util-rx
- group-15min-util-tx
- group-lacp-slot<range>
- group-lacp-port<range>
- group-lacp-port<range>-rx-count
- group-lacp-port<range>-tx-count

Notes:
- <range> = integer from 1 through 40.

**show link-aggregation info**

This command displays the following LAG statistics:
- LAG group id
- group state
- number of ports
- number of masters
- active master
- sysmac
- sysprio
show link-aggregation lACP info

This command displays the following Link Aggregation Control Protocol (LACP) statistics:

- LAG group id
- Rx Counters
- Tx Counters

show link-aggregation statistics

This command displays the following LAG statistics:

- LAG group id
- Line Card
- Rx Counter
  - Bytes
  - Unicast frames
  - Multicast frames
  - Broadcast frames
  - Data
- Tx Counter
  - Bytes
  - Unicast frames
  - Multicast frames
  - Broadcast frames
  - Data

show link-aggregation table

This command displays the following LAG statistics:

- Group
- Type
- Average Port Utilization (in mbps)
  - Current Rx/Tx
  - 5min Rx/Tx
  - 15min Rx/Tx

CSCul69462 - Need a way to configure no-password user account

Applicable Products: All
Feature Changes

Nopassword Option for Administrators

A new keyword allows the creation of administrative accounts without an associated password. Enable this option when using ssh public keys (authorized key command in SSH Configuration mode) as a sole means of authentication. Enabling this option prevents someone from using an administrative password to gain access to the user account.

Command Changes

administrator

A new nopassword keyword allows you to create an administrator without an associated password.

```plaintext
configure
  context context_name
  administrator username nopassword
end
```

config-administrator

A new nopassword keyword allows you to create a config-administrator without an associated password.

```plaintext
configure
  context context_name
  config-administrator username nopassword
end
```

inspector

A new nopassword keyword allows you to create an inspector without an associated password.

```plaintext
configure
  context context_name
  inspector username nopassword
end
```

operator

A new nopassword keyword allows you to create an operator without an associated password.

```plaintext
configure
  context context_name
```
operator username nopassword
end

CSCun71100 - show version changes needed for new version numbering scheme for 16.0

Applicable Products: All

Feature Changes

New StarOS Version Numbering System

The output of the `show version` command displays detailed information about the version of StarOS currently running on the ASR 5x00 or QvPC platform.

Prior to release 16.1, the Image Version version field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards the output of the `show version` command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, `show version` will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for 16.1 and onwards releases now include, at minimum, a major, maintenance, and emergency release number, for example “16.1.2”. The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Toolkit to research software releases.

The following diagram shows the differences between the old numbering format and the new numbering format.

![Comparison of Old and New StarOS Version Numbering Formats](image)

In the old format, the first two fields of the Build Version Number represented the Major release and subsequent releases (MRs/ERs) would differ only by build number. Documentation references to a release included descriptive text...
to indicate whether the release was an MR or ER. For instance, “16.0.65781 MR1” indicates via its descriptor that it is the first maintenance release for 16.0.

In the new format, the maintenance release number changes with subsequent Maintenance Releases (MRs). For example, “16.2” would represent the second maintenance release (MR2) of release 16.

A third digit in the Build Version Number now indicates an Emergency Release for a previous FCS or MR build. For example “16.1.3” indicates the third ER of the first MR of the 16.0 major release.

The Build Version Number may now also include an optional variant indicator just before the ER number to identify the release as a variant of an MR or ER Release. A variant release is one that is given to a particular customer or group of customers, as opposed to a mainstream release which is suitable for all customers.

**Important:** For detailed information on other changes associated with this numbering scheme, refer to the StarOS Version Numbering appendix in the System Administration Guide and the show version chapter of the Statistics and Counters Reference.

### Performance Indicator Changes

**show version**

Changes relative to the adoption of a new StarOS numbering system now appear in the output of the show version command for deployment builds that appear on customer systems.

A deployment build has been qualified as suitable for deployment in customer networks. The build number only appears in the Image Build Number line.

A sample output of the 16.1 `show version` command for a deployment build appears below.

```
[local]asr5000# show version
Active Software:
  Image Version: 16.1.0
  Image Build Number: 56012
  Image Description: Deployment_Build
  Image Date: Mon Jun 30 17:05:09 EDT 2014
  Boot Image: Unknown
```

**CSCuo70354 - Unable to set more than one BGP extended community using route-map**

*(Applicable Products: All)*

### Feature Changes

**Multiple BGP Community and Extcommunity Destinations**
Changes have been made to configuration commands to allow the setting of multiple destinations within a BGP community and extcommunity route map.

**Command Changes**

**ip community-list**

Modification of this command now supports listing of multiple destinations and AS:NN community numbers within this list.

```
context context_name

ip community-list { named named_list | standard identifier } { deny | permit } { internet | local-AS | no-advertise | no-export | value AS-community_number AS-community_number AS-community_number AS-community_number ... } }
```

Notes:

- You can enter multiple destinations and AS community numbers separated by spaces.

**ip extcommunity-list rt**

Modification of this command now supports listing of multiple AS:NN community numbers within this list.

```
context context_name

ip extcommunity-list { named named_list | standard identifier } { deny | permit } rt rt_number rt_number rt_number ...
```

Notes:

- You can enter multiple route numbers separated by spaces.

**set community**

Modification of this command now supports listing of multiple destinations and AS:NN community numbers within this list.

```
context context_name

route-map map_name { deny | permit } sequence_number
```
set community additive { internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ...

{ internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ...

{ internet | local-AS | no-advertise | no-export | none | value AS-community_number AS-community_number AS-community_number ...

Notes:
- You can enter multiple destinations and AS community numbers separated by spaces.

set extcommunity rt

Modification of this command now supports listing of multiple destinations and AS:NN community numbers within this list.

configure

context context_name

route-map map_name { deny | permit } sequence_number

set extcommunity rt value AS-community_number AS-community_number AS-community_number ...

Notes:
- You can enter multiple AS community numbers separated by spaces.

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.
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 exceed, the syslog event message is generated once, until the condition clears. Only then will it be generated again.
- By default this feature is disabled.

**CSCuo91363 - Non-Redundant MIO Failure recovery action upon initialization failure**

**Applicable Products:** All (ASR 5500)

**Feature Changes**

**Initialization of MIOs on Switchover**

During switchover from MIO5 to MIO6 initialization failed when it took too long due to control plane issues, resulting in a forced restart of the processes. Control plane issues in the chassis remained after restart. StarOS also came up with an incorrect boot configuration file after restart.

**Previous Behavior:** Failed switchover attempt caused forced restart of processes.

**New Behavior:** A StarOS restart now reboots both MIOs with improved handling of local card restart.
System and Platform Enhancements for 16.0

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.

---

**CSCtr55441 - VoLTE related ICSR optimization**

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

**Feature Changes**

**ICSR Framework Changes to Support VoLTE**

A significant number of internal enhancements have been made in support of voice-grade redundancy for Voice over LTE (VoLTE) deployments. ICSR components have been optimized to ensure that failure recovery is accomplished within acceptable limits for VoLTE. The impact on the data path is high priority. For data path interruptions, recovery be limited to no more than 50 milliseconds for intra-chassis failures and 1 to 2 seconds for inter-chassis failures.

The table below cross-references the various CDETS IDs that have been addressed as part of this ICSR-VoLTE performance optimization.

**Table 3. ICSR-VoLTE Enhancements**

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICSR Framework Changes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSCtz64076</td>
<td>GR Write List enhancement</td>
<td>Use a single buffer capable of containing multiple encoded checkpoints for the GR write list. Process multiple checkpoints simultaneously.</td>
</tr>
<tr>
<td>CSCud76965</td>
<td>Better statistics for ICSR sessmgr framework</td>
<td>Improve handling of micro-checkpoint counters.</td>
</tr>
<tr>
<td>CSCue52826</td>
<td>[ICSR-VoLTE] Reduce the flushing time during ICSR switchover.</td>
<td>See CSCtz64076 and CSCug86838.</td>
</tr>
<tr>
<td>CSCue52853</td>
<td>[ICSR-VoLTE] - Changes to allow data traffic in pending_standby</td>
<td>Allow data traffic (no control traffic) during the ICSR Pending-Standby(PS) state.</td>
</tr>
<tr>
<td>CSCue54471</td>
<td>ICSR-Volte] Changes to process pkts during sessmgr ICSR audit recovery</td>
<td>Allow packet processing while accepting new calls during audit procedure.</td>
</tr>
<tr>
<td>CDETS ID</td>
<td>Description</td>
<td>Impact</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCug42104</td>
<td>[ICSR-VoLTE] Include timestamp in the GR FSM events and flushing</td>
<td>Capture micro-checkpoint flushing during switchover, as well as internal audit stats with vpn and npu.</td>
</tr>
<tr>
<td>CSCug94606</td>
<td>ICSR-VoLTE] Mechanism to detect flush complete in pend_stdby</td>
<td>Add ICSR negotiation of VoLTE status between active and standby chassis.</td>
</tr>
<tr>
<td>CSCui16249</td>
<td>[ICSR-VoLTE] FSM changes to send stats Micro-Chk-Pts after S/O</td>
<td>In both planned and unplanned switchover scenarios, the stats micro-checkpoint now reaches the other chassis after the switchover is done.</td>
</tr>
<tr>
<td>CSCui16259</td>
<td>[ICSR-VoLTE] Internal audit is triggered in a time bounded manner</td>
<td>An internal audit is now triggered in a time-bounded, predictable manner.</td>
</tr>
<tr>
<td>CSCui24380</td>
<td>(ICSR) Framework support is required for instance level check-pointing</td>
<td>Add API to send session recovery and ICSR checkpoint messages, Enable periodic trigger of instance level checkpoints for session recovery and ICSR. Auditing performed as part of External Audit procedure; trigger re-transmissions if required.</td>
</tr>
</tbody>
</table>

**ICSR Component Changes**

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCug68853</td>
<td>[ICSR-Volte] CLP level distinction for VoLTE /nonVoLTE/Emrgncy calls.</td>
<td>See CSCuh97959.</td>
</tr>
<tr>
<td>CSCub86414</td>
<td>ECSv2 - Redesign Session recovery and ICSR</td>
<td>Addressed by all changes made for CSCug68853.</td>
</tr>
<tr>
<td>CSCuh97959</td>
<td>[ICSR-Volte] CLP level distinction for VoLTE /nonVoLTE/Emrgncy calls</td>
<td>VoLTE, non-VoLTE and Emergency calls are differentiated at the CLP level, so that VoLTE calls are treated differently from non-VoLTE calls at the time of ICSR switchover.</td>
</tr>
<tr>
<td>CSCuh97966</td>
<td>[ICSR-Volte] CLP level distinction for VoLTE /nonVoLTE/Emrgncy calls.</td>
<td>See CSCuh97966 ICSRVolte CLP level distinction for VoLTE nonVoLTEEmergency calls.</td>
</tr>
<tr>
<td>CSCug86838</td>
<td>[ICSR-Volte] Removing the usage of pacing queue for critical MCs</td>
<td>Minimize use of micro-checkpoint pacing queue. See related CDETS IDs below.</td>
</tr>
<tr>
<td>CSCuh97978</td>
<td>[ICSR-Volte] Removing the usage of pacing queue for critical MCs Micro-checkpoints are now sent out immediately.</td>
<td>Micro-checkpoints are now sent out immediately.</td>
</tr>
<tr>
<td>CSCuj70355</td>
<td>Separation of micro checkpoint for ECS call object and sub session info</td>
<td>Eliminate duplicate call object information in the micro checkpoint for an ECS sub session to reduce ICSR messaging.</td>
</tr>
<tr>
<td>CSCuj82209</td>
<td>[ICSR-Volte] dynamic rule checkingpointing redesign</td>
<td>Streamline recovery and ICSR framework for dynamic rule checkpointing.</td>
</tr>
<tr>
<td>CSCul07323</td>
<td>ECS ICSR statistics</td>
<td>Output of show active-charging subsystem all debug-only now displays recovery -related ECS statistics of acsmgr and aaamgr</td>
</tr>
<tr>
<td>CSCul12069</td>
<td>Inclusion of ECS internal audit information in Macro checkpoint</td>
<td>The current state of ECS (number of sub sessions, number of dynamic rules, etc.) on the active chassis now sent as internal audit information as a part of macro checkpoint to the standby chassis.</td>
</tr>
<tr>
<td>CSCul21305</td>
<td>QG and dynamic CA sessmgr recovery and ICSR support</td>
<td>Provide separate QG and CA checkpoint s for sessmgr recovery. Modify code to adhere to new framework.</td>
</tr>
</tbody>
</table>
CSCu65106 | Adding new ECS micro checkpoint command NACK for coherency key mismatch | ECS now uses the coherency key for its micro checkpoints to validate correct reception of its micro checkpoints on the standby chassis.

CSCug86780 | [ICSR-Volte] ECS related enhancement in switchover time for VoLTE ICSR | See CSCug86838.

CSCug86889 | [ICSR-Volte] Changes to allow control and data traffic in more states | During pending standby and internal audit ICSR states, data will be allowed for VoLTE bearers.

CSCuh64341 | [ICSR-Volte] Blocking new VoLTE calls in active chassis during audit | See CSCug86889.

CSCui06202 | SR: Control Plane changes to improve overall system Performance | See CSCuh85489.

CSCui19908 | [ICSR-Volte] Changes to allow control and data traffic in more states | See CSCug86889.

CSCui19916 | [ICSR-Volte] Changes to allow control and data traffic in more states | See CSCug86889.

CSCui19941 | [ICSR-Volte] Blocking new VoLTE calls in active chassis during audit | Traffic is allowed to in Pending-Standby(PS) and Active-Audit(AA) state to reduce outages for VoLTE-calls. However, packets will be dropped for non-VoLTE calls while in these states. Control messages are suppressed in Pending-Standby(PS) and Active-Audit(AA) states for all calls types.

CSCui19945 | [ICSR-Volte] Blocking new VoLTE calls in active chassis during audit | See CSCug86889.

CSCui19949 | [ICSR-Volte] Blocking new VoLTE calls in active chassis during audit | See CSCug86889.

CSCug23975 - VoLTE: Prioritized handling of VoLTE/Emergency calls

Applicable Products: LTE

Feature Changes

Prioritized Handling of for VoLTE/Emergency Calls

If prioritized APN/ARP handling is enabled and if the APN/ARP received in CSReq matches any of the configured prioritized APN/ARP values, any valid CSReq will not be rejected because of congestion control.

In summary, prioritized calls will not be rejected due to congestion.
CSCuh25721 - LAG CLI Enhancements

**Applicable Products:** All (ASR 5x00 only)

**Feature Changes**

**LAG Statistics**

A `show` command and LAG bulkstat schema have been added in this release to provide Link Aggregation Group (LAG) statistics.

**Performance Indicator Changes**

**link-aggr Schema**

The link-aggr schema provides the following LAG statistics:

- group-index
- group-state
- group-no-ports
- group-no-masters
- group-active-master
- group-sys-mac
- group-sys-prio
- group-rx-bytes
- group-tx-bytes
- group-rx-unicast-frames
- group-tx-unicast-frames
- group-rx-multicast-frames
- group-tx-multicast-frames
- group-rx-broadcast-frames
- group-tx-broadcast-frames
- group-curr-util-rx
- group-curr-util-tx
- group-5min-util-rx
- group-5min-util-tx
- group-15min-util-rx
- group-15min-util-tx
- group-lacp-slot<range>
- roup-lacp-port<range>
- group-lacp-port<range>-rx-count
- group-lacp-port<range>-tx-count

Notes:
- <range> = integer from 1 through 40.

**show link-aggregation info**

This command displays the following LAG statistics:
- LAG group id
- group state
- number of ports
- number of masters
- active master
- sysmac
- sysprio

**show link-aggregation lacp info**

This command displays the following Link Aggregation Control Protocol (LACP) statistics:
- LAG group id
- Rx Counters
- Tx Counters

**show link-aggregation statistics**

This command displays the following LAG statistics:
- LAG group id
- Line Card
- Rx Counter
  - Bytes
  - Unicast frames
  - Multicast frames
  - Broadcast frames
  - Data
- Tx Counter
  - Bytes
  - Unicast frames
  - Multicast frames
- Broadcast frames
- Data

**show link-aggregation table**

This command displays the following LAG statistics:

- Group
- Type
- Average Port Utilization (in mbps)
  - Current Rx/Tx
  - 5min Rx/Tx
  - 15min Rx/Tx

**CSCul69462 - Need a way to configure no-password user account**

**Applicable Products:** All

**Feature Changes**

**Nopassword Option for Administrators**

A new keyword allows the creation of administrative accounts without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. Enabling this option prevents someone from using an administrative password to gain access to the user account.

**Command Changes**

**administrator**

A new **nopassword** keyword allows you to create an administrator without an associated password.

```plaintext
configure

context context_name

administrator username nopassword

end
```

**config-administrator**

A new **nopassword** keyword allows you to create an config-administrator without an associated password.

```plaintext
configure

context context_name
```
System Changes in Release 16

CSCtr67709 - Configurable Subscriber State Management Audit Process

Applicable Products: All products supporting ICSR

Feature Changes

Configurable Subscriber State Management Audit Process (ICSR)

A new audit command and keywords in Context Configuration mode allow an operator to specify the start time and periodicity for generating Interchassis Session Recovery (ICSR) Service Redundancy Protocol (SRP) audit statistics. This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

Command Changes

audit

Sets the start time and periodicity for ICSR Service Redundancy protocol (SRP) audits.

configure

   context context_name

   operator username nopassword

   end

   inspector

   A new nopassword keyword allows you to create an inspector without an associated password.

   configure

   context context_name

   inspector username nopassword

   end

   operator

   A new nopassword keyword allows you to create an operator without an associated password.

   configure

   context context_name

   operator username nopassword

   end
service-redundancy-protocol

audit { daily-start-time hour minute | periodicity minutes }

end

CSCtw93119 - show rct stats should show cause of event

Applicable Products: All products supporting the Session Recovery feature.

Performance Indicator Changes

show rct stats [verbose]

This command displays statistics associated with Recovery Control Task (RCT) events, including migrations, switchovers and shutdowns. RCT statistics are associated with card-to-card session recovery activities.

The Detailed (verbose) output includes the following information:

- Recovery action taken – Migration, Shutdown, Switchover
- Type of event – Planned or Unplanned
- From card to card – slot numbers
- Start time – YYYY-MMM-DD+hh:mm:ss.sss
- Duration – seconds
- Card failure device (such as CPUn)
- Card failure reason
- Card is in usable state or not failed
- Recovery action status – Success or failure reason
- If recovery action failed, failure time stamp
- If recovery action failed, failure task facility name
- If recovery action failed, failure instance number

For additional information refer to the System Administration Guide and Statistics and Counters Reference.

CSCua66992 - IKEv1/v2 ACL & Subscriber mode combo support

Applicable Products: All products supporting IPSec

Feature Changes

ACL-only Local Index Table

<description>
**Previous Behavior:** When ipsecmgrs start they are only validated as subscribers with a maximum of six ipsecmgrs per CPU. The ACL mode ipsecmgrs also share the same local index entry table as that of the subscribers along with a combined limit of six.

**New Behavior:** A separate local_index table has been created for the ACL mode alone leaving the existing local_index table for use by subscribers.

---

**CSCua86606 - eXGW full support on ASR5500**

**Applicable Products:** E-XGW

**Feature Changes**

**E-XGW Supported on ASR 5500**

The Enhanced-XGW (GGSN, HA and P-GW for MPN services) is now fully supported on the ASR 5500 platform.

---

**CSCuf60462 - Activity to Remove mallocs in IPsec code**

**Applicable Products:** All products using IPSec

**Feature Changes**

**Optimization of Memory Allocation for IPSec**

<description>

**Previous Behavior:** Ipsecmgrs relied heavily on system memory allocations (mallocs) of fixed size which led to a large number of object and pointers on the memory heap.

**New Behavior:** Ipsecmgrs now rely on memory cache/ pool blocks for similar types of objects whose instance count is known or can be previously determined. This technique optimizes memory allocation by reducing fragmentation, especially for temporary allocations during session establishment that are subsequently released.

---

**CSCug70348 - Allow comments in the configuration files**

**Applicable Products:** E-XGW products

**Command Changes**

**description**

This command allows an operator to add a textual description (up to 79 characters) of the function or purpose of an object within the following configuration groups:

- AAA Server Group Configuration Mode Commands
- ACL Configuration Mode Commands
System Changes in Release 16

System and Platform Enhancements for 16.0

- ACS Rulebase Configuration Mode Commands
- ACS Ruledef Configuration Mode Commands
- APN Configuration Mode Commands
- BGP Configuration Mode Commands
- Context Configuration Mode Commands
- Diameter Endpoint Configuration Mode Commands
- DNS Client Configuration Mode Commands
- HA Proxy DNS Configuration Mode Commands
- HA Service Configuration Mode Commands
- Subscriber Configuration Mode Commands
- Traffic Policy-Group Configuration Mode Commands
- Traffic Policy-Map Configuration Mode Commands

CSCug96855 - Multiple Traffic Selectors

**Applicable Products:** All gateway products supporting IKEv2 crypto templates

**Related CDETS ID:** CSCug87380

**Feature Changes**

**Narrowing of IKEv2 Traffic Selectors (TSr)**

During traffic selector negotiation, the gateway should be able to narrow down the UE’s request for a range of traffic selectors it accordance with RFC 5996.

**Previous Behavior:** No traffic selector negotiant occurs between the UE and gateway. The gateway responds back with wild-card traffic selectors in the TSr.

**New Behavior:** If the TSr configuration is completed, traffic-selector negation takes place for the TSr according to RFC 5996. If no TSr is configured, the gateway simply respects the received traffic selectors and responds back with received traffic selectors. In either case, a maximum of four traffics selectors per TSr can be sent out from the gateway.

**Customer Impact:** Interoperability

**Important:** This feature is applicable only for subscriber mode. TSi and TSr are carried only in IKE_AUTH requests and IKE_AUTH responses during initial tunnel establishment, and CREATE_CHILD_SA requests and CREATE_CHILD_SA responses when rekeying.

**Command Changes**

**tsr start-address**

The `tsr start-address` command has been modified to process both IPv4 and IPv6 addresses.
configure

context context_name

crypto template tnplt_name ikev2-dynamic

payload payload_name match childsa match any

tsr start-address ipv4v6_address end-address ipv4v6_address

end

Notes:

- The configuration is restricted to a maximum of four TSrs per payload and per childsa.
- Overlapping TSrs are not allowed either inside the same payload or across different payloads.
- When a TSr is configured via this command, only the configured TSr will be considered for narrowing-down. For example, if one IPv4 TSr is configured, and the gateway receives an IPv6 TSr, the gateway will reject the call with a TS_UNACCEPTABLE notification.
- The UE must send both INTERNAL_IP4_ADDRESS and INTERNAL_IP6_ADDRESS in the Configuration Payload, whenever it needs both IPv4 and IPv6 addresses in TSrs. Otherwise, the gateway will respond back with only one type depending upon the type of address received in the Configuration Payload. For example, if the gateway receives only INTERNAL_IP4_ADDRESS in the Configuration Payload but both IPv4 and IPv6 addresses are in the TSrs, the GW will narrow down only the IPv4 address, and ignore the IPv6 TSrs.
- IPv4 TSrs are not allowed inside IPv6 payloads.
- IPv6 TSrs are not allowed inside IPv4 payloads.

Performance Indicator Changes

show configuration

Negotiated TSrs appear in the payload display.

- tsr start-address ipv4v6_address end-address ipv4v6_address

show crypto ipsec security-associations

Negotiated TSr address ranges appear in the output of this command.

- Protocol 0 Port port_number Address Range tsr_range

CSCuh02039 - NEMO v4/v6 scalability

Applicable Products: E-XGW

Feature Changes

Aggregated Framed-Routes in a VRF
This feature enables inserting an aggregate-address in a VRF and its advertisement in the routing domain, if at least one constituent framed-route exists in that VRF. By default the constituent routes will also be present along with the aggregate address. If a summary-only option is configured, the constituent routes are removed from the VRF. Up to 32 aggregate addresses can be configured in a VRF.

**Command Changes**

```plaintext
ip aggregate address
aggregate-address is a new keyword that specifies an IPv4 address/mask for aggregating frame routes in the VRF.
```

```plaintext
configure
context context_name
    ip aggregate-address ipv4_address/mask [summary-only]
end
```

**CSCuh23425 - VPNv4 and VPNv6 MP-BGP feature normalization**

Applicable Products: All

**Feature Changes**

**Support for BGP Communities and Extended Communities**

Route filtering based on a BGP community or extended community (route target) is now supported via CLI Context Configuration and Route Map Configuration mode commands.

For addition information, refer to the Routing chapter of the System Administration Guide.

**Command Changes**

**Context Configuration Mode**

The following CLI commands have been added in support of BGP communities and extended communities.

```plaintext
config
    context <context_name>
        ip community-list { named named_list | standard identifier } { deny | permit } { internet | local-AS | no-advertise | no-export | value AS-community_number }
        ip extcommunity-list { named named_list | standard identifier } { deny | permit } rt rt_number
```

**Route Map Configuration**
The following match and set commands have been added to Route-map Configuration mode in support of filtering via BGP communities and extended communities.

```
config

context <context_name>

route-map map_name { deny | permit }

set community { internet | local-AS | no-advertise | no-export | none | value AS-community_number }

match community { named named_list | standard identifier }

set extcommunity rt rt_number

match extcommunity { named named_list | standard identifier }

set local-preference pref_number
```

CSCuh25721 - LAG CLI Enhancements

Applicable Products: All – ASR 5000, ASR 5500

Performance Indicator Changes

`show configuration link-aggregation group`

This command displays the current Link Aggregation Group (LAG) configuration for a specified group number.

`show link aggregation`

This command displays various types of information for all LAG group numbers or a specified group number.

- `info group group_number` – LAG configuration and operating state.
- `lacp info group group_number` – LACP Rx and Tx counters.
- `statistics group group_number` – LAG Rx and Tx counters and data throughput statistics.
- `table [all]` – current LAG port configuration in tabular form. The `all` option includes ATM PVCs for ATM ports (ASR 5000 only)
- `utilization table` – LAG utilization data in tabular form

CSCuh35108 - PGW ASSERT Removal/reduction [Phase 1]

Applicable Products: All

Feature Changes

Call Processing Graceful Asserts
A new CLI Global Configuration command now enables call clearing logic that minimizes the automatic generation of asserts and core dumps during a specific call processing session that may lead to data outage and session manager recovery.

The call clearing logic is only applied to the first assert generated during a call processing session. When that assert occurs, a zero-second timer lets the current stack unwind to avoid reentrancy issues. The call is then dropped from all interfaces. This is considered to be a graceful assert.

A core dump is generated along with any application supplied debug info. The line number and file index of the ASSERT appears in the call-line; the current call-line is marked as being in “assert_hit” scenario.

With a disable-core option set, a core dump is not generated following a graceful assert.

An assert generated after a graceful assert for the same unexpected scenario will cause the call to be dropped and trigger an automatic core dump. Depending on the length of time required to generate the associated core dump, a session manager recovery may be initiated. This is a highly unlikely possibility.

**Previous Behavior:** Drop call and generate a core dump when an unexpected behavior is encountered during a call processing session. Initiate a session manager recovery.

**New Behavior:** When a call processing session encounters an unexpected behavior for the first time, use call clearing logic to drop the call without initiating a session recovery. The assert event is tracked and logged but call processing continues; a session manager recovery is not initiated

**Customer Impact:** Improved capability/functionality

---

**Important:** The graceful assert call clearing logic can only be applied to call processing events, such as VoLTE. It cannot be used for ICSR-SRP scenarios.

---

**Command Changes**

`unexpected-scenario session drop-call`

This is a new command that configures behavior during an unexpected call processing scenario.

```plaintext
configure

  unexpected-scenario session drop-call [ disable-core ]

end
```

**Notes:**

- The default behavior disables the call clearing logic for a graceful assert. This results in automatic core dump generation for unexpected scenarios resulting in control and data outage for the task instance until the core is fully generated.

- The **disable-core** option disables the automatic generation of core dumps when a call is dropped for a specific session.

---

**CSCuh97966 - [ICSR-Volte] CLP level distinction for VoLTE /nonVoLTE/Emergency calls**

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

ICSR Preferential Session Recovery for VoLTE Traffic

For VoLTE specific preferential treatment, it is important to distinguish between VoLTE-voice and non-VoLTE (data only) calls. A new tagging method can be used by ICSR to make VoLTE specific check-pointing decisions, support preferential treatment during session recovery, and identify VoLTE-voice data packets.

The following prerequisites apply to the implementation of this feature:

- A dedicated APN must be reserved for VoLTE traffic.
- A call connected to this APN will not be classified as Active VoLTE unless there is a dedicated bearer matching the VoLTE-configured QCI.
- Preferential treatment would be given to only those calls which are active VoLTE.
- A GGSN call connected to this APN will not be classified as Active VoLTE unless there is network initiated bearer matching the VoLTE-configured QCI.
- VoLTE marking is preserved across a Gn-Gp handoff.

When this feature is enabled via a CLI command, the actions are taken:

- During bearer creation
  - New bearer QCI is matched against APN configuration.
  - If the QCI matches an APN configuration, the bearer is marked for preferential treatment.
  - Flow_entries are modified with this information (if this is first VoLTE bearer).
  - Egtpu_session is updated with the VoLTE tag during a rx_setup request.
  - An indication message informs ECS about the VoLTE tagging.

- During bearer deletion
  - Flow_entry is updated with VoLTE information if this is the last VoLTE bearer.
  - ECS is informed of the deletion via an indication message.

Command Changes

qci

This new APN Configuration mode CLI command specifies the QoS Class Index (QCI) value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

configure

    context context_name

    apn apn_name

    [no] qci value_bytes ims-media

exit

Notes:
• \textit{value} \text\_\textit{bytes} specifies the QCI value [1–9] to be used to mark bearers meeting the subsequent configured classification

Performance Indicator Changes

\textbf{show apn name}

This output of this command will display the configured QCI values.

\textbf{show subscribers ims-only}

The \textit{ims-only} keyword displays VoLTE (IMS) call statistics.

\textbf{show subscribers ggsn-only full}

The IMS-media Bearer parameter in the output of this command shows whether or not a particular bearer is a VoLTE-speech bearer.

\textbf{show subscribers pgw-only full}

The IMS-media Bearer parameter in the output of this command shows whether or not a particular bearer is a VoLTE-speech bearer.

\textbf{CSCui91100 - 'nexthop-forwarding-address' with a dummy address in APN configuration}

\textbf{Applicable Products:} ASR 5000, ASR 5500

Feature Changes

\textbf{Change in next hop behavior in NPU to offload the traffic towards kernel}

\textbf{Previous Behavior:} If the nexthop bit was set in the MED header for the packets sent from the application to the NPU, the NPU found the next hop address from the forwarding route lookup. On failure the NPU did not fall back to the default route. Instead it sent the packet to the kernel (slowpath).

\textbf{New Behavior:} On failure of the forwarding route lookup, instead of sending the packet to the kernel, the NPU falls back to the default route and sends out the packet (fastpath).

\textbf{Customer Impact:} This change should reduce the traffic towards the kernel. High volume load forwarding of packets to the kernel could lead to packet drops due to rate limiting.

\textbf{CSCui91943 - Update default license to include 7 gateways by default}

\textbf{Applicable Products:} PDSN, GGSN, MME, P-GW, SGSN, S-GW
Feature Changes

Basic Configuration License Now Supports Additional Gateways

For manufacturing purposes, the basic configuration license supplied with ASR 5x00 hardware platforms now includes default licenses for the following products and features:

- PDSN [ASR5K-00-PN10SW]
- FA [ASR5K-00-FAXXFA]
- RADIUS AAA Server Groups [ASR5K-00-CSXXAAA]
- HA [ASR5K-00-HA10SW]
- MAG [ASR5K-00-GN10HMAG]
- GGSN [ASR5K-00-GN01S]
- ESS [ASR5K-00-GN10SESS]
- DHCP [ASR5K-00-CSXXDHCP]
- IPv4 Routing Protocols [No license required]
- IPSec [ASR5K-00-CS011-K9]
- L2TP LAC [ASR5K-00-PG01L2LA]
- L2TP LNS [ASR5K-00-CS10L2LN]
- Proxy MIP [ASR5K-00-PN01PMIP]
- IPv6 [No license required]
- Lawful Intercept [ASR5K-00-CSXXLI]
- PCF/BS Monitoring [ASR5K-00-CSXXPCFM]
- Dynamic RADIUS extensions (CoA and PoD) [ASR5K-00-CSXXDYNR]
- User Layer3 Tunneling [No license required]
- RADIUS AAA Server Groups [ASR5K-00-CSXXAAA]
- Starent-Only SGSN [No license required]
- PGW [ASR5K-00-PW10GTWY]
- SGW [ASR5K-00-SW10LIC]
- MME [ASR5K-00-ME01BASE]
- Session Recovery [ASR5K-00-PN01REC]
- ASR5500 Initial System SW, Per UDP C [ASR55-00-SWUDPCK9]
- ASR5500 Initial System SW, Per UMIO [ASR55-00-SWUMIOK9]
- SAE GW Bundle [ASR5K-00-SG01 / ASR5K-00-SG10]

Each gateway license – PDSN, HA, SGSN, GGSN, MME, S-GW and P-GW – includes support for up to 500 sessions. You can display the list of licenses by running the show license info command.
**Important:** Feature and session licenses purchased and installed by the customer will override these default base-level keys.

CSCuj63837 - Remove PSC-PPC-PSCA Support

**Applicable Products:** All (ASR 5000)

**Feature Changes**

**No Support for PSC, PSCA and PPC Packet Processing Cards**

The PSC, PSCA and PPC have reached End of Life (EOL) and are no longer supported with StarOS release 16.0 in the ASR 5000. These cards will be automatically set to offline status – “unknown/unsupported” under release 16.0

CSCun05839 - Show crash all output change is not documented

**Applicable Products:** All

**Performance Indicator Changes**

**show crash**

The outputs of the `show crash list` and `show crash all` commands have been modified to include a timestamp for when the command was run and add it on all information about the management card and card that crashed.

A sample output of the modified output of the crash list command appears below.

```
show crash list

Tuesday January 21 17:04:52 EST 2014

# Time Process Card/CPU/ SW HW_SER_NUM

1 2014-Jan-20+19:26:57 sessmgr 03/0/02715 14.0(51469) SAD151701GD/SAD151903ND
2 2014-Jan-20+18:19:52 sessmgr 02/0/04389 14.0(51469) SAD151701GD/SAD1516024K
3 2014-Jan-20+18:07:16 sessmgr 03/0/26695 14.0(51469) SAD151701GD/SAD151903ND
4 2014-Jan-21+00:39:09 sessmgr 03/0/05060 15.0(52633) SAD151701GD/SAD151903ND
```
Total Crashes : 12

Important: Information about similar crash events is suppressed in the output of this command.

The output of the **show crash all** or **show crash number** commands may contain the following information (based on event type):

- Crash # – unique number assigned by StarOS when logging the crash event
- SW Version – StarOS build release in format: RR.n(bbb)
- Similar Crash Count – number of similar crashes
- Time of first crash – timestamp when first crash occurred in format: YYYY-MM-DD+hh:mm:ss
- Failure message – text of event message
- Function – code identifier
- Process – where the crash occurred (Card, CPU, PID, etc.)
- Crash time – timestamp for when the crash occurred in the format: YYYY-MM-DD+hh:mm:ss <time zone>
- Recent errno – text of most recent error number.
- Stack – memory stack information
- Last Bounce – information about the messaging received prior to the crash
- Registers – memory register contents
- Current inbound message – hexadecimal information for the current inbound message
- Address Map
- Recent heap activity (oldest first)
- Recent events (oldest first)
- Profile depth
StarOS Version Numbering System

The output of the `show version` command displays detailed information about the version of StarOS currently running on the ASR 5x0 or QvPC platform.

Prior to release 16.1, the Image Version version field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the `show version` command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, `show version` will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for 16.1 and onwards releases now include, at minimum, a major, maintenance, and emergency release number, for example “16.1.2”. The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Toolkit to research software releases.

The following diagram shows the differences between the old numbering format and the new numbering format.

![Comparison of Old and New StarOS Version Numbering Formats](image)

In the old format, the first two fields of the Build Version Number represented the Major release and subsequent releases (MRs/ERs) would differ only by build number. Documentation references to a release included descriptive text to indicate whether the release was an MR or ER. For instance, “16.0.65781 MR1” indicates via its descriptor that it is the first maintenance release for 16.0.

In the new format, the maintenance release number changes with subsequent Maintenance Releases (MRs). For example, “16.2” would represent the second maintenance release (MR2) of release 16.

A third digit in the Build Version Number now indicates an Emergency Release for a previous FCS or MR build. For example “16.1.3” indicates the third ER of the first MR of the 16.0 major release.

The Build Version Number may now also include an optional variant indicator just before the ER number to identify the release as a variant of an MR or ER Release. A variant release is one that is given to a particular customer or group of customers, as opposed to a mainstream release which is suitable for all customers.
**Important:** For detailed information on other changes associated with this numbering scheme, refer to the StarOS Version Numbering appendix in the System Administration Guide and the show version chapter of the Statistics and Counters Reference.
Limitations

Demux on MIO/UMIO Restrictions (ASR 5500, CSCub87612)

The following restrictions apply when enabling an MIO/UMIO as a demux card:

- The `require demux management-card` command must be configured before any service or contexts have been created on the system. The command will not execute after a mode of operation has been selected for the chassis.

- Only the following services currently support the designation of an MIO/UMIO card for demux functions: GGSN, HA, LNS-L2TP, P-GW, SAEGW, and S-GW.

- EXGW, HSGW, LAC-L2TP, MME, NEMO, PDSN, and SGSN are not supported.

- After the ASR 5500 has booted with demux functions running on an MIO/UMIO, you cannot configure non-supported services. A maximum of eight Demux Managers are supported. Any attempt to add more than eight Demux Managers will be blocked.

- Service/products requiring a large number of VPN Managers, VRFs and/or Demux Managers must not enable demux functions on an MIO.

- With demux functions running on an MIO, the ASR 5500 supports a maximum of 10 contexts, 15 interfaces per context, with a maximum of 64 interfaces and 250 VRFs per system.

Implementation of this feature assumes that CEPS (Call Events Per Second) and the number of subscribers will remain constant, and only the data rate will increase. This ensures that the CPU demand will not increase on the MIO/UMIO.

Important: Contact Cisco TAC for additional assistance when assessing the impact to system configurations when enabling the Demux on MIO/UMIO feature.

IPv6 Prefix Lengths

On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported. A default route ::/0 is handled as a special case.