CONTENTS

CHAPTER 1

AAA Changes in Release 18  1

AAA Enhancements for 18.5  1

CSCuw61382 - Rf support on HA for offline charging - diameter part  1

Feature Changes  2

Support to Generate RF records for HA Service  2

AAA Enhancements for 18.4  3

CSCuu32592, CSCuv92889 - AAA-Failure-Indication AVP support  3

Feature Changes  3

Support for AAA Failure Indication  3

Limitations and Dependencies  4

Performance Indicator Changes  4

Diameter Authentication Schema  4

show diameter aaa-statistics  4

CSCuu63094 - Supporting an option to include Destination-Host AVP during redirection  5

Feature Changes  5

Destination-Host AVP in Redirected Requests  5

Command Changes  5

destination-host-avp  5

CSCut97277 - Create new customer specific diameter dictionaries for S6b and SWm  6

Feature Changes  6

New Custom Dictionaries for S6b/STa/SWm Interfaces  6

CSCuw38105 - FUI behavior incorrect with both CC-Time and CC-Total-Octets  6

Feature Changes  6

Customized Behavior for MSCC-Level Grant and FUI  6

CSCuv73663 - Suppressing USU in subsequent CCR for 4012/4010 cases  7

Feature Changes  7

Enhancements to Suppress USU in CCR for Blacklisted Content  7

Command Changes  8
diameter msg-type 8

AAA Enhancements for 18.2 8

CSCu023463 - 4 PCSCF addresses per row in PCSCF table 8

Feature Changes 8

IMSA Changes to Support P-CSCF Enhancements 8

Command Changes 9

p-cscf table 9

Performance Indicator Changes 9

show ims-authorization sessions full all 9

CSCup51941 - IMSA changes for pegging stats for Rule Installation failure. 9

Feature Changes 9

Bulk Statistics for Rule Installation Failure 9

Performance Indicator Changes 10

IMSA Schema 10

show ims-authorization policy-control statistics 10

CSCup75954 - P-GW/GGSN needs P-CSCF failure detection support 10

Feature Changes 11

IMSA Changes for P-CSCF Failure Detection 11

CSCup75961 - Req63 - Timers in Deciseconds for Gx interface 11

Feature Changes 11

Configuration Changes to Gx Timers 11

Command Changes 12

diameter request-timeout 12

CSCup95156 - Minimum of 30 IMS_auth_service profiles 12

Feature Changes 12

Extended Support for Configuration of IMS Authorization Service Profiles 12

CSCus02884 - CLI based support for SGSN Change/SGSN Address for 3g call on PGW 12

Feature Changes 13

Configuration Support for SGSN_CHANGE Event Trigger and SGSN-Address AVP 13

Command Changes 13

diameter sgsn-change-reporting 13

Performance Indicator Changes 14

show ims-authorization service name 14
CSCut26593 - Need support for New Gx AVPs for Override Control 14
Feature Changes 14
   New Diameter AVPs for Override Control 14
CSCut41965 - Transparent-Data over Gx (eGCDRand Gy) 14
Feature Changes 14
   Parsing Support for SN-Transparent-Data AVP over Gx 14
AAA Enhancements for 18.1 15
CSCtz79646, CSCuh67284 - PCSCF discovery - v4/v6 addresses not sent always for v4/v6 pdn req 15
Feature Changes 16
   Send P-CSCF Address Based on PCO Request 16
CSCud26703 - Enable / disable multiple back to back CCR-Us from PGW/GGSN 16
Feature Changes 16
   Multiple CCR-Us Support Over Gx Interface 16
Command Changes 17
   max-outstanding-ccr-u 17
Performance Indicator Changes 17
   show ims-authorization policy-control statistics 17
CSCup48777 - Allow OOC Triggers to fire for the same rating group in different rules 18
Feature Changes 18
   Generating OOC/ROC with Changing Association between Rule and RG 18
CSCup48800, CSCur13722, CSCuo03073 - Any cut IR must contain a snapshot of all present RGs usage 18
Feature Changes 18
   Snapshot of all RGs during Rf Interim Record 18
Command Changes 19
   rf report-all-active-rgs 19
CSCup58702, CSCuo53205 - Support for 3gpp based RAN/NAS Cause IE on gx interface 19
Feature Changes 19
   Support for "RAN/NAS Cause" IE on Gx Interface 19
Command Changes 20
   diameter encode-supported-features 20
Performance Indicator Changes 20
   show ims-authorization sessions full all 20
CSCup71713, CSCup71684 - PGW RTT Support for Diameter procedures 20
Feature Changes 20
  RTT Support for P-GW 20
Command Changes 21
  reporting-action event-record 21
  show event-record 22
Performance Indicator Changes 22
  System Schema 22
  show event-record statistics pgw 23
CSCup75820, CSCup77479, CSCuq75294, CSCuq05896, CSCur84088 - Rel 11 - Support
  ADC rules 23
Feature Changes 24
  Support ADC Rules over Gx 24
Performance Indicator Changes 24
  show ims-authorization service statistics 24
  show ims-authorization sessions full all 24
CSCup75830, CSCus96670 - DPC2: Diam proxy scaling 25
Feature Changes 25
  Scaling of Diameter Proxy to Support DPC2 25
Command Changes 25
  require diameter proxy 25
  logging filter 26
Performance Indicator Changes 26
  show diameter proclet-map-memcache 26
  show diameter proclet-map-table 26
CSCup75837 - Wild Card Diameter Routing 26
Feature Changes 26
  Configuration Support for Wildcard Diameter Routing 26
Command Changes 27
  route-entry 27
CSCup75969, CSCuq46538 - EDR to include PCRF correlation identifier 27
Feature Changes 28
  Support for Parsing PCRF-Correlation-Id AVP 28
CSCup75973 - Req70 - AVP Charging-Information and AVP Redirect-Host 28
Feature Changes 28
  Support for Charging-Information and Redirect-Host AVPs 28
CSCup75991 - IPSG support for SN-CF-Policy ID AVP on Gx interface 28
   Feature Changes 28
      Support for SN-CF-Policy-ID AVP on IPSG 28
CSCup75999 - Static Rulebase for CCR 29
   Feature Changes 29
      Static Rulebase for CCR 29
      Command Changes 29
         charging-rulebase-name 29
CSCup76005 - Populate Serving Node PLMN on Rf for eHRPD 30
   Feature Changes 30
      Populate Serving Node AVP on Rf for eHRPD 30
CSCup89673, CSCup89677, CSCup73076, CSCup92630, CSCup82660 - Gx changes to support
   Timezone in CCR-U and CCR-T 30
   Feature Changes 30
      Support for Timezone in CCR-U and CCR-T 30
CSCup91609 - Diamproxy memory usage is in over state for 3G S4 Ceps tests 31
   Feature Changes 31
      IMSI Table in Diamproxy 31
CSCup95956, CSCum42002 - DPC2: AAA Proxy/AAA MGr scaling 31
   Feature Changes 31
      Scaling of AAA Proxy/AAA Manager to Support DPC2 31
CSCup95998 - PSP algorithm modification - AAA changes 31
   Feature Changes 31
      New AAA Attribute for APN Configured Bandwidth Policy 31
CSCuq06614 - Radius AVP SN-Rad-APN-Name to be added in custom67 32
   Feature Changes 32
      Support for SN1-RAD-APN-Name AVP in custom67 32
CSCuq07202 - DPC2: CoA/DM from non-admin AAAMgr should send msg to messenger
   proxy 32
   Feature Changes 32
      Broadcast Messenger Support in AAAMgr and AAAProxy 32
CSCuq08626 - Separate Rf implementation for Customers 33
   Feature Changes 33
      Customer-Specific Dictionaries for Rf Implementation 33
CSCuq12013 - IMSA LTE/WiFi GTP S2b Make-Before-Break HO Compliance 33
Feature Changes 33

IMSA Changes for LTE/WiFi GTP S2b Make-Before-Break HO Compliance 33

CSCuq14925 - Gx support for GTP based s2a/s2b 33

Feature Changes 33

Gx Support for GTP based S2a/S2b 33

CSCuq14928, CSCuq23613 - Gy support for GTP based s2a/s2b 34

Feature Changes 34

AVP Support in Gy for GTP based S2a/S2b 34

Command Changes 34

diameter update-dictionary-avps 34

CSCuq65644, CSCup42837 - Diameter support for PMIPv6 Subscriber Continuity Support 34

Feature Changes 35

AVP Support for PMIPv6 Subscriber Continuity 35

CSCur08378 - DCCA LTE/WiFi GTP S2b Make-Before-Break HO Compliance 35

Feature Changes 35

Suppress OOC/ROC During LTE-WiFi Handoff 35

CSCur15061 - State of RADIUS server stuck in 'Waiting-for-response-to-Acct-On' 35

Feature Changes 35

Change in Accounting-On Transaction Logic 35

CSCur35107 - Abnormal bearer termination 36

Feature Changes 36

New Disconnect Reasons for GTP Path Failures 36

CSCur62919 - Change to the logging facility for diactrl 37

Feature Changes 37

New Logging Facility for Diactrl 37

Command Changes 37

logging filter 37

CSCus62331 - PGW NOT sending CCR-T to PCRF on arrival of CCA-I post guard timer expiry 37

Feature Changes 37

CCR-T Triggering Post Tx Timer Expiry 37

CSCus66465 - show diameter route status command causes high CPU utilization alarms 38

Feature Changes 38
Changes to "show diameter route" Command 38
CSCus75159 - PGW not populating NRS AVP on handoff to LTE 38
Feature Changes 38
Encoding of Network-Request-Support AVP During Handoff to LTE 38
CSCut02257 - Retrigger timer-expiry triggers if its suppressed during ICSR switchover 38
Feature Changes 38
Triggering of CCRs for Validity Timer During ICSR Switchover 38
CSCut06448 - ASR5500 diameter peers fail to come up after planned SRP switchover 39
Feature Changes 39
Diamproxies in Standby Chassis Mode 39
CSCut25885 - Fatal Sig 11: Seg fault PC: acsmgr_get_bearer_bw_from_rules.isra.176() 39
Feature Changes 39
Handling of BCM Value 39
AAA Enhancements for 18.0 39
CSCup38881 - [ePDG]- Diameter stack enh for custom SWm to SWu mapping 40
Feature Changes 40
Attribute Support for Custom SWm to SWu Error Code Mapping 40
CSCuq11182 - [ePDG]: dia auth fail handling does not support 5xxx codes for retry 40
Feature Changes 40
Failure Handling for 5xxx Result Codes in SWm Dictionary 40
CSCur26626 - [ePDG] Non UICC device support EAP-TLS/EAP-TTLS support Diameter changes 40
Feature Changes 41
New AVP in DER Message for SWm Dictionary 41
CSCur31589 - [SAMOGR18] Need support in Diameter dictionary to support LBO AVPs 41
Feature Changes 41
Diameter AVP Support for LBO 41

CHAPTER 2

ADC Changes in Release 18 43
ADC Enhancements for 18.1 43
CSCuq05896 - ADC support over Gx 43
Feature Changes 44
ADC Support over Gx Interface 44
Limitations 45
Command Changes 45
action priority 45
diameter encode-supported-features 46
show subscribers 46
Performance Indicator Changes 46
show active-charging service statistics 46
show active-charging sessions full all 46
show ims-authorization service statistics 47
show ims-authorization sessions full all 47
show subscribers callid <callid> adc readdress statistics 47

CHAPTER 3

ECS Changes in Release 18 49

ECS Enhancements for 18.4 49
CSCuw12560, CSCuw33132 - IPv6-OS-Signature based Tethering solution 49
Feature Changes 49
IPv6 OS-based Tethering Detection 49
Command Changes 50
tethering-database 50
tethering-detection 50
tethering-detection 51
rule-variable 51
upgrade tethering-detection 52
Performance Indicator Changes 52
ECS Schema 52
show active-charging rulebase statistics name 52
show active-charging tethering-detection statistics 52
CSCuw36228 - Incorrect tagging of TTL in the EDR records 52
Feature Changes 52
IP TTL Value in EDR Records 52
ECS Enhancements for 18.2 53
CSCus80666 - Dis-engage TRM when a flow moves from one bearer to another 53
Feature Changes 53
TRM Flows 53
CSCus96377 - Reset Flow-Bearer mapping is missed in certain scenarios 53
Feature Changes 54
ACS Data Flow-Bearer Association 54
CSCut05534 - Per subscriber traffic steering/marking  54
Feature Changes  54
   Per Subscriber Traffic Steering  54
   Performance Indicator Changes  55
      show active-charging subscribers callid <call_id> override-control  55
CSCut93985 - IP-TTL based Tethering solution  55
Feature Changes  55
   IP-TTL based Tethering Detection  55
Command Changes  56
   tethering-detection  56
   tethering-detection  56
   rule-variable  56
Performance Indicator Changes  57
   ECS Schema  57
      show active-charging rulebase name  57
      show active-charging rulebase statistics name  57
      show active-charging tethering-detection statistics  57
CSCut97261 - FAPA support for Customer  58
Feature Changes  58
   Tethered Flows using FAPA  58
CSCut99876 - No CCR-U for rule-binding failure incase CBR was pending  58
Feature Changes  58
   Triggering of CCR-U for Reporting Rule Failure During Collision  58
ECS Enhancements for 18.1  59
   CSCui85235, CSCut15652 - Change-condition issue in Rf record when OCS/ Gy is down during CCR  59
      Feature Changes  59
         New Change Condition for Rf Record in Gy Server Unreachable Scenario  59
   CSCun96897 - Simplification of ECS show CLI's- phase II  59
      Feature Changes  59
         Enhancement for Ruledef Statistics  59
Command Changes  60
   statistics-collection  60
   statistics-collection  60
   show active-charging subscribers  61
Performance Indicator Changes 61
  show active-charging sessions full 61
  show active-charging subscribers full 62
CSCuo23808, CSCup52344, CSCuq97903 - Enhancement for SIP Analyzer Statistics 63
  Feature Changes 63
    Support for enhanced SIP Analyzer Statistics 63
  Command Changes 64
    sip request method 64
Performance Indicator Changes 64
  ECS Schema 64
    show active-charging analyzer statistics name sip 66
CSCuo61507 - Enhance EDR timestamps with 10ms granularity 67
  Feature Changes 67
    New Timestamp Formats for more Granular EDRs 67
  Command Changes 67
    attribute 67
CSCuo68909 - TCP flows modification (RFC 1122, Section 4.2.2.13) 68
  Feature Changes 68
    Modification of TCP Flows 68
  Command Changes 68
    tcp 2msl-timeout 68
Performance Indicator Changes 68
  show active-charging rulebase name 68
  show active-charging rulebase statistics name 69
CSCup42837, CSCup44247 - PMIPv6 Subscriber Continuity Support 69
  Feature Changes 69
    Support for PMIPv6 Analyzer 69
  Command Changes 69
    clear active-charging analyzer statistics 69
    permission 70
    permission 70
    route priority 70
Performance Indicator Changes 70
  ECS Schema 70
    show active-charging analyzer statistics name mipv6 70

show active-charging subsystem all 71
CSCup44069, CSCup91558 - EDR enhancement to support NEMO MR Hosts 71
Feature Changes 71
   EDR Enhancement to Support NEMO MR Hosts 71
Command Changes 72
   attribute 72
   rule-variable 72
   edr nemo-call 72
CSCup77479 - ADC rule support over Gx interface as per Release 11 73
Feature Changes 73
   ADC over Gx Interface 73
   Limitations 74
Command Changes 74
   diameter encode-supported-features 74
   show subscribers 74
Performance Indicator Changes 75
   show active-charging service statistics 75
   show active-charging sessions full all 75
   show ims-authorization service statistics 75
   show ims-authorization sessions full all 76
   show subscribers callid <callid> adc readdress statistics 76
CSCup92630, CSCup82660, CSCup89677, CSCup89673, CSCup73076 - ECS support for ULI Enhancements 76
Feature Changes 76
   Enhancements In Network Provided Location Information 76
CSCup99498 - ECS support for IPv6 wildcards in "ip server-ip-address" CLI 76
Feature Changes 77
   IPv6 Wildcard Support 77
Command Changes 77
   ip 77
CSCuq04032 - [A-ECS] RTP flows can be accelerated after first rule-match 77
Feature Changes 77
   Support for Accelerated RTP Flows 77
Performance Indicator Changes 78
   ECS Schema 78
show active-charging analyzer statistics name rtp

CSCq12003, CSCq11994, CSCup98379, CSCus94777 - ECS LTE/WiFi GTP S2b
Make-Before-Break HO Compliance

Feature Changes

Support for Seamless Handoff from LTE to WiFi

CSCq26322, CSCup89524 - Discontinue "if-protocol" CLI from ruledef config mode

Feature Changes

Deprecation of "if-protocol" CLI command

Command Changes

if-protocol

CSCq46538, CSCup75969, CSCq04720 - EDR to include PCRF correlation identifier

Feature Changes

Inclusion of PCRF Correlation ID in EDRs

Command Changes

rule-variable bearer

Performance Indicator Changes

show active-charging edr-format all

show configuration

CSCq73688 - Debug CLI to show subscriber map info

Feature Changes

Support for Subscriber Map Information

Command Changes

debug acsmgr

CSCq89417 - Allow use of TAB character as EDR delimiter rather than COMMA

Feature Changes

New Delimiter for EDRs

Command Changes

delimiter

CSCur31337 - vrf-name attribute in EDR and UDR

Feature Changes

UDR Enhancement to Support NEMO Hosts

Command Changes

attribute
CSCur65367 - HO trigger handling needed in populate_edr_field_sgsn for GGSN PGW calls 82
  Feature Changes 82
  Handling Inter SGSN and Inter S-GW Handoff Triggers 82

CSCus28519 - Incorrect UL/DL byte count when non-wsp traffic routed to WSP analyzer 83
  Feature Changes 83
  Non-WSP traffic to WSP analyzer 83

CSCus77206 - Rule level volume is reported as 0 in CCR-T for CCA-U delay 83
  Feature Changes 83
  Rule Level Usage Monitoring for CCA-U Delay 83

CSCus78756 - Need to add support for override control license 83
  Feature Changes 84
  New License for Override Control Feature 84

CSCut05601 - Signal Aborted at libc.so.6/___ncmp_ia32 84
  Feature Changes 84
  Maximum SIP Calls Per Susbcriber 84

CSCuu00275 - unlink_ca_prime_for_sub() Sessmgr crash seen on Customer Ares DxGW Setup 84
  Feature Changes 84
  Use of "update active-charging override-control rulebase-config" Command on Standby Chassis 84

CSCuu05981 - [acsmgr91300 info] debug logs printed only once with update act-chg CLI 85
  Feature Changes 85
  Change in Error Log Display 85

CHAPTER 4  ePDG Changes in Release 18 87
  ePDG Enhancements for 18.4 87
    CSCux26495 - Configurable EBI range on ePDG 88
      Feature Changes 88
      Configuring EBI range 88
      Monitoring and Troubleshooting the Configurable EBI range for Bearers in ePDG 89
      Configurable EBI Range for Bearers Support Show Command Outputs 89
    CSCuu32592 - AAA-Failure-Indication AVP support 89
    CSCuv73157 - UE Local IP Address IE in the S2b Interface over GTPv2 90
      Feature Changes 90
SUE Local IP Address IE in the S2b Interface over GTPv2t 90

ePDG Enhancements for 18.2 90
  CSCuu24382 - Support for IPSEC Integrity algorithm HMAC-SHA2 91
    Feature Changes 91
    SHA2 HMAC algorithms support 91
  CSCut20186 - Fast reauth support for ePDG 91
    Feature Changes 91
    Performance Indicator Changes 91
    Monitoring and Troubleshooting the ePDG Fast Re-Auth Support 91
    ePDG Fast Re-Auth Support Show Command Outputs 91
  CSCut20186 - Support for DSCP marking in SWu interface downlink packets 92
    Feature Changes 92
    vPC-DI for ePDG 92
    Feature Changes 92
  CSCut20141 - Offline Charging (CDR) support for ePDG 92
    Feature Changes 92
    Data buffering support for DL pkts for DL pkts before session establishment 92
    Performance Indicator Changes 93
    GTPP Schema 93
  CSCuu51841 - Unable to scale when OCSP is not reachable 93
    Feature Changes 93
    Scale up issue 93
    Command Changes 93
    timeout 93

ePDG Enhancements for 18.0 94
  CSCun88535 - Data buffering support for DL pkts before session establishment 94
    Feature Changes 94
    Data buffering support for DL pkts for DL pkts before session establishment 94
    Command Changes 94
    data-buffering 94
  CSCup26465 - Non VoLTE data outage improvements 95
    Feature Changes 95
    Non VoLTE data outage improvements 95
  CSCup35998 - IPSec scale and performance improvement on SSI 95
    Feature Changes 95
IPSec scale and performance improvement on SSI  
CSCup38880, CSCup38881, CSCup38882 - Custom SWm to SWu error code mapping  
Feature Changes  
Custom SWm to SWu error code mapping  
Command Changes  
custom-swm-swu-error-mapping  
CSCup44422 - Session Audit Removal from demuxmgr ePDG  
Feature Changes  
Session Audit Removal from demuxmgr ePDG  
CSCup90380 - ePDG bearer duration KPIs  
Feature Changes  
ePDG bearer duration KPIs  
Performance Indicator Changes  
show session duration apn  
ePDG Schema  
ePDG APN QCI Duration Schema  
ICSR based upgrade and downgrade between N and N-2 Release Support  
Feature Changes  
Upgrade and Downgrade between N and N-2 Release  

CHAPTER 5 GGSN Changes in Release 18  
GGSN Enhancements for 18.5  
CSCuw08643 - v6 support on newcall duplicate subscriber requested addr accept  
Feature Changes  
Duplicate Address Support for IPV6  
Command Changes  
duplicate-subscriber-requested-v6-address  
Performance Indicator Changes  
show configuration  
show configuration verbose  
show ggsn-service name <ggsn-service-name>  
GGSN Enhancements for 18.4  
CSCuv49840 - Non standard QCI modificaiton fails when mapped to same pre-rel8 QCI  
Feature Changes  
Pre-Release 8 QoS Mapping
GGSN Enhancements for 18.2 102
CSCuc83409 - 'show gtpc summary' not able to filter on imsi, ip-address, callid, username 103
  Feature Changes 103
    Change to the 'show gtpc' CLI Command 103
  Performance Indicator Changes 103
    show gtpc 103
    show gtpc summary 104
CSCur80803 - Supporting Counters to Report 2G & 3G PDP Numbers in GTP-C Schemas 104
  Feature Changes 104
    New Counters to Report 2G and 3G PDP Numbers in GTP-C Schema 104
  Performance Indicator Changes 104
    GTP-C Schema 104
    show gtpc statistics 105
CSCur85219 - New GGSN counter to measure connected subscribers 105
  Feature Changes 105
    New GGSN Counter to Measure Connected Subscribers 105
  Performance Indicator Changes 105
    GTP-C Schema 105
    show gtpc statistics 105
CSCur85237 - SFR: Licensing Bulkstats enhancements (Subscriber vs Sessions count) 106
  Feature Changes 106
    Licensing Bulkstats Enhancements 106
  Performance Indicator Changes 106
    APN Schema 106
    show apn statistics name <apn_name> | all 106
CSCus11708 - L2TP support with Demux on MIO 107
  Feature Changes 107
    L2TP Support with Demux on MIO (ASR 5500) 107
GGSN Enhancements for 18.1 107
CSCun23280 - GTP Throttling Stats plugging to RLF Stats 108
  Feature Changes 108
    Support for GTP-C RLF Statistics 108
Performance Indicator Changes  108
  show rlf-context-statistics sessmgr gtpc-context-name ingress  108
  show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress  108
  show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress summary  108
  show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress verbose  108
  show rlf-memcache-statistics sessmgr  108
  show rlf-memcache-statistics sessmgr instance 1  108
  clear rlf-context-statistics sessmgr gtpc-context-name ingress  108

CSCus07270 - [GGSN]: CLI 'show subscribers ggsn-only full all' having incorrect value  109

Feature Changes  109
  Correction In The Output Text of CLI Command  109
  Performance Indicator Changes  109
    show subscribers ggsn-only full all  109

CSCus25086 - Incorrect qosNegotiated seen in custom6 GCDR  109

Feature Changes  109
  Change in Peak Throughput in QoS  109

CHAPTER 6

GTPP Changes in Release 18  111

GTPP Enhancements for 18.4  111
  CSCux26716 - Not able to specify GTPP data record format on using custom48 dictionary  111
    Feature Changes  112
      Data Record Format Version for CDRs  112

GTPP Enhancements for 18.2  112
  CSCut20167 - [ePDG] AAAMGR support for Offline Charging (CDR) feature in ePDG  112
    Feature Changes  112
      New GTPP Dictionary to Support ePDG CDRs  112

Performance Indicator Changes  113
  IMSA Schema  113
    show gtpp counters all  113
    show gtpp statistics  113
    show session subsystem facility aaaprox all  113

CSCuu25810 - Add AF-Charging-Identifier to new custom CDR dictionary  114
    Feature Changes  114
New GTPP Dictionary to Support AF-Charging-Identifier AVP 114

GTPP Enhancements for 18.1 114
CSCua96527 - SP WiFi - LMA support for P-GW CDR 114

Feature Changes 114
CDR Support for Trusted/Untrusted WLAN 114
Command Changes 115
gtp command 115

Performance Indicator Changes 115
show gtpp group all 115
CSCup88805, CSCur35107, CSCuq08380 - Abnormal bearer termination info in CDR for Customer 115

Feature Changes 115
Support for Abnormal Bearer Termination Cause in CDR 115
CSCuq08380, CSCup88805 - Diagnostic field to be updated in SGWCDR for custom34/35 116

Feature Changes 116
Abnormal Bearer Termination Cause in Diagnostic Field for SGW-CDRs 116
Command Changes 117
gtp attribute diagnostics 117
CSCuq15013 - Removing the limitation of one Service Data container per CDR for Customer 117

Feature Changes 117
Configurable Service Data Container for CDR 117
CSCuq51466 - [ECS] Release closure CDRs handling with NPLI feature 118

Feature Changes 118
Applying New ULI/Tz across all Bearers 118
CSCus30283 - PGW-Gz Redesign Cust35: Cause sequence reversed in PGWCDR 118

Feature Changes 118
Cosmetic Change to PGW-CDR Fields 118

HA Changes in Release 18 119

HA Enhancements for 18.2 119
CSCup91515 - Enhancement for Additional AVPs in MIP Tunnel 119

Feature Changes 119
MIP RRQ Enhancement 119
CHAPTER 8

HeNBGW Changes in Release 18 125

HeNBGW Enhancements for 18.2 125

CSCu28128 - HeNB-GW: Support for show subscribers henbgw-only ebi | qci. 126

Performance Indicator Changes 126

show henbgw session qci 126

show henbgw session full qci 126

show henbgw session summary qci 126

CSCuo65686 - Support R12 CMAS PWS Restart Indication Message 126

Performance Indicator Changes 126

henbgw-access schema 126

henbgw-network schema 126

CSCuo78931 - HeNBGW MOCN support 127

Performance Indicator Changes 127

show henbgw-access-service henb-association full 127

show henbgw henb-association full 127
CSCup47037 - HeNBGW: Default and configured Overload params show support is needed 127

Feature Changes 127
   Overload parameters show support 127

CSCup68855 - HeNBGW support on Virtual Platform (QvPC-DI) 128

Feature Changes 128
   Virtual platform support 128

CSCup68867 - HeNBGW support on ASR5500 128

Feature Changes 128
   ASR 5500 platform support 128

CSCup71541 - HeNBGW Support for X2 proxy 128

Feature Changes 128
   X2 proxy GW support 128

Command Changes 128
   bind 128
   x2-c 129
   associate x2gw-service 129

Performance Indicator Changes 129
   show x2gw-service 129

CSCuq06852 - HENBGW - Bulkstats var missing for WRWReq WRWResp in access and network 129

Performance Indicator Changes 129
   henbgw-access schema 129
   henbgw-network schema 129

CSCuq16083 - HENBGW-neg: Crash on handling 10k pws msg | sn_s1ap_pws_get_decoded_msg 130

Feature Changes 130
   Handling 10k pws msg 130

CSCuq28605 - HeNBGW:S1 association shouldn't successful with MME of duplicate GUMMEI 130

Duplicate GUMMEI handling 130
   Handling of duplicate GUMMEIs 130

CSCuq59203 - HeNBGW support on Virtual Platform (QvPC-SI) 130

Feature Changes 130
   HeNBGW QvPC-SI supprot 130
CSCur84827 - HENBGW: Bulkstats support required for PWS Restart message.  131
  Performance Indicator Changes  131
    henbgw-access schema  131
    henbgw-network schema  131
CSCut40006 - HENBGW:Di: drvctrl process in warn state on loading build 18.2.0.59380  131
CSCut55898 - S1 Full/Partial Reset for MOCN  131
  Command Changes  131
    s1-reset  131
CSCuu12717 - Handling of RESET messages from MME and HENB  132
  Feature Changes  132
    Handling RESET messages from MME and HENB  132
CSCuu24106 - S1AP Cause based stats based on TAI for MOCN  132
  Feature Changes  132
    TAI for MOCN  132

CHAPTER 9  HENBGW Changes in Release 18  133

HNBGW Enhancements for 18.2  133
  CSCts49192 - ASR5K-HNBGW-00040 - Enhancements to Access Control List (ACL)  134
    Feature Changes  134
    Command Changes  134
      hnb-access-mode closed  134
    Performance Indicator Changes  134
      show hnbgw-service  134
CSCup01809 - [CBS] Incorrect value of CLI "sabp timer <timer_value>"  135
  Feature Changes  135
    sabp timer <timer_value>  135
CSCup96215 - RTCP enhancements to support RTCP on Iu interface  135
  Feature Changes  135
    RTCP on Iu interface support  135
CSCup96781 - HNBAP Configuration transfer procedure support  135
  Feature Changes  135
    HNBAP Configuration transfer procedure  135
    Command Changes  136
      hnb-config-transfer  136
CSCup97007 - Emergency call behavior overhaul  136
CSCur55959 - 10k UEs per HNB support for HNBGW 136
  Feature Changes 136
    10k UEs per HNB support 136
  Command Changes 136
    hnb-aggregation 136
  Performance Indicator Changes 137
    show configuration 137
    show configuration verbose 137
    show hnbgw-service all 137
CSCur79073 - F2F SRNS relocation fails due to access control failure for emergency IU 138
  Feature Changes 138
    Relocation failure due to access control failure 138
CSCut18057 - [16.1.7] CLI o/p is not correct when phase2/3 timers are disabled 138
  Feature Changes 138
    CLI Output when Phase 2/3 timers are disabled 138
CSCus25924 - [18.0] HNB accept msg is coming with different Cell-access-mode in ACL 139
  Feature Changes 139
    Accept msg is coming with different Cell-access-mode in ACL 139

CHAPTER 10  HSGW Changes in Release 18 141
  HSGW Enhancements for 18.2 141
  CSCut74593 - MEID in PBU 142
    Feature Changes 142
      Hardware ID Support in Proxy Binding Update (PBU) Messages 142
    Command Changes 142
      information-element-set 142
    Performance Indicator Changes 143
      show configuration 143
      show configuration context mag 143
      show lma-service session full 143
      show mag-service all 143

CHAPTER 11  MME Changes in Release 18 145
MME Enhancements for 18.5 145

CSCuv27053 - Purge-request towards only one HSS after sessmgr crash 146
  Feature Changes 146
  Purge Request Behavior 146
CSCuw29857 - M-TMSI Allocation algorithm enhancement 146
  Feature Changes 146
  P-TMSI/M-TMSI Allocation Algorithm Enhancements 146
CSCuw97149 - Operator Policy based on IMEI TAC selection 147
  Feature Changes 147
  Operator Policy Selection Based on IMEI-TAC 147
  Command Changes 147
  precedence 147
CSCux04060 - Non-delivery of Modify Bearer Msg leads to loss of PDN 148
  Feature Changes 148
  NAS-NON-DELIVERY for Modify Bearer Msg 148
  Command Changes 148
  policy 148
CSCux13166 - MME releases UE context with Category NAS Unspecified for non-TAU 149
  Feature Changes 149
  Command Changes 149
  s1-ue-context-release 149
CSCux26819 - MME should intimate dedicated bearer its default bearer will be deleted 150
  Feature Changes 150
CSCux33388, CSCur41900 - CLI Control for Target Access Restriction 151
  Feature Changes 151
  Target Access Restriction 151
  Command Changes for the MME 152
  access-restriction-data 152
  Command Changes for the SGSN 152
  access-restriction-data 152
  Performance Indicator Changes 153
  show call-control-profile 153
  show configuration verbose 153
MME Enhancements for 18.4 153
CSCuu94088, CSCuu87580 - A-MSISDN / MSIM for VoLTE 154
Feature Changes 154
   A-MSISDN Flag Support in Features List AVP for ULR 154
Command Changes 155
   diameter update-dictionary-avps 155
   a-msisdn 155
Performance Indicator Changes 155
   show call-control-profile full all 155
CSCu53725, CSCu14176 - Enforce License for SBC 156
Feature Changes 156
   SBC License Enforced 156
CSCu73207 - MME not compliant with 3GPP 24.301 CR 2098 156
Feature Changes 156
   Cause Code in Attach Reject when EPS Subscription Not Present 156
Performance Indicator Changes 157
   MME Schema 157
CSCu17197 - PLA dropped by DRA when sent from another PSC card 157
Feature Changes 157
   PLA and PLR Using Same Connection 157
MME Enhancements for 18.2 157
CSCu17478, CSCu29064 - Support for Mis-Spelled APN Name Correction 158
Feature Changes 158
   Default APN for DNS Failures 158
Command Changes 159
   apn-selection-default 159
Performance Indicator Changes 159
   show apn-remap-table full all 159
CSCu24510 - MME support for EMERGENCY_CALL_RELEASE event in lcs service 159
Feature Changes 159
   MME Notifies GMLC of Emergency Call Release 159
CSCus32031 - Separate Authentication Message routing from MME to AuC 160
Feature Changes 160
   Additional Routing for Authentication Messages from MME to AuC 160
Command Changes 160
   diameter hss-endpoint 160
Performance Indicator Changes 161
  show hss-peer-service service all 161
CSCus96030 - CSFB support for CDMA Network enhancements - lab quality 161
Feature Changes 161
  CSFB for 1XRTT 161
Command Changes 162
Performance Indicator Changes 162
  S102 Schema 162
CSCut68757 - Need support of 'Change to Report Flags' IE in EGTP 163
Feature Changes 163
  'Change to Report Flags' IE 163
CSCuu02102 - eSRVCC Implementation for 1XRTT 163
Feature Changes 163
  eSRVCC for CDMA 163
Command Changes 164
Performance Indicator Changes 164
  S102 Schema 164
MME Enhancements for 18.1 165
CSCtx81747 - MME Integration to IPNE to activate Location Report Procedures 165
Feature Changes 165
  IPNE Service Support 165
Command Changes 166
  ipne-service 166
  ipne-endpoint 166
  associate 167
Performance Indicator Changes 167
  MME Schema 167
    show ipne peers { all | service | summary } 168
    show ipne statistics { all | service | summary } 168
CSCui82362, CSCum50067, CSCur31142, CSCup89617 - MME to select the co-located SGSN in case of handoffs from MME to SGSN 169
SGSN-MME Combo Optimization 169
Command Changes 169
  sgsn-mme 169
Performance Indicator Changes 170
MME Schema 170
show lte-policy sgsn-mme summary 170
show hss-peer-service statistics all 170
show mme-service statistics handover 171

CSCu07975 - Splitting up of points of failure when the MME signals Network failure. 171
Feature Changes 171
 Counters Focusing on Points of Failure 171
Performance Indicator Changes 172
 MME Schema 172
 show mme-service statistics 174

CSCul34979 - MME TAI level stats for ESM procedures 175
Performance Indicator Changes 175
 TAI Schema 175

CSCul63403 - MME S6a: Skip-Subscriber-Data when UE moves to 4G from a colocated SGSN 178
Feature Changes 178
 Skip-Subscriber-Data Bit Reduces Signaling 178

CSCup66362, CSCup66417 - MME: Scale IMSIMgr 178
Feature Changes 178
 IMSI Manager Scaling 178
Command Changes 179
 task facility imsimgr 179
Performance Indicator Changes 180
 show task resources facility imsimgr all 180
 show subscribers mme-only full all 180
 show mme-service session full all 180
 show mme-service db record call-id 180
 show demux-mgr statistics sgtcpmgr instance <instance> 180
 show demux-mgr statistics egtpegrmgr all 180
 show session subsystem facility mmemgr instance <instance> 180
 show snmp trap history 180

CSCup66691, CSCuq25983 - eCSFB support for CDMA Network 181
Feature Changes 181
 CSFB-SRVCC for CDMA and for S102 181
Command Changes 181
Performance Indicator Changes  181
  S102 Schema  181
CSCup66766 - MME support on VPC-DI  182
  Feature Changes  182
    MMEMgr Scaling to Support VPC-DI  182
Command Changes  183
  task facility mmemgr  183
  congestion-control threshold  183
Performance Indicator Changes  184
  show congestion-control configuration  184
CSCur24765 - Instance number should be included in the snmp trap generated by imsimgr  184
  Feature Changes  184
    Support for Multiple IMSIMgr Instances  184
CSCur34618 - [MME] IMSI Mgr Audit and show CLI  184
  Feature Changes  184
    IMSIMgr Audit  184
    Command Changes  185
      mme imsimgr  185
CSCus32182 - MME doesn't store the ARD related info under any CLI output  185
  Feature Changes  185
    New Fields Display ARD-related Data  185
Performance Indicator Changes  185
  show mme-service db record  185
CSCus34861 - MME is not using NAPTR with least preference first for MSC selection  186
  Feature Changes  186
    Enabling Weight-based MSC Selection  186
Command Changes  186
  peer-msc  186
Performance Indicator Changes  186
  show configuration  186
CSCut28685 - SGSN - Issue with Combo subscription sharing wrt ambr values  187
  Feature Changes  187
    Subscription Sharing Issues for MME/SGSN Combo  187

CHAPTER 12  NAT Changes in Release 18  189
NAT Enhancements for 18.1 189

CSCuo78207 - [NAT] Stats to display MAX port usage of subscribers 189

Feature Changes 189

Port Utilization by Subscribers 189

Performance Indicator Changes 190

show active-charging firewall statistics verbose 190

show active-charging nat statistics 190

CSCup47715 - Pilot Packet Format and Trigger Update 190

Feature Changes 190

Support for Pilot Packet Format and Trigger 190

Command Changes 191

pilot-packet 191

Performance Indicator Changes 191

APN Schema 191

System Schema 191

show apn statistics name 192

show pilot-packet statistics all 192

show session subsystem facility sessmgr all 192

CSCup49820 - [NAT] Support for forcible NAT IP release CLI as part of MOP 192

Feature Changes 192

Forcible NAT IP Release 192

Command Changes 193

clear nat-ip 193

CHAPTER 13

PDSN Changes in Release 18 195

PDSN Enhancements for 18.1 195

CSCup44247, CSCup42837 - SM support for PMIPv6 Subscriber Continuity Support 195

Feature Changes 195

Session Manager (SM) support for PMIPv6 Subscriber Continuity 195

CSCus41228 - PDSN not to terminate PPP session when handoff within a restricted zone 196

Feature Changes 196

PDSN not to terminate PPP session when handoff is within a restricted zone. 196

CHAPTER 14

P-GW Changes in Release 18 197
P-GW Enhancements for 18.5 197
  CSCuw08643 - v6 support on newcall duplicate subscriber requested addr accept 198
  Feature Changes 198
  Duplicate Address Support for IPV6 198
  Command Changes 198
  duplicate-subscriber-requested-v6-address 198
  Performance Indicator Changes 199
  show configuration 199
  show configuration verbose 199
  show pgw-service name <pgw-service-name> 199
  CSCuw86628 - UBR suppression should not be applied to Modify Bearer command scenarios 200
  Feature Changes 200
  UBR Suppression Should Not Be Applied to Modify Bearer Command Scenarios 200

P-GW Enhancements for 18.4 200
  CSCut53373, CSCuu63751, CSCuu64308 - PGW initiates UBR while no QoS change 201
  Feature Changes 201
  UBR Suppression Feature 201
  Command Changes 201
  suppress-ubr no-bitrate-change 201
  Performance Indicator Changes 202
  show configuration 202
  show configuration verbose 202
  show pgw-service name <pgw-service-name> 202

P-GW Enhancements for 18.3 202
  CSCuv03271 - s2b-ho-no-context details not shown in show egtp-service all 203
  Feature Changes 203
  Correction to show egtp-service all Command Output 203
  Performance Indicator Changes 203
  show egtp-service all 203

P-GW Enhancements for 18.2 204
  CSCum59119, CSCus32111, CSCus32116 - SM support for non standard QCI 204
  Feature Changes 204
  Non-standard QCI Support 204
Command Changes 205

operator-defined-qci 205

Performance Indicator Changes 206

APN Schema 206

show apn statistics 207

show qci-qos-mapping table all 207

CSCum70938 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure 207

Feature Changes 207

Graceful Cleanup During Audit Failure 207

Command Changes 208

require graceful-cleanup-during-audit-failure 208

Performance Indicator Changes 209

show srp checkpoint statistics 209

show session disconnect-reasons 209

CSCuo72738 - VoLTE-ICSR:GTPC Flow preinstallation 209

Feature Changes 209

GTP-C Flow Pre-installation with ICSR 209

CSCup49111, CSCuq45024, CSCup89018 - PGW/GGSN/SAEGW RLF enhancements 209

Feature Changes 209

Bypass Rate Limit Function Enhancement 209

Command Changes 210

gtpc overload-protection egress 210

throttling-override-policy 211

egress bypass-rlf 211

Performance Indicator Changes 212

show configuration config 212

show configuration verbose 212

show ggsn-service { all | name <name>} 213

show pgw-service { all | name <name>} 213

show throttling-override-policy { all | name <name>} 213

show rlf-context-statistics sessmgr gtpc-context-name ingress 214

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress 214

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress summary 214
show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress verbose 214
show rlf-memcache-statistics sessmgr 214
show rlf-memcache-statistics sessmgr instance 1 214
clear rlf-context-statistics sessmgr gtpc-context-name ingress 214
CSCuq00838 - SM Support for P-GW/GGSN needs P-CSCF failure detection support 215
Feature Changes 215
P-CSCF Failure Detection Support Enhancement 215
Command Changes 215
pcscf-restoration 215
Performance Indicator Changes 215
show pgw-service name 215
show pgw-service all 216
CSCuq30097 - packets shown as dropped at sessmgr with ipv6 ecs readdressing 216
Feature Changes 216
Packet Drop at Session Manager 216
CSCur80218 - SAEGW - support for S2b standard based call flow 216
Feature Changes 216
GTP-based S2b Interface Support on the SAEGW 216
CSCur85237 - SFR: Licensing Bulkstats enhancements (Subscriber vs Sessions count) 217
Feature Changes 217
Licensing Bulkstats Enhancements 217
Performance Indicator Changes 217
APN Schema 217
show apn statistics name <apn_name> | all 217
CSCus74504 - Appropriate disconnect reason should be displayed 218
Feature Changes 218
New Disconnect Reason 'Reject-ho-old_tun-path-failure' Added 218
CSCus96089 - GTPC stats on ICSR setup 219
Feature Changes 219
GTP-C Statistics on ICSR Setup 219
CSCut22844 - SegFault: libc.so.6/__strlen_sse2_bsf() 219
Feature Changes 219
Behavior Change in APN Removal 219
Command Changes 219
CSCut76641 - GTPC ingress throttling should have strict rate limiting

Feature Changes

GTPC Ingress Throttling Feature Enhancement

Performance Indicator Changes

GTPC Schema
EGTPC Schema

show demux-mgr statistics egtpinmgr instance <>
show gtpe statistics

CSCut82166 - P-cscf restoration disconnect reason and disconnect stats

Feature Changes

P-CSCF Failure Detection Support Disconnect Reason and Disconnect Statistics

Performance Indicator Changes

P-GW Schema

show pgw-service statistics all
show session disconnect reason verbose
show subscribers pgw-only full all

CSCuu56803 - [SysTest] vpnctrl over mem usage during longevity

Feature Changes

IPMS Configuration Update During VPN-ctrl Start

CSCuu58335 - Unable to retrieve bulkstats server information

Feature Changes

Bulkstat Process Retries for Connection Attempt After Transfer Interval

P-GW Enhancements for 18.1

CSCuh44477, CSCuq65471 - Dynamically allocate protocol_(username/password) in sessmgr_callline_t

Feature Changes

Removal of ‘Protocol Username’ from CLI Output

Command Changes

show subscribers [ pgw-only | sgw-only | saegw-only | ipsg-only | ggsn-only ] full all

CSCul17189 - [PGW] Enhance Clear subs CLI to generate DBReq to control the pace

Feature Changes

Enhanced Clear Subscribers Command for VoLTE
Command Changes 224

clear subscriber 224

CSCum70938, CSCup77221, CSCur78635 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure 225

Feature Changes 225

Graceful Cleanup During Audit Failure 225

Command Changes 225

require graceful-cleanup-during-audit-failure 225

Performance Indicator Changes 226

show srp checkpoint statistics 226

show session disconnect-reasons 226

CSCuo53205, CSCum49101, CSCup41814, CSCup58702, CSCup86021 - Rel12 New Cause-code IE 226

Feature Changes 226

Support for RAN/NAS Cause Standard IE 226

CSCuo61687 - PGW Bearer Duration KPI's 227

Feature Changes 227

Bearer Duration Statistics Expanded 227

Command Changes 227

bearer-duration-stats 227

show session duration 227

Performance Indicator Changes 228

apn-qci-duration Schema 228

show apn name apn_name 228

show session duration apn apn_name qci { all |1|2|3|4|5|6|7|8|9 } + 228

CSCuo61706 - Configurable Guard Timer on Create Session Request Processing 229

Feature Changes 229

Configurable Guard Timer on Create Session Request Processing 229

Command Changes 230

setup-timeout 230

Performance Indicator Changes 230

P-GW Schema 230

SAEGW Schema 230

show pgw-service statistics all 230

show saegw-service statistics all 230
CSCuo97254, CSCuq44967, CSCuq44973 - R12 Overload Support  231
Feature Changes  231
R12 GTP-C Load and Overload Support on the P-GW  231
Operation  231
Command Changes  232
gtpc-load-control-profile  232
inclusion-frequency  232
weightage  233
gtpc-overload-control-profile  233
inclusion-frequency  233
throttling-behavior  234
tolerance  234
validity-period  235
weightage  235
associate  236
associate  236
associate  236
Performance Indicator Changes  237
EGTPC Schema  237
show egtpc statistics  237
show gtpc-load-control-profile full all  238
show gtpc-overload-control-profile full all  238
show pgw-service all  239
show sgw-service all  239
CSCup17404, CSCur88824 - ICSR IDLE Secs checkpointing optimization  239
Feature Changes  239
Stop Sending Idlesecs Micro-checkpoint  239
Command Changes  240
timeout idle  240
Performance Indicator Changes  240
show apn  240
show configuration  240
show configuration verbose  240
CSCup29785, CSCup56949, CSCus96432 - Show command enhancements  241
Feature Changes  241
Show Command Enhancements 241
Command Changes 241
show session counters historical 241
Performance Indicator Changes 242
show session counters historical 242
show session summary 242
CSCUp32111 - Configurable behavior on PDN type IPv4v6 with DAF set to False 243
Feature Changes 243
Configurable Behavior on PDN Type IPv4v6 243
Command Changes 243
daf-pdp-type 243
Performance Indicator Changes 244
P-GW Schema 244
SAEGW Schema 244
show apn { <name> | all } 244
show configuration apn 244
show pgw-service statistics all 245
show saegw-service statistics all function pgw 245
CSCUp44635 - SM support for CSCul22770, SFR - PSP algorithm modification 245
Feature Changes 245
Modification in Bandwidth Policy Selection During Call Setup 245
CSCup71684, CSCup98374, CSCup71747 - PGW RTT Support for GTP procedures 245
Feature Changes 245
RTT Support for P-GW 245
Command Changes 246
reporting-action event-record 246
show event-record 247
Performance Indicator Changes 247
System Schema 247
show event-record statistics pgw 248
CSCup88929 - PGW/GGSN/SAEGW Abnormal bearer termination info in CDR 249
Feature Changes 249
Abnormal Bearer Termination Information in CDR 249
Performance Indicator Changes 249
show session disconnect-reasons 249
CSCup89677, CSCup73076, CSCup92630 - PGW/GGSN/SAEGW ULI enhancements 250
Feature Changes 250
P-GW, GGSN, SAEGW ULI Enhancements 250

CSCuq11994, CSCup98379, CSCus94777 - PGW/GGSN/SAEGW LTE/WiFi GTP S2b Make-Before-Break HO Compliance 250
Feature Changes 250
DBR is delayed until HO completion for Inter-rat HO from S2a/S2b to LTE 250

CSCuq13125, CSCuq00838 - SM Support for P-GW/GGSN needs P-CSCF failure detection support 251
Feature Changes 251
P-CSCF Failure Detection Support 251

CSCuq30097 - packets shown as dropped at sessmgr with ipv6 ecs readdressing 252
Feature Changes 252
Packet Drop at Session Manager 252

CSCuq44987 - License for WiFi integration support in 18.0. 252
Feature Changes 252
License for WiFi Integration Support in Release 18.0. 252

CSCuq51507 - License enforcement for GTP based S2a and S2b in 18.0. 252
Feature Changes 252
License Enforcement for GTP based S2a and S2b in Release 18.0 252
Command Changes 253
interface-pgw-ingress 253
Performance Indicator Changes 253
show egtp-service all 253

CSCuq74490 - PGW not rejecting session when HI = 1 & no Context 254
Feature Changes 254
P-GW Rejecting WLAN request if there is No Valid S2b Session for that PDN and UE indicates Handover 254
Command Changes 255
gtpc 255

CSCur51701 - Disconnect Reason Not Updated correctly For Saegw-collapsed call 255
Feature Changes 255
P-GW and SAEGW Session Disconnect Reason Not Updated Correctly for Multi Bearer Ca 255

CSCur65231 - Different disconnect reason is required for PCRF unreachable case 256
Feature Changes

Value Change for Diagnostics AVP in Rf Record

CSCu06045 - gtpu-service echo-interval 'default' keyword should disable echo

Feature Changes

Change to 'default gtpu-service echo-interval' Command

Command Changes

default echo-interval

CSCu30437 - Std QCI(Non-GBR) wrongly incrmtd whn traffic dropd whn traffic dropd for GBR bearer in OCP

Feature Changes

Downlink Dropped Packets Shown for Proper Bearer

CSCu74784 - No QOS-Change is sent to Gy on receiving now qos from Gx on 4G to 3G

Feature Changes

Bearer Control Mode Treated as Mixed Mode if CLI is Configured on APN

CSCu82761 - Charging Id in GTPv2 S2b/S2a

Feature Changes

Charging ID sent in Create-Session-Response and Create-Bearer-Request

CSCu10653 - 2 rules with different QCI/ARP are installed on single bearer: SM support

Feature Changes

Change in Call Flow Related to Update PDP Request from SGSN

CSCu15652 - change-condition issue in Rf record when OCS/ Gy is down during CCR

Feature Changes

Different Session Disconnect Reason Due to Unreachability of Gy

Performance Indicator Changes

show session disconnect-reasons

CSCu15657 - Assertion failure while handling MBReq

Feature Changes

New Disconnect Reason

Performance Indicator Changes

show session disconnect-reasons

CSCu31458 - PGW Stats to count discarded DHCPv4 DISCOVER due to AAA conflicts

Feature Changes

P-GW Statistics Added to Count Discarded DHCPv4 DISCOVER Due to AAA

Conflicts

Performance Indicator Changes

show session disconnect-reasons
System Schema 261
show dhcp counters all 261
show dhcp statistics dhcp-service dhcp service name 261
CSCut38233 - egtp modify-bearer-cmd-negotiate-qos not enforcing the authorized QoS 261

Feature Changes 261

Enforcement of Authorized QoS 261
CSCut38800 - PGW sends CCR-U with RESOURCES_LIMITATION for VoLTE calls in 17.1 build. 262

Feature Changes 262

Handling of Collision of GnGp (LTE to GnGP GGSN) Handoff with Ongoing CBReq or UBReq Transaction 262
CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure 262

Feature Changes 262

Control of GTP Cause Being Sent in Create Session Response 262
Command Changes 263
map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail 263

CHAPTER 15

PSF Changes in Release 18 265

PSF Enhancements for 18.1 265
CSCuh13901 - SFW counting license enforcement 265

Feature Changes 265

Stateful Firewall License Enforcement 265
Command Changes 266
firewall license 266
Performance Indicator Changes 266
show resources session 266
show task info 266
CSCuo78207 - [NAT]Stats to display MAX port usage of subscribers 267

Feature Changes 267

Port Utilization by Subscribers 267
Performance Indicator Changes 267
show active-charging firewall statistics verbose 267
show active-charging nat statistics 268
SAEGW Changes in Release 18 269

SAEGW Enhancements for 18.5 269

DHCP Options 1, 3, 6, 28, 43, 60 and 61 Relayed Between UE and External DHCP Server 270

Feature Changes 270

DHCP Deferred IPv4 Enhancements 270

Performance Indicator Changes 271

show dhcp full all 271

Correction for Missing QoS/AMBR AVP in CCA to PCEF 271

Subscriber Session Preserved in Case of P-GW Failing to Renew IP Address 272

SAEGW Enhancements for 18.4 272

SAEGW Enhancements for 18.3 272

SAEGW Enhancements for 18.2 272

CSCup18703 - 18.2 - Collision counter support in GTP layer 273

Feature Changes 273

Collision Counter Support in the GTP Layer 273

Performance Indicator Changes 273

show egtp statistics verbose 273

CSCur61470, CSCur80218, CSCus87350 - S2B Support on SAE-GW 274

Feature Changes 274

GTP-based S2b Interface Support on the SAEGW in StarOS Version 18.2 274

Command Changes 275

interface-type interface-pgw-ingress 275

Performance Indicator Changes 275

SAEGW Schema 275

show saegw-service statistics all function pgw 275

show subscribers saegw-only full all 276

CSCuu17820 - S2B: GW is sending incorrect Event Trigger in case of Wifi to LTE HO 277

Feature Changes 277

S2b Event Trigger Corrected 277

CSCuu31324 - Idle subscribers not being cleared from SPGW 277

Feature Changes 277

Idle Subscribers Cleared Properly 277

CSCuu37427, CSCut14324 - Assertion failure

egtpc_handle_create_sess_req_msg_at_sgw_ingress 278
Feature Changes 278
  Parallel Create Session Requests Processed Correctly 278
SAEGW Enhancements for 18.1 279
  CSCuh13685, CSCuo97254 - Overload controls (congestion prevention by singalling) 279
Feature Changes 279
  R12 Load and Overload Support 279
CSCur61470 - S2B Support on SAE-GW 279
Feature Changes 279
  GTP-based S2b Interface Support on the SAEGW 279
CSCut07427 - [SAEGW-stats] display changes needed for saegw-service stat 279
Feature Changes 279
  Change in Display for show saegw-service statistics all function pgw verbose 279
Performance Indicator Changes 280
  show saegw-service statistics all function pgw verbose 280
CSCut09582 - [18.0]:gy iface is not shown in func-pgw in template for saegw NE 280
Feature Changes 280
  Support for Gy Interface in Session Tracing on the SAEGW 280
Command Changes 280
  session tracerandom 280
  template-session-trace 281
Performance Indicator Changes 281
  show session trace template network-element saegw all 281
CSCut28557 - Assertion failure while handling MBReq 281
Feature Changes 281
  New Disconnect Reason disconnect-irat-fail-hi-missing(611) 281
Performance Indicator Changes 281
  show session disconnect-reasons 281

CHAPTER 17

SaMOG Changes in Release 18 283
SaMOG Enhancements for 18.5 283
  CSCuw17212 - [SaMOG] - Webauth Optimization for IPv4 subscriber session 284
Feature Changes 284
  Optimized SaMOG Web Authorization 284
Command Changes 285
  newcall 285
Performance Indicator Changes  285
  show samog-service statistics  285
  show subscriber samog-only full  286

SaMOG Enhancements for 18.4  286
  CSCux31916 - SaMOG to include NAS-ID in radius-disconnect towards WLAN Access  287

  Feature Changes  287
    NAS-Identifier Support for SWw Interface  287

  Performance Indicator Changes  287
    show subscribers samog-only full  287

  CSCuv92889 - [SaMOG] - AAA-Failure-Indication AVP support needed by SaMOG  287

  CSCuv74173 - [SaMOG] - IPv6 Transport Support for S2a GTPv2 Interface  288

  Feature Changes  288
    IPv6 Transport Support Using the S2a GTPv2 Interface  288

  Performance Indicator Changes  288
    SaMOG Schema  288
    show samog-service statistics  289
    show subscribers samog-only full  291

  CSCuv74182 - [SaMOG] - IPv6 Transport Interface support for EoGRE Access-Type  291

  Feature Changes  291
    IPv6 Transport Support Using EoGRE Access Type  291

  Command Changes  291
    bind  291

  Performance Indicator Changes  292
    SaMOG Schema  292
    show cgw-service all  293
    show subscribers samog-only full  293
    show samog-service all  293
    show samog-service statistics  293

  CSCuv74193 - [SaMOG] - Captive Portal Integration with IPv6 Transport for end-user  294

  Feature Changes  294
    SaMOG Web Authorization IPv6 Support for UE (Pre-Authentication Phase)  294

  Command Changes  295
    ipv6 address  295

  Performance Indicator Changes  295
    show apn-profile full name profile_name  295
CSCuw31457 - [SAMOG] Provide DHCP lease time configuration of WebAuth pre-auth calls 295

Feature Changes 295

SaMOG Web Authorization DHCP Lease Time Configuration 295

Command Changes 296
dhcp lease 296

Performance Indicator Changes 296

show apn-profile full name profile_name 296

CSCuw54703 - [SAMOG] Trigger unsolicited RA to deprecate and/or advertise IPv6 prefix 296

Feature Changes 296

SaMOG Unsolicited Router Advertisement Support 296

Virtual MAC Validation 297

Command Changes 297
ipv6 unsolicited-router-advt 297
virtual-mac 298

Performance Indicator Changes 298

show samog-service statistics 298

SaMOG Enhancements for 18.2 298

CSCus51250 - [SaMOG] - IPv6 Support for Subscriber Sessions 299

Feature Changes 299

IPv6/Dual-Stack Support for Subscriber User Equipment (UE) 299

Command Changes 299
associate 299
dns 300

Performance Indicator Changes 300

SaMOG Schema 300

show samog-service all 300

show subscriber samog-only full 300

show subscriber full 301

show samog-service statistics 301

CSCut22121 - [SaMOG] - Qualification of SaMOG on VPC-DI platform 303

Feature Changes 303
SaMOG vPC-DI Qualification 303

SaMOG Enhancements for 18.0 303
CSCuo87191 - [SAMOG]: UE and Access Point Identity Support 304
  Feature Changes 304
    User Equipment (UE) Identity Support 304
    Access Point (AP) Location Support 304
  Command Changes 305
    samog-gtpv1 305
    samog-s2a-gtpv2 305
  Performance Indicator Changes 305
    show call-control-profile full name <profile_name> 305
    show subscriber samog-only <full> 306
CSCup63891 - [SaMOG] - Delay sending Access-Accept till to complete s2a/Gn
  Procedures 306
  Feature Changes 306
    TWAP Triggered PDN 306
  Performance Indicator Changes 306
    show subscriber samog-only <full> 306
CSCup60901, CSCup60896, CSCuo83066 - Out of Band DHCP Support in SaMOG 307
  Feature Changes 307
    SaMOG Wireless Acess Gateway (WAG) 307
    License Requirements 307
  Command Changes 308
    associate 308
    ue-address 308
    access-type 308
    radius 309
  Performance Indicator Changes 309
    SaMOG Schema 309
    show mrm-e-service statistics 309
    show samog-service statistics 309
    show samog-service { all | name <name>} 310
    show subscriber samog-only full 310
    show subscriber full 310
    show twan-profile all 310
CSCup60958 - Local Breakout Basic 310
  Feature Changes 310
show apn-profile full { all | name <profile_name>}  

CSCup61006, CSCur35158 - EAP authentication method agnostic SAMOG service  

Feature Changes  

EAP Agnostic Authentication  

Command Changes  

aaa  

Performance Indicator Changes  

SaMOG Schema  

show mrme-service all  

show samog-service statistics  

show subscribers samog-only full

C H A P T E R 1 8

SGSN Changes in Release 18  

SGSN Enhancements for 18.5  

CSCur57085 - Inter-SRNS SGSN to send ULI to GGSN  

Feature Changes  

ULI Containing Valid SAI with PLMN, LAC and SAC  

CSCux33388, CSCur41900 - CLI Control for Target Access Restriction  

Feature Changes  

Target Access Restriction  

Command Changes for the MME  

access-restriction-data  

Command Changes for the SGSN  

access-restriction-data  

Performance Indicator Changes  

show call-control-profile  

show configuration verbose  

SGSN Enhancements for 18.3  

CSCuu74352 - No rab release during upc/dpc collision  

Feature Changes  

Send Activate PDP Reject Instead of De-activate PDP Request  

SGSN Enhancements for 18.1  

CSCtq92045 - Need Linkmgr CPU added to bulkstats for SGSN cpety monitoring  

Feature Changes  

Additional Card-level Bulk Statistics Added
Performance Indicator Changes  329
Card Schema  329
CSCtx04694, CSCum82005 - [S4-SGSN] CLI required for controlling GPRS/EPC info flags in HSS/HLR  330
Feature Changes  330
Operator Control for GPRS/EPS Subscription Data Requests in UGL/ULR Messages to the HLR/HSS.  330
Command Changes  331
map  331
hss  331
CSTy22738 - lmgr stats classification for connection-less ranap msg  332
Feature Changes  332
Link Manager Parser Statistics Updated with New Statistics  332
Performance Indicator Changes  332
show linkmgr all parser statistics all  332
CSTui82344, CSTcum50067, CSCur94662, CSCur94708, CSCur40028, CSCur33100 - SGSN to select the co-located MME in case of PS-HO from SGSN to MME  332
Feature Changes  332
SGSN & MME Combo Optimization  332
Command Changes  333
sgsn-mme  333
hss  333
Performance Indicator Changes  334
show lte-policy sgsn-mme summary  334
show demux-mgr statistics imsimgr all sgsn  334
show subscribers sgsn-only summary  334
show subscribers gprs-only summary  334
show subscribers sgsn-only full all  334
show subscribers gprs-only full all  335
show session subsystem facility aaamgr instance <instance>  335
show hss-peer-service statistics all  335
show mme-service statistics handover  336
CSTcum50020, CSTcur73892, CSTcur30903 - Scale IMSIMGR  337
Feature Changes  337
SGSN Support for IMSI Manager Scaling  337
Command Changes 337
  task facility imsimgr 337
  sgsn imsimgr 338
Performance Indicator Changes 338
  show linkmgr all 338
  show linkmgr instance parser statistics all 338
  show gbmgr instance parser statistics all 338
  show demuxmgr statistics imsimgr verbose 339
  show demux-mgr statistics sgtpcmgr instance <id> 339
  show session subsystem facility mmemgr instance <id> 339
  show subscribers mme-only full all/ show mme-service session full all 339
  show mme-service db record call-id <id> 339

CSCup86883, CSCuq24364, CSCuq55842 - VPC-DI Serving GPRS Support Node 340

Feature Changes 340
  VPC-DI platform Support for SGSN 340

CSCuq06573 - Removal of TPO Code 340

Feature Changes 340
  Support for TPO Feature Withdrawn 340

Performance Indicator Changes 341
  show sgtpc statistics 341
  show sgtpc statistics sgtp-service <service_name> 341
  show sgtpu statistics sgtp-service <service_name> 341

CSCur33100 - [18.0] SGSN/MME Combo - F PTMSI Attach support is required 341

Feature Changes 341
  Support to Copy Subscription Information From MME during FPTMSI Attach Procedure 341

CSCur40028 - Subs-info to be shared during attach,srn scenarios in coloc sgsn/mme 342

Feature Changes 342
  Support to Share Subscription Information during Attach and SRNS scenarios in co-located SGSN/MME. 342

Performance Indicator Changes 342
  show demux-mgr statistics imsimgr all sgsn 342
  show subscribers sgsn-only summary 342
  show subscribers gprs-only summary 342
  show subscribers sgsn-only full all 343
CHAPTER 19

S-GW Changes in Release 18 347

S-GW Enhancements for 18.5 347

Private Extension IE in DDN Message Sent Only if S-GW Paging Feature is Enabled 348

S-GW Enhancements for 18.4 348

S-GW Enhancements for 18.3 348

S-GW Enhancements for 18.2 348

CSCuq37460 - Min ARP calculation at SessMgr does not consider individual parameters 349

Feature Changes 349

ARP Value Calculation Change 349

CSCut49838 - Statistics error displayed for sgw or pgw stats associated in saegw 349

Feature Changes 349

Error Message Changed 349

CSCuu37427, CSCu14324 - Assertion failure

egtpc_handle_create_sess_req_msg_at_sgw_heartbeat 350

Feature Changes 350

Parallel Create Session Requests Processed Correctly 350

CSCuu50651 - SGW: MBR from S4SGSN with HI not fwded to PGW for WiFi to UTRAN/GERAN HO 351

Feature Changes 351

S-GW Support for Non-3GPP (WiFi) to UTRAN/GERAN Handover 351

CSCuu52039 - SGW is rejecting UBR in case of wifi to LTE HO 351

Feature Changes 351

Change in Action Taken During MBReq-UBReq Collision at S-GW Egress Interface 351

S-GW Enhancements for 18.1 351

CSCu17192 - [SGW] Enhance Clear subs CLI to generate DBReq to control the pace 352

Feature Changes 352

Enhanced Clear Subscribers Command for VoLTE 352
Command Changes 353

clear subscriber 353

CSCup56736 - SGW Bearer Duration KPIs 353

Feature Changes 353

Bearer Duration KPIs 353

Performance Indicator Changes 353

System Schema 353

show session duration qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | non-std } + 358

CSCup82065 - Abnormal bearer termination info in CDR 359

Feature Changes 359

Abnormal Bearer Termination Cause in CDR 359

Performance Indicator Changes 360

System Schema 360

show session disconnect-reasons 360

CSCup82477 - [SGW]: ICSR IDLE Secs checkpointing optimization 361

Feature Changes 361

ICSR Micro Checkpoint Optimization for Idle Seconds 361

Command Changes 361

timeout-idle 361

Performance Indicator Changes 361

show sgw-service name 361

CSCup82660 - ULI enhancements 362

Feature Changes 362

ULI Enhancements 362

CSCup86002, CSCup33431, CSCuq44967, CSCuq44973 - R12 GTP-C load and overload control Support on SGW 362

Feature Changes 362

R12 GTP-C Load and Overload Support on the S-GW 362

Operation 363

Command Changes 363

gtpc-load-control-profile 363

inclusion-frequency 364

weightage 364

gtpc-overload-control-profile 365

inclusion-frequency 365
throttling-behavior 365
tolerance 366
validity-period 366
weightage 367
associate 367
associate 368
associate 368
Performance Indicator Changes 368

EGTPC Schema 368
show egtpc statistics 369
show gtpc-load-control-profile full all 369
show gtpc-overload-control-profile full all 370
show pgw-service all 370
show sgw-service all 371

CSCup86011 - VoLTE-ICSR-SR: IMS Sessions hung after SR failure 371

Feature Changes 371
VoLTE-ICSR-SR: Resolving IMS Sessions Hung after SR Failure 371

Command Changes 371
require graceful-cleanup-during-audit-failure 371

Performance Indicator Changes 372
show session disconnect-reasons 372
show srp checkpoint statistics 372

CSCup86021, CSCum49101 - Rel12 New Cause-code IE 372

Feature Changes 372
3GPP Release 12 Cause-Code IE Support 372

CSCuq03551 - [SGW] Show command enhancements 373

Feature Changes 373
show session Counter Enhancements 373

Performance Indicator Changes 373
show session counters historical all 3g 373
show session counters historical all 4g 373
show session summary 374
show session counters historical all 3g 374
show session counters historical all 4g 375
CSCuq11129 - SGW SM Support for P-GW/GGSN needs P-CSCF failure detection support 375

Feature Changes 375
P-CSCF Failure Detection Support 375

CSCur47721 - [SGW]: Integration test support for abnormal bearer info feature 375

Feature Changes 375

Behavior Change Resulting from Fix for CSCur47721 375

Performance Indicator Changes 376
show session disconnect-reasons 376

CSCur98632 - show egtpc peer need to display immediate and remote peer separately 376

Feature Changes 376
Immediate and Remote Peer Listed Separately in show egtpc peer Command 376

Performance Indicator Changes 376
show egtpc peer 376

CHAPTER 20
SNMP MIB Changes in Release 18 377

SNMP MIB Object Changes for 18.5 378
New SNMP MIB Objects 378
Modified SNMP MIB Objects 378
Deprecated SNMP MIB Alarms 378

SNMP MIB Alarm Changes as of 18.5 378
New SNMP MIB Alarms 378
Modified SNMP MIB Alarms 379
Deprecated SNMP MIB Alarms 379

SNMP MIB Conformance Changes for 18.5 379
New SNMP MIB Conformance 379
Modified SNMP MIB Conformance 379
Deprecated SNMP MIB Conformance 379

SNMP MIB Object Changes for 18.4 380
New SNMP MIB Objects 380
Modified SNMP MIB Objects 380
Deprecated SNMP MIB Objects 380

SNMP MIB Alarm Changes as of 18.4 380
New SNMP MIB Alarms 380
Modified SNMP MIB Alarms 381
<table>
<thead>
<tr>
<th>Deprecated SNMP MIB Alarms</th>
<th>381</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP MIB Conformance Changes for 18.4</td>
<td>381</td>
</tr>
<tr>
<td>New SNMP MIB Conformance</td>
<td>381</td>
</tr>
<tr>
<td>Modified SNMP MIB Conformance</td>
<td>381</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Conformance</td>
<td>381</td>
</tr>
<tr>
<td>SNMP MIB Object Changes for 18.3</td>
<td>382</td>
</tr>
<tr>
<td>New SNMP MIB Objects</td>
<td>382</td>
</tr>
<tr>
<td>Modified SNMP MIB Objects</td>
<td>382</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Objects</td>
<td>382</td>
</tr>
<tr>
<td>SNMP MIB Alarm Changes as of 18.3</td>
<td>382</td>
</tr>
<tr>
<td>New SNMP MIB Alarms</td>
<td>382</td>
</tr>
<tr>
<td>Modified SNMP MIB Alarms</td>
<td>383</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Alarms</td>
<td>383</td>
</tr>
<tr>
<td>SNMP MIB Conformance Changes for 18.3</td>
<td>383</td>
</tr>
<tr>
<td>New SNMP MIB Conformance</td>
<td>383</td>
</tr>
<tr>
<td>Modified SNMP MIB Conformance</td>
<td>383</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Conformance</td>
<td>383</td>
</tr>
<tr>
<td>SNMP MIB Object Changes for 18.2</td>
<td>384</td>
</tr>
<tr>
<td>New SNMP MIB Objects</td>
<td>384</td>
</tr>
<tr>
<td>Modified SNMP MIB Objects</td>
<td>384</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Objects</td>
<td>384</td>
</tr>
<tr>
<td>SNMP MIB Alarm Changes as of 18.2</td>
<td>384</td>
</tr>
<tr>
<td>New SNMP MIB Alarms</td>
<td>384</td>
</tr>
<tr>
<td>Modified SNMP MIB Alarms</td>
<td>385</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Alarms</td>
<td>385</td>
</tr>
<tr>
<td>SNMP MIB Conformance Changes for 18.2</td>
<td>385</td>
</tr>
<tr>
<td>New SNMP MIB Conformance</td>
<td>385</td>
</tr>
<tr>
<td>Modified SNMP MIB Conformance</td>
<td>385</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Conformance</td>
<td>385</td>
</tr>
<tr>
<td>SNMP MIB Object Changes for 18.1</td>
<td>386</td>
</tr>
<tr>
<td>New SNMP MIB Objects</td>
<td>386</td>
</tr>
<tr>
<td>Modified SNMP MIB Objects</td>
<td>386</td>
</tr>
<tr>
<td>Deprecated SNMP MIB Objects</td>
<td>386</td>
</tr>
<tr>
<td>SNMP MIB Alarm Changes as of 18.1</td>
<td>386</td>
</tr>
<tr>
<td>New SNMP MIB Alarms</td>
<td>386</td>
</tr>
</tbody>
</table>
Modified SNMP MIB Alarms 387
Deprecated SNMP MIB Alarms 387
SNMP MIB Conformance Changes for 18.1 387
New SNMP MIB Conformance 387
Modified SNMP MIB Conformance 387
Deprecated SNMP MIB Conformance 387
SNMP MIB Object Changes for 18.0 388
New SNMP MIB Objects 388
Modified SNMP MIB Objects 388
Deprecated SNMP MIB Objects 388
SNMP MIB Alarm Changes as of 18.0 388
New SNMP MIB Alarms 389
Modified SNMP MIB Alarms 389
Deprecated SNMP MIB Alarms 389
SNMP MIB Conformance Changes for 18.0 389
New SNMP MIB Conformance 389
Modified SNMP MIB Conformance 390
Deprecated SNMP MIB Conformance 390
SNMP Command Changes for 18.0 390
CSCur13393 - Cisco ASR5000 SAE-GW High CPU Utilisation Vulnerability 390
Command Changes 390
snmp runtime-debug 390

CHAPTER 21

System Changes in Release 18 393

System and Platform Enhancements for Release 18.5 393
CSCuv45511 - When an invalid license is applied, CLI should throw error 393
Feature Changes 394
Invalid License Automatically Rejected 394
CSCuw44496 - Explicit route limit enhancement 394
Feature Changes 394
System and Platform Enhancements for Release 18.4 394
CSCut24782 - RAID support for new FSC with single 400GB SSD 394
Feature Changes 395
New Version of FSC with Single 400GB SSD 395
Performance Indicator Changes 395
show card table 395
show hd raid verbose 395

System and Platform Enhancements for Release 18.3 395
CSCuv23480 - RAID: CLI options for FSC cards must show only drives that are present 395

Feature Changes 396
Only FSC Slots with Available HD Arrays Can Be Selected 396
Command Changes 396
hd-raid select 396

System and Platform Enhancements for Release 18.2 396
CSCuo77496 - Upgrade version of OpenSSH used in StarOS 396

Feature Changes 396
Upgrade Remote SSH Service 396
CSCup47534 - DPC2: GTPU manager, memory + session reconciliation optimization 397

Feature Changes 397
Potential Impact on Unplanned Card Migration 397
CSCuq86655 - TACACS+ commands not being logged or some commands missing 397

Feature Changes 397
StarOS Authorizations for TACACS+ Users 397
Command Changes 397
priv-lvl 397
user-id 398

Performance Indicator Changes 399
show tacacs priv-lvl 399

CSCus11708 - L2TP support with Demux on MIO 399

Feature Changes 399
L2TP Support with Demux on MIO (ASR 5500) 399
CSCut57399 - Output pkts stats post recovery/switchover 399

Feature Changes 399
Adjusted Packet Counts for Collapsed Calls 399
CSCuu14795 - [MARS] uDPC2 license not being enforced 399

Feature Changes 400
Add Support for UDPC2 on ASR 5500 Chassis 400
CSCuu20436 - Increase the number of configurable tacacs server priorities to 4 400

Feature Changes 400
Increase Number of TACACS+ Server Priorities

Command Changes

tserver priority

CSCuu58335 - Unable to retrieve bulkstats server information

Feature Changes

Retry Bulkstat Connection at Configured Transfer Interval

System and Platform Enhancements for Release 18.1

CSCum24783 - Live Migrate Support

Feature Changes

Traffic Handling During Planned Card Migration

CSCuo82292 - [ICSR Perf] srp chkpnt stats need to include counters for all checkpoints

Feature Changes

SRP Checkpoint Counters

System and Platform Enhancements for Release 18.0

CSCuj74022 - Support ICSR upgrade/downgrade across N-2 builds

Feature Changes

ICSR Support for Upgrade and Downgrade Across Two StarOS Releases

CSCum70938 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure

Feature Changes

Graceful Cleanup of ICSR After Audit of Failed Calls

Command Changes

require gracefull-cleanup-during-audit-failure

Performance Indicator Changes

System Schema

show srp checkpoint statistics

show session disconnect-reasons

CSCum84097 - Enhance messenger vector call internal APIs

Feature Changes

Replace Existing Message Vector API

CSCum92365 - ICSR:SRP link DSCP marking

Feature Changes

DSCP Marking of SRP Messages

Command Changes

dscp-marking

Performance Indicator Changes
show srp info 406

CSCun88539 - [ePDG] Memory optimization for ePDG sessmgr component 406

Feature Changes 407

Memory Optimization for ePDG Sessmgr 407

CSCuo72680 - ICSR IDLE Stats checkpointing issue 407

Feature Changes 407

Stop Sending Idlesecs Micro-checkpoint 407

CSCuo72783 - VoLTE-ICSR: Starting the audit in pending active state 407

Feature Changes 407

Optimization of Switchover Control Outage Time 407

Command Changes 408

switchover control-outage-optimization 408

CSCuo91183 - Finish config versioning support for services 408

Feature Changes 408

Service Reconciliation Optimization for S-GW and P-GW Services 408

CSCup29785 - Show command enhancements 408

Feature Changes 409

Enhancements to show session Commands and Bulkstats 409

Performance Indicator Changes 409

System Schema 409

show session counters historical 410

show session summary 410

CSCup30816 - ICSR Non VoLTE Outage Improvement 412

Feature Changes 412

Allow Non-VoLTE Traffic During ICSR Switchover 412

Command Changes 413

switchover allow-all-data-traffic 413

switchover allow-volte-data-traffic 413

CSCup47085 - Time slice lport utilization stats collection 413

Feature Changes 413

Improved Collection of Logical Port Statistics on ASR 5500 413

CSCup47715 - Pilot Packet Format and Trigger Update 414

Feature Changes 414

Support for Pilot Packet Format and Trigger 414

Command Changes 414
pilot-packet 414

Performance Indicator Changes 415

APN Schema 415

System Schema 415

show apn statistics name 415

show pilot-packet statistics all 415

show session subsystem facility sessmgr all 415

CSCup56736 - SGW Bearer Duration KPIs 415

Feature Changes 416

Session Duration Statistics by QCI 416

Performance Indicator Changes 416

System Schema 416

show session duration 417

CSCup66766 - MME support on QvPC-DI 417

Feature Changes 417

MMEmgr Linear Scalability 417

Command Changes 418

mmemgr-average-cpu-utilization 418

Performance Indicator Changes 418

congestion-control configuration 418

CSCup68867 - HeNBGW support on ASR5500 419

Feature Changes 419

Support for HeNB-GW on ASR 5500 419

CSCup71713 - PGW RTT Support for Diameter procedures 419

Feature Changes 419

P-GW Event Reporting Statistics 419

Command Changes 419

show event-record 419

Performance Indicator Changes 420

System Schema 420

show event-record statistics pgw 420

CSCup75830 - DPC2: Diam proxy scaling 421

Feature Changes 421

Enhance Diameter Proxy Pool to Handle a Higher Number of Transactions 421

Command Changes 422
snmptrap-pdu-v1tov2  430

CSCur19167 - Bulkstats Improvement - using msg proxy for System APIs  430

Feature Changes  430

Bulkstats Performance Improvement  430

CSCur34253 - Reduce time to detect MIO failure subsequent to kernel panic.  430

Feature Changes  430

Reduce Restart Time for MIO Failure  430

CSCur53463 - Factor micro-BFD dist exclude status into lag switchover calc  431

Feature Changes  431

Exclude BFD Member-Link Port Bandwidth from Aggregator Calculation  431

CSCus04073 - Update support for Russian Timezones  431

Feature Changes  431

Correction for Russian Timezone 1  431

CHAPTER 22

VPC-DI Changes in Release 18  433

VPC-DI Feature Changes for 18.2  433

CSCue09140 - StarOS Mgmt Interface VLAN  433

Feature Changes  434

VLAN Support on Management Interfaces  434

Command Changes  434

vlan  434

CSCuo97621 - DI: planned CF switch new standby can't boot from new active - no eth0  434

Feature Changes  434

Boot from Newly Active CF Upon Switchover  434

CSCup36001 - [ePDG] IPSec Support on VPC - DI  435

Feature Changes  435

ePDG Support on VPC-DI  435

CSCup36063 - [ePDG] IPSec Scale - Performance Improvement in SSI  435

Feature Changes  435

Increased ESP Packet Processing Performance  435

Command Changes  435

text  435

hmac  436

CSCup66766 - MME support on VPC-DI  436

Feature Changes  436
MMEmgr Linear Scalability 436
Command Changes 437
mmemgr-average-cpu-utilization 437
Performance Indicator Changes 437
congestion-control configuration 437
CSCup68855 - HeNBGW support on Virtual Platform (VPC-DI) 437
Feature Changes 438
HeNB-GW Support on VPC-DI 438
CSCup75830 - DPC2: Diam proxy scaling 438
Feature Changes 438
Enhance Diameter Proxy Pool to Handle a Higher Number of Transactions 438
CSCup86883 - VPC-DI Serving GPRS Support Node 438
Feature Changes 438
SGSN Support on VPC-DI 438
CSCuq12270 - Add support for multiple IP interfaces in the same IP subnet 438
Feature Changes 438
Multiple IP Interfaces in the Same IP Subnet 438
CSCuq12399 - Implement flow-redirect mechanism. 439
Feature Changes 439
Packet Flow Redirection 439
CSCuq13710 - openstack cfgdisk metadata for DI Slot number 439
Feature Changes 439
OpenStack Configuration Metadata 439
CSCuq60328 - LESS: Qualify with VPC 439
Feature Changes 439
L-ESS Now Supported on VPC-DI 439
CSCuq97176 - VPC-DI Network mapping and A-B bonding support 439
Feature Changes 440
Network Mapping of NICs for non-UCS Hardware 440
CSCut22121 - [SaMOG] - Qualification of SaMOG on VPC-DI platform 440
Feature Changes 440
SaMOG Running on VPC-DI Platform 440
CSCut30530 - 32 BGP ECMP Support for vPC-DI 440
Feature Changes 441
Increase Maximum Number of ECMP Paths 441
CHAPTER 23

VPC-SI Changes in Release 18 443

VPC-SI Feature Changes for 18.2 443

CSCue09140 - StarOS Mgmt Interface VLAN 443
   Feature Changes 443
      VLAN Support on Management Interfaces 443
   Command Changes 444
      vlan 444

CSCum64947 - [ePDG] - ePDG service support on SSI 444
   Feature Changes 444
      ePDG and HNB-GW Support on VPC-SI 444

CSCup35998 - [ePDG] IPSec scale and performance improvement on SSI 444
   Feature Changes 445
      Higher Number of IPSec Sessions for ePDG 445

CSCup36063 - [ePDG] IPSec Scale - Performance Improvement in SSI 445
   Feature Changes 445
      Increased ESP Packet Processing Performance 445
   Command Changes 445
      encryption 445
      hmac 446

CSCup66766 - MME support on VPC-DI 446
   Feature Changes 446
      MMEmgr Linear Scalability 446
   Command Changes 447
      mmemgr-average-cpu-utilization 447
   Performance Indicator Changes 447
      congestion-control configuration 447

CSCuq59203 - HeNBGW support on Virtual Platform (VPC-SI) 447
Feature Changes 448

HeNB-GW Support on VPC-SI 448

CSCuq60328 - LESS: Qualify with VPC too (in addition to ASR5000 and ASR5500) 448

Feature Changes 448

L-ESS Now Supported on VPC 448
AAA Changes in Release 18

This chapter identifies accounting management features and functionality added to, modified for, or deprecated from AAA in StarOS 18 software releases.

- AAA Enhancements for 18.5, page 1
- AAA Enhancements for 18.4, page 3
- AAA Enhancements for 18.2, page 8
- AAA Enhancements for 18.1, page 15
- AAA Enhancements for 18.0, page 39

AAA Enhancements for 18.5

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

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

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

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

**CSCuw61382 - Rf support on HA for offline charging - diameter part**

*Applicable Products:* HA

*Related CDETS ID:* CSCuw19222
Feature Changes

Support to Generate RF records for HA Service

Important: This is a customer-specific implementation. Contact your Cisco account representative for more information.

In order to support customer’s specific billing requirements, some AVP level changes are introduced for RF support on HA node. Now the customer-specific RF accounting dictionary “aaa-custom6” includes only the desired AVPs excluding the following ones that are not applicable for HA call:

- 3GPP-Charging-Id
- Node-Id
- Called-Station-Id
- 3GPP-Charging-Characteristics
- Charging-Characteristics-Selection-Mode
- Dynamic-Address-Flag
- IMSI-Unauthenticated-Flag
- 3GPP-IMSI-MCC-MNC
- User-Equipment-Info

Also, the Serving-Node-Type and Node-Functionality AVPs in the aaa-custom6 dictionary are customized to use the enumerated values PDSN (99) and HA (99) respectively.

For an HA call, the following values are applicable for Diagnostics AVP:

- PMIP_LIFETIME_EXPIRED (17)
- PCRF_INITIATED_SESSION_TERMINATION (9)
- ADMIN_DISCONNECT (3)
- IDLE_TIMEOUT (4)
- SESSION_TIMEOUT (1)
- PMIP_LIFETIME_EXPIRED (17)
- PCRF_UNREACHABLE (5)
- UNSPECIFIED (0)
- PMIP_INITIATED_SESSION_TERMINATION (12)

For the HA RF records to be generated, the following configuration should be performed in the sequence:

1. Enable RF interface in the ACS Configuration
2. Configure the accounting policy in the desired context
3 Define the Diameter endpoint for Rf accounting, configure AAA group and Diameter accounting dictionary "aaa-custom6" and associate the dictionary to the aaa group.

4 Set the Accounting-Level to 'sdf' in the accounting policy and associate the Rf accounting policy to a subscriber profile.

5 In the subscriber configuration, execute the following commands to send the 3GPP2-BSID and 3GPP-RAT-Type AVPs to HA.
   mobile-ip send bsid custom-2
   mobile-ip send service-option custom-2

AAA Enhancements for 18.4

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

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

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

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

CSCuu32592, CSCuv92889 - AAA-Failure-Indication AVP support

Applicable Products: ePDG, P-GW, SaMOG

Feature Changes

Support for AAA Failure Indication

This enhancement is applicable to 18.4.3 and later releases.

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

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

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

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

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

Limitations and Dependencies

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

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

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

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

Performance Indicator Changes

Diameter Authentication Schema

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

- `aaa-failure-indication`

show diameter aaa-statistics

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

- `AAA-Failure-Indication`
CSCuu63094 - Supporting an option to include Destination-Host AVP during redirection

Applicable Products: ePDG, P-GW, SaMOG

Feature Changes

Destination-Host AVP in Redirected Requests

Important
This enhancement is applicable to 18.4.3 and later releases.

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

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

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

New Behavior: The encoding of Destination-Host AVP in redirected message is based on the new configurable option redirected-request in "destination-host-avp" CLI command. If the CLI command is enabled, Destination-Host AVP will be included in any type of Diameter redirected messages.

As per the current implementation, it is not possible to send retried messages to a different host using the same peer. This behavior is applicable for normal retry and failure-handling scenarios.

Command Changes

destination-host-avp

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

configure context context_name
diameter endpoint endpoint_name
destination-host-avp { always | initial-request [ redirected-request ] | retried-request [ ... ]

Release Change Reference, StarOS Release 18
redirected-request | | session-binding | redirected-request | }
  default destination-host-avp
  end

Notes:

• **redirected-request**: Encodes the Destination-Host AVP in any redirected request message.
• **always**: Encodes the Destination-Host AVP in all types of request messages.
• **initial-request**: Encodes the Destination-Host AVP in initial request but not in retried request.
• **retried-request**: Encodes the Destination-Host AVP in retried request but not in initial request.
• **session-binding**: Encodes the Destination-Host AVP after the Diameter session is bound with a host.

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

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

**Feature Changes**

**New Custom Dictionaries for S6b/STa/SWm Interfaces**

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

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

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

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

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

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

**Feature Changes**

**Customized Behavior for MSCC-Level Grant and FUI**

A new Diameter dictionary "dcca-custom31" is defined to support the customized FUI behavior when multiple granted quota types are available at MSCC.
This behavioral change is applicable to 18.3.5 and later releases.

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

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

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

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

---

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

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

**Feature Changes**

**Enhancements to Suppress USU in CCR for Blacklisted Content**

This enhancement is applicable to 18.3.1 and later releases.

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

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

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

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

diameter msg-type

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

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

Notes:

• **suppress-final-reporting**: When used with the diameter msg-type ccru command, this keyword disables immediate FINAL reporting for result code 4010/4012. When used with the diameter msg-type ccrt command, this keyword disables FINAL reporting for no-quota FUA Redirect/Restrict-access.

• **suppress-blacklist-reporting**: Disables FINAL reporting for blacklisted (4010/4012) content in CCR-T.

AAA Enhancements for 18.2

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

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

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

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

CSCuo23463 - 4 PCSCF addresses per row in PCSCF table

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

**Feature Changes**

**IMSA Changes to Support P-CSCF Enhancements**

The P-CSCF configuration can accept only one primary and one secondary P-CSCF IP address, that is, one IPv4 and one IPv6 address per row in the P-CSCF address table.

Two IP addresses are insufficient to address the PDN type v4v6 request for VoLTE setup. The IMSA interface is enhanced to support four P-CSCF addresses that might be needed for IPv4v6 request.
**Previous Behavior:** Only two P-CSCF IP addresses were allowed to be configured per row in the P-CSCF address table. This was sufficient for PDN type IPv4-only and IPv6-only.

**New Behavior:** This P-CSCF configuration is enhanced to allow users to configure a maximum of two IPv4 addresses (primary/secondary) and two IPv6 addresses (primary/secondary).

**Command Changes**

`p-cscftable`

The P-CSCF configuration is enhanced to accept two IPv4/IPv6 addresses for primary and two for secondary in any combination.

`configure context context_name ims-auth-service service_name p-cscftable {1 | 2} row-precedence precedence_value {ipv4-address ipv4_address | ipv6-address ipv6_address | ipv4-address ipv4_address | ipv6-address ipv6_address | ipv4-address ipv4_address | ipv6-address ipv6_address | ipv4-address ipv4_address | ipv6-address ipv6_address} [secondary {ipv4-address ipv4_address | ipv6-address ipv6_address | ipv4-address ipv4_address | ipv6-address ipv6_address}] [weight value] no p-cscftable {1 | 2} row-precedence precedence_value end`

**Notes:**
- `ipv4_address` must be entered in IPv4 dotted-decimal notation.
- `ipv6_address` must be entered in IPv6 dotted-decimal notation.

**Performance Indicator Changes**

`show ims-authorization sessions full all`

The following fields now display the configured IPv4 and IPv6 addresses:

- Primary P-CSCF
- Secondary P-CSCF

**CSCup51941 - IMSA changes for pegging stats for Rule Installation failure.**

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

**Feature Changes**

**Bulk Statistics for Rule Installation Failure**

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

IMSA Schema

The following new bulkstat variables are added to the IMSA schema to track the reasons for rule installation failure.

- dpca-imsa-rule-install-failure-unknown-bid
- dpca-imsa-rule-install-failure-invalid-qci
- dpca-imsa-rule-install-failure-resource-limit
- dpca-imsa-rule-install-failure-invalid-arp
- dpca-imsa-rule-install-failure-bid-in-qos
- dpca-imsa-rule-install-failure-parse-err
- dpca-imsa-rule-install-failure-in-mon-mthd
- dpca-imsa-rule-install-failure-in-rg
- dpca-imsa-rule-install-failure-in-on-avp
- dpca-imsa-rule-install-failure-in-off-avp
- dpca-imsa-rule-install-failure-in-flow-stn
- dpca-imsa-rule-install-failure-in-usg-mon
- dpca-imsa-rule-install-failure-in-req-accs-i
- dpca-imsa-rule-install-failure-in-fl-descp
- dpca-imsa-rule-install-failure-in-rep-lvl

show ims-authorization policy-control statistics

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

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

CSCup75954 - P-GW/GGSN needs P-CSCF failure detection support

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

IMSA Changes for P-CSCF Failure Detection

P-CSCF failure detection support is required on the P-GW/GGSN to ensure a failed P-CSCF address is not provided to the IMS client. In release 17.0, HSS-based P-CSCF restoration was supported using Private Extension IE. In this release, the failure detection mechanism is supported as per the Rel. 12 version of 3GPP 23.380 standard.

This feature supports only HSS-based P-CSCF restoration. The only change with this feature is supporting IMSA-based P-CSCF addresses and receiving the P-CSCF restoration indication as per Rel. 12 version of 3GPP standard.

Previous Behavior: The look-up and forwarding of P-CSCF server information from P-CSCF table to the session manager were performed by IMS Authorization (IMSA) server only during the setup.

New Behavior: When IMSA receives a Modify Bearer Request with P-CSCF address request indication, the list of P-CSCF IP addresses are sent to the session manager through Modify Bearer Response message.

This look-up and forwarding functionality works even when the call is with the Local Policy (LP) engine when the Modify Bearer Request is triggered.

CSCup75961 - Req63 - Timers in Deciseconds for Gx interface

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

Feature Changes

Configuration Changes to Gx Timers

Previous Behavior: Timers on the Gx interface were configured in seconds. Additionally, the Gx timers were common for all message types. For example, CCR-I, CCR-T, CCR-U.

New Behavior: This feature involves modifying the existing CLI command "diameter request-timeout" under Policy Control Configuration mode to accept the timeout value in deciseconds instead of seconds and allowing independent timers to be configured for all message types like CCR-I, CCR-U and CCR-T.

Customer Impact: This enhancement provides additional flexibility for operators to configure independent timers with reduced granularity. It helps optimize the user session setup or control and seamlessly manage the Gx interfaces.
Command Changes

diameter request-timeout

The existing CLI command "diameter request-timeout" under Policy Control Configuration mode is modified such that the time can be specified in deciseconds along with different message types. The default time is 100 deciseconds (10 seconds).

```plaintext
configure
  context context_name
  ims-auth-service service_name
  policy-control
    diameter request-timeout timer_value deciseconds msg-type { any | ccr-initial | ccr-terminate |
    | ccr-update }
    default diameter request-timeout
  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 is shown in seconds. When the CLI is displayed, the seconds are converted to deciseconds and msg-type is shown as any.

**CSCup95156 - Minimum of 30 IMS_auth_service profiles**

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

Feature Changes

**Extended Support for Configuration of IMS Authorization Service Profiles**

**Previous Behavior:** Up to a maximum of 16 authorization services can be configured in the system.

**New Behavior:** The configuration limit has been increased. Now, up to a maximum of 30 IMS authorization service profiles can be configured within the system.

**CSCus02884 - CLI based support for SGSN Change/SGSN Address for 3g call on PGW**

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

Configuration Support for SGSN_CHANGE Event Trigger and SGSN-Address AVP

The current implementation does not send SGSN_CHANGE event trigger and SGSN-Address AVP. Instead it sends AN-GW-Address AVP and AN_GW_CHANGE event trigger for GnGp scenario. This behavior is not compliant to 3GPP standard TS 29.212 specification. Hence, in this release, a new CLI command "diameter sgsn-change-reporting" has been introduced to control this behavior.

This release provides the GnGp P-GW users with the flexibility to configure detection of SGSN_CHANGE event trigger and to send SGSN-Address AVP for a 2G/3G subscriber on Gx interface to enable the PCRF to use this information to apply appropriate policies.

**Previous Behavior:** AN-GW-Address AVP was sent in CCR-I message on GnGp scenario. AN_GW_CHANGE event trigger and AN-GW-Address AVP were sent when the inter-SGSN handoff or 4G to 2G/3G GnGp handoff occurs.

**New Behavior:** When the diameter sgsn-change-reporting CLI command is configured, SGSN-Address AVP is sent in the CCR-I message to 2G/3G GnGp P-GW subscribers. SGSN_CHANGE event trigger and SGSN-Address AVP is sent when the inter-SGSN handoff or 4G to 2G/3G GnGp handoff occurs.

<table>
<thead>
<tr>
<th>Important</th>
<th>This feature is applicable only for SGSN IPv4 address. For SGSN IPv6 address, the SGSN-Address AVP is not sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>By default, AN-GW-Address AVP is sent during the call setup, when SGSN change occurs, or during the handoff from 4G to 3G.</td>
</tr>
</tbody>
</table>

Command Changes

diameter sgsn-change-reporting

This new CLI command is introduced to control the reporting of AN-GW-Address AVP and SGSN-Address AVP in CCR-I messages during GnGp scenario.

```
configure
  context context_name
    ims-auth-service service_name
    policy-control
      [ no ] diameter sgsn-change-reporting
  end
```

Notes:

- When configured, this CLI detects SGSN change and sends the SGSN-Address AVP in the CCR-I when the inter-SGSN handoff or 4G to 2G/3G GnGp handoff occurs.
- By default, AN-GW-Address AVP is sent during the call setup, when SGSN change occurs or during the handoff from 4G to 3G.
Performance Indicator Changes

show ims-authorization service name

The following field is added to the output of this show command to track if the SGSN Change reporting feature is configured.

- Sgsn Change Reporting

CSCut26593 - Need support for New Gx AVPs for Override Control

Applicable Products: GGSN, P-GW
Related CDETS ID = CSCut05534

Feature Changes

New Diameter AVPs for Override Control

To provide Override Control support to TOS and Nexthop Address, the following new Diameter AVPs are introduced in this release:

- Override-Nexthop-Address
- Override-Tos-Value
- Override-Tos-Direction
- Override-Tos-Value-Standard
- Override-Tos-Value-Custom

Override-Nexthop-Address AVP is added to override the nexthop address of the static rules.
Customer Impact: These override AVPs can be used in the CCA and RAR to override the existing static rules.

CSCut41965 - Transparent-Data over Gx (eGCDR and Gy)

Applicable Products: GGSN, P-GW

Feature Changes

Parsing Support for SN-Transparent-Data AVP over Gx

A dynamic dictionary has been created based on r8-gx-standard dictionary to support parsing of SN-Transparent-Data AVP in CCR and CCA messages sent over Gx interface. This AVP will be sent in CCR request only when this dynamic dictionary is used by the customer.
SN-Transparent-Data is a vendor-specific AVP, and it contains current PDP session information. This AVP provides information obtained from the RADIUS server during Access-Accept that can be put into vendor-specific extension towards the CGF and Prepaid server for billing purposes.

If the SN-Transparent-Data AVP is received in the RADIUS Access-Accept message during session authorization, and if the session is using PCRF/Gx interface, new value of SN-Transparent-Data AVP is present in CCR-I message. Content of this AVP should be copied from original RADIUS provided SN-Transparent-Data AVP. PCRF will either respond with the same SN-Transparent-Data content, or change it to a different value. If PCRF responds with a different value of SN-Transparent-Data AVP in CCA-I, then this value is used as a new SN-Transparent-Data information, that will be used in all other communication where "Transparent-Data" field is used (Gy, eG-CDR, PGW-CDR). If Gx and RADIUS server sends the information, Gx will take precedence.

RADIUS provided value will be used in case GGSN/P-GW does not receive any value from PCRF. If RADIUS server has not provided any value then PCRF provided value in CCA-I will be used.

---

**Important**

The maximum length of SN-Transparent-Data AVP is 247.

**Limitations:**

- SN-Transparent-Data AVP is not supported in CCA-U. If PCRF sends this AVP in CCA-U then P-GW will ignore the received data.
- SN-Transparent-Data over PCRF is supported only in dynamic dictionary of IMS Authorization service.

---

### AAA Enhancements for 18.1

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

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

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

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

---

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

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

Send P-CSCF Address Based on PCO Request

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

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

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

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

Feature Changes

Multiple CCR-Us Support Over Gx Interface

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

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

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

Though the **max-outstanding-ccr-u** CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

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

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

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

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

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

**Command Changes**

`max-outstanding-ccr-u`

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

`configure`

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

Notes:

• *value* must be an integer value from 1 through 12. The default value is 1.

**Performance Indicator Changes**

`show ims-authorization policy-control statistics`

The following fields are newly added to the output of this show command to support multiple outstanding CCR-Us per session.

• Responses in Queue
  • Current Responses in Queue
  • Purged Responses
  • Total Response in Queue

• Requests in Queue for LP
  • Current Requests in Queue
  • Purged Requests
  • Total Requests Fwd to LP
CSCup48777 - Allow OOC Triggers to fire for the same rating group in different rules

Applicable Products: GGSN, P-GW

Feature Changes

Generating OOC/ROC with Changing Association between Rule and RG

The existing Gy implementation prevents duplicate Out-of-Credit (OOC) / Reallocation of Credit (ROC) report for the same rule to the PCRF. Subscriber throttling with the same rule with different Rating-Group across OOC event does not work. To overcome this, the following implementation is considered:

When a Rating-Group runs out of credit, OOC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already OOC’d or not. Similarly, when a Rating-Group gets quota after being in OOC state, a ROC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already ROC’d or not.

Previous Behavior: MSCC’s state was previously being maintained at MSCC and rule-level to suppress OOC/ROC events. So if MSCC triggered an OOC/ROC the same was suppressed by the status maintained at the rule-level if the previous event on the rule was the same.

New Behavior: With this release, the rule level status bits are no longer used to avoid similar back-to-back OOC/ROC events. Now, the triggering of OOC/ROC events will solely be dependent on the MSCC state and triggers.

Customer Impact: Customers might see an increase in OOC/ROC events on Gx if they change the association of the rule and RG or if they use the Override feature.

CSCup48800, CSCur13722, CSCuo03073 - Any cut IR must contain a snapshot of all present RGs usage

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

Feature Changes

Snapshot of all RGs during Rf Interim Record

There are several change conditions where a partial Service Data Container (SDC) is not cut for a particular RG but ACR-Interim is generated due to maximum change conditions. There are many triggers like time limit, volume limit, etc., that will lead to maximum change condition. Because of this some RGs SDC may not be generated for a longer period of time.

With this release, Rf will be activated to take a snapshot of all the active Rating Groups (RGs) whenever an Interim Record (IR) is generated.
Previous Behavior: When a Maximum Change Condition event was triggered, only those RGs that have hit one of the Change Conditions that require a caching of data as opposed to cutting an IR, used to have their data in the generated IR.

New Behavior: When the Maximum Change Condition happens, the current Rf implementation is changed to make sure all RGs that have not been cached have a snapshot of their usage taken.

Customer Impact: This feature will facilitate in having the snapshot of every RG including the default bearer's RG. Thus, it will ensure accounting of all traffic data during the billing cycle.

Command Changes

rf report-all-active-rgs
This is a new command introduced to control the reporting of subscriber traffic data for all active Rating Groups (RGs) based on the generation of Interim Record (IR).

configure
context context_name
    policy accounting policy_name
       | default | no | rf report-all-active-rgs
end

Notes:
- rf report-all-active-rgs: This keyword will enable Rf to report the traffic data in SDC whenever an IR is sent. By default, this feature is enabled.

CSCup58702, CSCuo53205 - Support for 3gpp based RAN/NAS Cause IE on gx interface

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

Feature Changes

Support for "RAN/NAS Cause" IE on Gx Interface

New supported feature "Netloc-RAN-NAS-Cause" has been introduced to be in compliance with the Release 12 specification of 3GPP TS 29.212. This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. It requires that the NetLoc feature is also supported.

Important
This feature can be enabled only when the NetLoc feature license is installed.

A new Diameter AVP "RAN-NAS-Release-Cause" will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively, when the NetLoc-RAN-NAS-Cause supported feature is enabled. This AVP will indicate the cause code for the subscriber/bearer termination.
Command Changes

diameter encode-supported-features

The netloc-ran-nas-cause is a new keyword in this command introduced to enable the supported feature "Netloc-RAN-NAS-Cause".
configure
   context context_name
       ims-auth-service service_name
       policy-control
           diameter encode-supported-features netloc-ran-nas-cause
           | default | no | diameter encode-supported-features
   end

Notes:

• netloc-ran-nas-cause: Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.

• If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF.

Performance Indicator Changes

show ims-authorization sessions full all

This show command will display the new supported feature "netloc-ran-nas-cause" as part of the output under "Negotiated Supported Features" if it is configured.

CSCup71713, CSCup71684 - PGW RTT Support for Diameter procedures

Applicable Products: P-GW
Related CDETS ID: CSCup71684 - PGW RTT Support for GTP procedures

Feature Changes

RTT Support for P-GW

RTT feature will enable P-GW to generate event records containing a series of fields or IEs at the completion of specific Diameter procedures identified below:

• Diameter S6b - AAR/ AAA
• Diameter S6b - RAR/RAA
• Diameter S6b – Session Termination
• Diameter S6b – Abort Session
Similarly, the RTT feature will enable P-GW to generate event records at the completion of specific GTPv2 procedures identified below:

- Create Session Request/ Response
- Create Bearer Request/ Response
- Delete Bearer Request/ Response
- Delete session Request/ Response
- Modify Session Request/ Response
- Update Bearer Request/ Response

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

**Important**

These records are made available to customers in CSV file format through their Real Time Tool (RTT) system. This feature allows for near real time monitoring of the LTE network.

Enabling the new `reporting-action event-record` CLI command at APN level causes event records for GTPv2/Diameter to be sent to CDR modules. This should be enabled for both Access side APN and RADIUS returned APNs (or virtual APNs). Existing CLI command `session-event-module` in Context Configuration Mode should also be initialized.

This CLI is used for enabling RTT records of both Diameter and GTPv2 procedures.

### Command Changes

**reporting-action event-record**

This new command enables the reporting of APN-related events to a log.

```
configure
c  ontex t context_name
  apn apn_name
      [ default | no ] reporting-action event-record
end
```

**Notes:**

- **default**: Disables reporting of events to a log. By default, reporting is disabled.
• no: Disables reporting of events to a log if reporting has been enabled.

show event-record

This new command displays event record statistics for a P-GW node.

show event-record statistics pgw

Performance Indicator Changes

System Schema

The following bulkstats have been added to the system schema:

• sess-pgw-total-number-event-records
• sess-pgw-total-gtpv2-event-records
• sess-pgw-total-csr-event-records
• sess-pgw-total-cbr-event-records
• sess-pgw-total-dsr-event-records
• sess-pgw-total-dbr-event-records
• sess-pgw-total-mbr-event-records
• sess-pgw-total-ubr-event-records
• aaa-pgw-total-diam-event-records
• aaa-pgw-total-s6b-aar-event-records
• aaa-pgw-total-s6b-rar-event-records
• aaa-pgw-total-s6b-asr-event-records
• aaa-pgw-total-s6b-str-event-records
• sess-pgw-total-gx-ccri-event-records
• sess-pgw-total-gx-ccrt-event-records
• sess-pgw-total-gx-ccru-event-records
• sess-pgw-total-gy-ccri-event-records
• sess-pgw-total-gy-ccrt-event-records
• sess-pgw-total-gy-ccru-event-records
• sess-pgw-total-gy-rar-event-records
• sess-pgw-total-gy-ccru-event-records
• sess-pgw-total-gy-rar-event-records
show event-record statistics pgw

This is a new show CLI command that provides events statistics for the P-GW service. The following information appears in the output of this command:

- Total Number of Event Records
- GTPv2 Event Records:
  - CSR
  - CBR
  - DSR
  - DBR
  - MBR
  - UBR
- Diameter Event Records
- S6b Procedures:
  - AAR
  - RAR
  - ASR
  - STR
- Gx Procedures:
  - CCR-I
  - CCR-U
  - CCR-T
  - RAR
- Gy Procedures:
  - CCR-I
  - CCR-U
  - CCR-T
  - RAR

Applicable Products: P-GW
Feature Changes

Support ADC Rules over Gx

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard. ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a certain protocol or a group of protocols.

Important

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

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- TDF-Application-Identifier – It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.

- Redirect-Information – This indicates whether the detected application traffic should be redirected to another controlled address.

- Mute-Notification – This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.

- Application Detection Information – If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers "APPLICATION_START" and "APPLICATION_STOP" are generated for reporting purpose. These triggers will be displayed in the show ims-authorization full all CLI command and the corresponding statistics will be displayed in show ims-authorization service statistics CLI command.

Note that the CCR-U generated for Application-Start/Stop will have additional information about TDF-Application-Identifier in grouped AVP "Application-Detection-Information".

Performance Indicator Changes

show ims-authorization service statistics

The following fields are added to the output of this command as part of the Re-Authorization Triggers.

- Application Start
- Application Stop

show ims-authorization sessions full all

The following fields are added to the output of this command as part of the Event Triggers.
Feature Changes

Scaling of Diameter Proxy to Support DPC2

The Diameter Proxy scaling feature has been developed to increase the number of transactions handled per proxy for ASR 5500. This feature is implemented to support the requirement for the new DPC2 card in ASR 5500.

In support of this feature, the existing CLI command "require diameter-proxy" has been enhanced to allow multiple Diameter proxies per card and specify the proxy selection algorithm type in ASR 5500.

Command Changes

require diameter proxy

This command has been enhanced to allow multiple Diameter proxies per card with a specified proxy selection algorithm.

configure
  require diameter proxy {{ { single | multiple } | diamproxy-per-card 2 } | algorithm { facility | round-robin } } | master-slave
no require diameter-proxy
end

Notes:

- The CLI option [ diamproxy-per-card 2 ] [ algorithm { facility | round-robin } ] is applicable only for DPC2 hardware in ASR 5500. Multiple Diamproxies per card is the default behavior for DPC2 card. If required it can be extended to DPC with a maximum of 2 instances of Diamproxies.

- diamproxy-per-card: Option to configure the number of Diameter proxies per card. By default, two Diamproxies are spawned for DPC2 card. This is supported mainly to handle more number of transactions per proxy.

- algorithm: Option to configure the algorithm to be used to distribute the load to Diamproxies.

  The algorithm determines how the endpoints are distributed. Whenever an endpoint is associated to a service, session controller will send an Allocate-Request message specifying the endpoint name with the facility type. The framework will allocate a CPU based on the algorithm that has been configured.

  facility: This algorithm specifies that the Diameter proxy (endpoint) will be selected based on the facility type. This is the default option.

  In this algorithm, all AAA endpoints will be present in CPU 0 and all session manager endpoints will be present in CPU 1.
round-robin: This algorithm specifies that the Diameter proxy selection will be in round-robin fashion. For example, if the number of proclets running per card is 2, the first endpoint configured will be associated with CPU 0 (i.e., proxy running in CPU 0 of the same card) and the next endpoint configured will be associated with CPU 1, the third one with CPU 0 and fourth one with CPU 1.

logging filter

A new logging facility "proclet-map-frwk" has been added to track the proclet mapping framework.

logging filter active facility proclet-map-frwk level severity_level [ critical-info | no-critical-info ]

Performance Indicator Changes

show diameter proclet-map-memcache

This show command is newly added to display the Diamproxy cached memory table for AAA manager, Diameter controller and session manager.

show diameter proclet-map-memcache { aaamgr integer | diactrl | sessmgr integer }

show diameter proclet-map-table

This show command is newly added to display the Diamproxy map table for AAA manager, Diameter controller and session manager.

show diameter proclet-map-table { aaamgr integer | diactrl | sessmgr integer }

CSCup75837 - Wild Card Diameter Routing

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

Feature Changes

Configuration Support for Wildcard Diameter Routing

This feature provides customers the ability to configure wildcard based Diameter realm routing to avoid configuring individual Diameter peers and/or realms for all possible Diameter servers in their network.

The wildcard Diameter routes can be statically configured under a Diameter endpoint configuration using the CLI "route-entry realm * peer peer_name".

These route entries are treated as default route entries and they will be selected when there is no matching host@realm based or no realm based route entry available.

The wildcard route entry can be configured in the following ways:

route-entry realm * peer peer_name

- or -

route-entry host * realm * peer peer_name
Both these configurations have the same effect; matches to any host and any realm.

The wildcard Diameter route is added along with other realm based route entries in diabase. The wildcard route entry will be selected to route a message only if the message's destination realm does not match with any of the other static realm based routes.

For example,

```
route-entry realm abc.com peer peer1
route-entry realm def.com peer peer2
route-entry realm * peer peer-default
```

If the message's destination realm is `abc.com` then the message will be routed to `peer1`. If the message's destination realm is `def.com` then the message will be routed to `peer2`. If the destination realm is `xyz.com` then the message will be routed to "peer-default".

When multiple wildcard route entries are configured with same weights, then the routes are selected in a round robin fashion. When multiple wildcard route entries are configured with different weights, then the route with the highest weight will be selected.

In case when there are multiple wildcard routes with higher and equal weights and some routes with lower weights, then only the higher weight routes will be selected in round robin-fashion. The lower weight route can be selected only when the higher weight routes are not valid because of the peers being not in good state.

**Command Changes**

**route-entry**

This command has been enhanced to additionally accept wildcard character (*) for Diameter realm and host to allow routing of Diameter messages destined to any host @ any realm through the next-hop peer.

**configure**

```
context context_name
diameter endpoint endpoint_name
  route-entry { [ host ] * host_name { [ peer peer_id ] [ weight priority ] } [ realm ] * realm_name
    [ application credit-control peer peer_id ] [ weight value ] [ peer peer_id ] [ weight value ]
  }
no route-entry { [ host ] * host_name } [ peer peer_id ] [ realm ] * realm_name { application
credit-control peer peer_id ] peer peer_id ]
end
```

Notes:

- `host_name` and `realm_name` will now accept alphanumeric characters and wildcard character (*) to support wildcard based Diameter realm routing.

**CSCup75969, CSCuq46538 - EDR to include PCRF correlation identifier**

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

Support for Parsing PCRF-Correlation-Id AVP

With this release, Gx interface is extended to carry a new Diameter AVP "PCRF-Correlation-Id" with tariff plan/correlation identifier information from PCRF to GGSN/P-GW node. This AVP contains the PCRF correlation identifier of the bearer flow sent through the Gx interface. The PCRF correlation ID can be included in the EDRs only when this AVP information is obtained from Gx interface through the session setup request, session modify request or policy change request.

CSCup75973 - Req70 - AVP Charging-Information and AVP Redirect-Host

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

Feature Changes

Support for Charging-Information and Redirect-Host AVPs

Currently the gateway supports obtaining the Destination-Host from "Charging-Information" AVP received over Gx interface, and "Redirect-Host" AVP received over Gy interface.

With this release, the "Destination-Realm" AVP is also derived from the "Charging-Information" and "Redirect-Host" AVPs. The realm is extracted from the FQDN of the DiameterURI in the Charging-Information and Redirect-Host AVPs.

Previous Behavior: In the case of redirection, Destination-Realm AVP values were encoded based on the configured value without considering the server received value.

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

---

Important

This behavioral change is applicable only to a customer-specific Gy dictionary.

CSCup75991 - IPSG support for SN-CF-Policy ID AVP on Gx interface

Applicable Products: GGSN, IPSG

Feature Changes

Support for SN-CF-Policy-ID AVP on IPSG

IPSG now supports SN-CF-Policy-ID AVP to optimize the use of network resources and the ASR5K configuration for IPSG service. PCRF sends this AVP for sessions that require Content Filtering so that the IPSG only applies Integrated Content Filtering Services to relevant user sessions as instructed by the PCRF.
The Content Filtering function can be enabled/disabled per subscriber based on the policy ID received through the SN-CF-Policy-ID AVP from Gx.

To support this feature, dynamic dictionary has been created based out of dpca-custom22 with SN-CF-Policy-ID AVP added to CCA and RAR messages.

**CSCup75999 - Static Rulebase for CCR**

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

### Feature Changes

**Static Rulebase for CCR**

With this feature, an APN/subscriber can have a single rulebase applied to it, but allowing a static rulebase configuration to always pass a different or same rulebase to the OCS through CCR messages.

A new CLI command "**charging-rulebase-name rulebase_name**" is added under Credit Control (CC) group to override/change the rulebase name present in APN/subscriber template, in the CCR AVP "Charging-Rule-Base-Name". The rulebase value configured in CC group will be sent to OCS via CCR. If this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

**Customer Impact:** This feature, when activated with the CLI command, reduces the complication involved in configuration of services like adding and removing services per enterprise on the OCS system.

### Command Changes

**charging-rulebase-name**

This is a new command introduced in Credit Control group to allow static configuration of rulebase name to be passed to OCS via CCR message.

```
configure
    require active-charging
    active-charging service service_name
        credit-control group ccgroup_name
        charging-rulebase-name rulebase_name
    no charging-rulebase-name
end
```

**Notes:**

- By default, the rulebase obtained from APN/subscriber template will be sent to OCS through the CCR message.
CSCup76005 - Populate Serving Node PLMN on Rf for eHRPD

Applicable Products: eHRPD, GGSN, P-GW

Feature Changes

Populate Serving Node AVP on Rf for eHRPD

Currently, the Serving Node PLMN AVP which contains the MCC and MNC of the serving network is available on LTE. It is also available on Gy in eHRPD. But, this AVP is not populated in the Rf messages for eHRPD sessions.

Previous Behavior: For eHRPD service, the 3GPP-SGSN-MCC-MNC AVP was not sent in the Rf records.

New Behavior: The 3GPP-SGSN-MCC-MNC AVP will now be included in all Rf messages for eHRPD calls as well.

Customer Impact: This feature will allow the customers to more easily identify roaming sessions based on MCC and MNC.

CSCup89673, CSCup89677, CSCup73076, CSCup92630, CSCup82660 - Gx changes to support Timezone in CCR-U and CCR-T

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

Feature Changes

Support for Timezone in CCR-U and CCR-T

Previous Behavior: Required-Access-Info AVP was sent only during rule installation.

New Behavior: The Required-Access-Info AVP is now sent during charging rule removal process as well. That is, the Required-Access-Info AVP will be included in the Charging-Rule-Remove AVP if the Application Function (AF) requests the PCRF to report user access network information. The Required-Access-Info AVP will be sent as User Location Information (ULI)/MS timezone in the CCR-U messages.

If the NetLoc feature is enabled, then ULI or timezone information will be sent to the PCRF since the Required-Access-Info AVP was requested.

Important

Use of NPLI requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

MS-Timezone AVP will be sent in the CCR-T during ip-session termination if the NetLoc feature is enabled and if the UE sent the timezone.

While sending CCR-T if new timezone is received from UE it will be sent to PCRF. When PCRF removes a rule, if PCRF requests for access info by including Required-Access-Info AVP, CCR-U is triggered with the requested information.
CSCup91609 - Diamproxy memory usage is in over state for 3G S4 Ceps tests

Applicable Products: MME, SGSN

Feature Changes

IMSI Table in Diamproxy
Currently, Diamproxy maintains a mapping table of all the IMSIs present in the system to support stateless applications like S6a/S6d, Cx, SLg. This mapping table is used to find and forward the message to the correct session manager instance.

In this release, instead of maintaining the table in Diamproxy, it will be queried from IMSI manager as it already has the infrastructure.

If a crash occurs at Diamproxy, the IMSI table will not be recovered and hence the server initiated messages might be lost. Hence, maintaining the IMSI table is now managed at IMSI manager.

CSCup95956, CSCum42002 - DPC2: AAA Proxy/AAA MGr scaling

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

Feature Changes

Scaling of AAA Proxy/AAA Manager to Support DPC2
AAA proxy and AAA manager operations are scaled to suitably match the requirements/capabilities for DPC2 hardware.

As part of this enhancement, various changes are done to reduce the memory usage by AAA manager/AAA proxy. Also, the interaction between AAA proxy and HD controller are changed such that, even under heavy load, the HD controller will be able to sync the CDR files to HDD in background.

CSCup95998 - PSP algorithm modification - AAA changes

Applicable Products: GGSN, P-GW

Feature Changes

New AAA Attribute for APN Configured Bandwidth Policy
A new AAA attribute "Bandwidth-Policy-Secondary" is added to hold the APN configured Bandwidth-Policy value when there is RADIUS returned value present and is stored in "Bandwidth-Policy" attribute. If there is bandwidth-policy value received from AAA (RADIUS), AAA manager will send "Bandwidth-Policy" attribute as the one received from AAA and "Bandwidth-Policy-Secondary" as the one configured in APN. If there is
no value received from AAA (RADIUS), AAA manager will set "Bandwidth-Policy" attribute as the one configured in APN and the "Bandwidth-Policy-Secondary" attribute to invalid.

**Previous Behavior:** When a RADIUS returned Bandwidth Policy was received through Class AVP, the APN configured Bandwidth Policy was lost.

**New Behavior:** When the RADIUS returned Bandwidth Policy is received through Class AVP, the APN configured BW Policy is stored in the newly added AAA attribute "Bandwidth-Policy-Secondary".

**Customer Impact:** If the Class AVP arrives with undefined value, then the call is not rejected, instead the default bandwidth policy configured in APN is applied.

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

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

**Feature Changes**

**Support for SN1-RAD-APN-Name AVP in custom67**

A new RADIUS attribute "SN1-RAD-APN-Name" is included in Access-Accept message for custom67 dictionary. This attribute specifies the RADIUS returned APN name. 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.

This attribute is used to configure the virtual APN, and it is mandatory for IPv6 deployment.

**Customer Impact:** 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-RADIUS-APN-NAME is sent in Access-Accept message.

**CSCuq07202 - DPC2: CoA/DM from non-admin AAAMgr should send msg to messenger proxy**

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

**Feature Changes**

**Broadcast Messenger Support in AAAMgr and AAAProx**

**Previous Behavior:** If the accounting session ID is not present in CoA/DM message, the messages are sent from Admin AAA manager to Session managers through vectored call.

**New Behavior:** When accounting session ID is not present in CoA/DM, the messages are sent from Admin AAA manager to Session managers through a new messenger proxy.
CSCuq08626 - Separate Rf implementation for Customers

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

**Feature Changes**

**Customer-Specific Dictionaries for Rf Implementation**

It has been verified that separate dictionaries (aaa-custom6 and aaa-custom4) are supported for customers for their implementation on Rf interface.

CSCuq12013 - IMSA LTE/WiFi GTP S2b Make-Before-Break HO Compliance

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

**Feature Changes**

**IMSA Changes for LTE/WiFi GTP S2b Make-Before-Break HO Compliance**

The current implementation during LTE to WiFi Handoff (HO) has been changed from "break and make" to "make and break" in order to be compliant with the 3GPP standard specification. That is, both the old and new access types (WiFi and LTE) will remain active until the handoff is complete.

If there are multiple outstanding CCR-Uss supported, all requests prior to the LTE-WiFi handoff request will be dropped.

CSCuq14925 - Gx support for GTP based s2a/s2b

**Applicable Products:** P-GW

**Feature Changes**

**Gx Support for GTP based S2a/S2b**

**Previous Behavior:** For WiFi integration in P-GW, Gx support was already available for GTP based S2a/S2, but the implementation was specific to a particular customer.

**New Behavior:** Now the Gx support for GTP based S2a/S2 interface is extended to all customers. This implementation is in compliance with standard Rel.8 Non-3GPP specification part of 29.212, along with C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CRs from Rel.10/Rel.11.

As part of this enhancement, the following changes are introduced:

- AVP support for TWAN ID is provided
- TWAN-ID is added to r8-gx-standard dictionary
CSCuq14928, CSCuq23613 - Gy support for GTP based s2a/s2b

**Applicable Products:** P-GW

### Feature Changes

**AVP Support in Gy for GTP based S2a/S2b**

With this release, Gy support is provided for WiFi integration in P-GW for GTP based S2a/S2b. This implementation is in compliance with standard Rel.11 non-3GPP access spec of 32.399: S5-120748 S5-131017 S5-143090.

As part of this enhancement, the following AVP changes are introduced:

- Added TWAN as a new enum value for Serving-Node-Type AVP
- Added a new Diameter AVP "TWAN-User-Location-Info". This is a grouped AVP and it contains the UE location in a Trusted WLAN Access Network (TWAN): BSSID and SSID of the access point.

The TWAN AVPs will be effective only for 3GPP release 11 and it is added only to the standard Gy dictionary. That is, the TWAN AVP will be included in CCR-I/CCR-U/CCR-T messages only when the CLI command "diameter update-dictionary-avps 3gpp-rel11" is configured.

### Command Changes

**diameter update-dictionary-avps**

A new keyword **3gpp-rel11** has been introduced in this command to support 3GPP Rel.11 specific AVPs in the standard Gy dictionary.

```bash
configure
  require active-charging
  active-charging service service_name
    credit-control group ccgroup_name
      diameter update-dictionary-avps 3gpp-rel11
        [ default | no ] diameter update-dictionary-avps
  end
```

CSCuq65644, CSCup42837 - Diameter support for PMIPv6 Subscriber Continuity Support

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

AVP Support for PMIPv6 Subscriber Continuity

The PMIPv6 Subscriber Continuity Support feature is deployed to support PMIPv6 between external MAG and LMA over 3G-CDMA, GGSN and 4G LTE/eHRPD sessions. As part of this feature, the Diameter AVP "Starent-Subscriber-Permission" is used on the S6b interface to signal Mobile Router (MR) permission to the E-XGW as the Enterprise PDN connection is being authorized.

**Previous Behavior:** Starent-Subscriber-Permission AVP sent through S6b interface is allowed only with 0x20 value.

**New Behavior:** In this release, the Starent-Subscriber-Permission AVP can accept both 0x20 and 0x40 values. A new enumerated value "PMIPv6" is added to the Starent-Subscriber-Permission AVP to support the PMIPv6 Subscriber Continuity feature.

---

**CSCur08378 - DCCA LTE/WiFi GTP S2b Make-Before-Break HO Compliance**

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

Feature Changes

Suppress OOC/ROC During LTE-WiFi Handoff

The current implementation during LTE to WiFi Handoff (HO) has been changed from "break and make" to "make and break" in order to be compliant with the 3GPP standard specification. That is, both the old and new access types (WiFi and LTE) will remain active until the handoff is complete.

**Previous Behavior:** Out-of-Credit (OOC) / Reallocation of Credit (ROC) events were triggered during WiFi–LTE HO.

**New Behavior:** OOC/ROC events are suppressed during HO and retriggered only after the HO is complete.

**Customer Impact:** There will not be any impact to the customers since the PCRF is updated once the HO is complete.

---

**CSCur15061 - State of RADIUS server stuck in 'Waiting-for-response-to-Acct-On'**

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

Feature Changes

Change in Accounting-On Transaction Logic

**Previous Behavior:** Whenever a chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS
server in all the AAA manager instances was initialized to "Waiting-for-response-to-Accounting-On". The Accounting-On transmission and retries are processed by the Admin-AAAmgr.

When the Acct-On transaction is complete (i.e., when a response for Accounting-On message is received or when Accounting-On message is retried and timed-out), Admin-AAAmgr changes the state of the RADIUS accounting server to Active in all the AAA manager instances. During the period when the state of the server is in "Waiting-for-response-to-Accounting-On", any new RADIUS accounting messages which are generated as part of a new call will not be transmitted towards the RADIUS accounting server but it will be queued. Only when the state changes to Active, these queued up messages will be transmitted to the server.

During ICSR, if the interface of the radius nas-ip address is srp-activated, then in the standby chassis, the sockets for the nas-ip will not be created. The current behavior is that if the interface is srp-activated Accounting-On transaction will not happen at ICSR standby node and the state of the RADIUS server in all the AAAmgr instances will be shown as "Waiting-for-response-to-Accounting-On" till the standby node becomes Active.

**New Behavior:** Whenever the chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server will be set to Active for all the non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" for only Admin-AAAmgr instance. The Accounting-On transaction logic still holds good from Admin-AAAmgr perspective. However, when any new RADIUS accounting messages are generated even before the state changes to Active in Admin-AAAmgr, these newly generated RADIUS accounting messages will not be queued at the server level and will be transmitted to the RADIUS server immediately.

During ICSR, even if the interface of radius nas-ip address is srp-activated, the state of the RADIUS accounting server will be set to Active in all non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" in Admin-AAAmgr instance.

**Customer Impact:** Customers who use RADIUS servers to make some decisions based on Acct-On transaction should understand the change in behavior and make necessary modifications, if any, at their RADIUS server. Because even before the Accounting-On transaction is complete, ASR5K could potentially send RADIUS accounting messages for active calls to the RADIUS server.

Though there is a change in terms of state set to Active in non-Admin-AAAmgr instances of the standby node, there are no behavioral changes in ICSR setup as no messages will be sent from standby node towards the RADIUS server.

### CSCur35107 - Abnormal bearer termination

**Applicable Products:** P-GW, S-GW, SAEGW  
**Related CDETS ID:** CSCup88929

**Feature Changes**

**New Disconnect Reasons for GTP Path Failures**

In support of the Abnormal Bearer Termination feature, the following disconnect reasons have been added to indicate the proper bearer release for all failure cases identified in the VoLTE network:

- path-failure-s5(590)
- path-failure-s11(591)
For all these session disconnect reasons, IMSA sets the termination cause as "DIAMETER_LINK_BROKEN".

**CSCur62919 - Change to the logging facility for diactrl**

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

**Feature Changes**

**New Logging Facility for Diactrl**

**Previous Behavior:** DIACTRL logs were logged under diameter logging facility.

**New Behavior:** Diactrl logs will now be generated under diactrl logging facility instead of diameter logging facility.

**Command Changes**

```bash
logging filter

A new logging facility "diactrl" has been added to track the Diameter Controller proclet.

logging filter active facility diactrl level severity_level [critical-info | no-critical-info ]
```

**CSCus62331 - PGW NOT sending CCR-T to PCRF on arrival of CCA-I post guard timer expiry**

**Applicable Products:** P-GW

**Feature Changes**

**CCR-T Triggering Post Tx Timer Expiry**

**Previous Behavior:** CCR-T was not sent if the call was cleared before receiving CCA-I.

**New Behavior:** The existing implementation is modified so that P-GW will now send CCR-T to PCRF when CCA-I is received from PCRF post guard timer expiry and prior to Tx timer expiry.

It should be noted that CCR-T will not be triggered to PCRF when CCA-I is received from PCRF post guard timer expiry and Tx timer expiry.
CSCus66465 - show diameter route status command causes high CPU utilization alarms

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

**Feature Changes**

**Changes to "show diameter route" Command**

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

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

CSCus75159 - PGW not populating NRS AVP on handoff to LTE

**Applicable Products:** P-GW

**Feature Changes**

**Encoding of Network-Request-Support AVP During Handoff to LTE**

**Previous Behavior:** Network-Request-Support AVP was encoded by default when an eHRPD call is established and a standard R8 dictionary is configured.

**New Behavior:** Network-Request-Support AVP will not be sent in CCR message by default when an eHRPD call is established and a standard R8 dictionary is configured. It is encoded only when the value toggles during handover from LTE to WiFi.

CSCut02257 - Retrigger timer-expiry triggers if its suppressed during ICSR switchover

**Applicable Products:** P-GW

**Feature Changes**

**Triggering of CCRs for Validity Timer During ICSR Switchover**

**Previous Behavior:** Validity Timer (VT) and OCS unreachable interim timer were started immediately after the switchover of chassis to active state. When the standby chassis is switched to active state if the VT had already expired the CCR-U for VT was not generated.

**New Behavior:** VT and OCS unreachable interim quota timers will be started only after the audit is complete in the active state.
When a standby chassis is moved to active state if the VT timer has already expired then a CCR-U for the same will be generated.

**Customer Impact:** VT timer or the OCS unreachable interim quota timer may not trigger at the exact threshold if an ICSR switchover is happening. If VT has not expired during the switchover transition then there will be no impact to the customers.

**CSCu06448 - ASR5500 diameter peers fail to come up after planned SRP switchover**

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

**Feature Changes**

Diamproxies in Standby Chassis Mode

**Previous Behavior:** When the chassis was in standby state, all the diamproxies were stopped.

**New Behavior:** In this release, all the diamproxies will be running even when the chassis is in standby mode. Any change in ICSR grouping mask will lead to stopping and restarting of all the diamproxies on the standby chassis.

**CSCu25885 - Fatal Sig 11: Seg fault PC:**
**acsmgr_get_bearer_bw_from_rules.isra.176()**

**Applicable Products:** P-GW

**Feature Changes**

Handling of BCM Value

**Previous Behavior:** Any value was accepted for Bearer Control Mode (BCM) for GTP P-GW calls from PCRF.

**New Behavior:** Now only UE_NW BCM will be accepted for GTP P-GW calls. This behavior change is introduced to avoid any inconsistencies in the BCM value between modules, resulting in the session manager crash.

**AAA Enhancements for 18.0**

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

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

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

**CSCup38881 - [ePDG]- Diameter stack enh for custom SWm to SWu mapping**

**Applicable Products:** ePDG

**Feature Changes**

**Attribute Support for Custom SWm to SWu Error Code Mapping**

A new AAA attribute "Diameter-Result-Code" is added to support custom SWm to SWu error code mapping. This attribute will carry the Result-Code and Experimental-Result-Code AVPs to session manager. A bitmask is used to carry two AVPs in one attribute by assigning first 16 bits (MSBs) to Result-Code and the last 16 bits (LSBs) to Experimental-Result-Code. The result codes are used to map SWm errors towards UE in case of EAP transaction failure.

---

**Important**

This is a customer-specific implementation.

---

**CSCuq11182 - [ePDG]: dia auth fail handling does not support 5xxx codes for retry**

**Applicable Products:** ePDG

**Feature Changes**

**Failure Handling for 5xxx Result Codes in SWm Dictionary**

For SWm dictionary, failure-handling support is now available for 5xxx result-codes. That is, when ePDG receives 5xxx result-code, failure handling will be implemented for Diameter authentication requests and Diameter Extensible Authentication Protocol (EAP) requests.

**CSCur26626 - [ePDG] Non UICC device support EAP-TLS/EAP-TTLS support Diameter changes**

**Applicable Products:** ePDG
Feature Changes

New AVP in DER Message for SWm Dictionary

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

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

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

CSCur31589 - [SAMOG R18] Need support in Diameter dictionary to support LBO AVPs

Applicable Products: SaMOG

Feature Changes

Diameter AVP Support for LBO

As part of the Local Breakout (LBO) feature, the following Diameter AVPs are added to STa dictionary for MRME service.

- Filter-Id
- Framed-Pool
- SN1-VPN-Name
- SN1-Rulebase
- SN1-Primary-DNS-Server
- SN1-Secondary-DNS-Server

When this feature is enabled, these AVPs will be parsed in the Diameter-EAP-Answer (DEA) message.
CSCur31589 - [SAMOG R18] Need support in Diameter dictionary to support LBO AVPs
ADC Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from ADC in StarOS 18.0 software releases.

- ADC Enhancements for 18.1, page 43

ADC Enhancements for 18.1

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.

---

**Important**

For enhancements pertaining to the latest ADC Plugin release, refer to the ADC Plugin Release Notes dated March 25, 2015. Contact your Cisco account representative for more information.

CSCuq05896 - ADC support over Gx

**Applicable Products:** P-GW

**Related CDETS IDs:** CSCup75820, CSCup77479, CSCuq75294, CSCur84088
Feature Changes

ADC Support over Gx Interface

The ADC Rule feature will support detection of application level flows as described in Release-11 of 3GPP standard. ADC Rules are certain extensions to dynamic and predefined PCC Rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC Rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified application(s) and report detection of application traffic to the PCRF. Reporting of application traffic are controlled by PCRF and generates Application Start/Stop events along with the Application ID. Application mute status can be enabled or disabled on both dynamic and predefined ADC rules. When mute is disabled, Application Start/Stop event trigger will be generated by PCEF for that specific Application ID. Mute status for dynamic rule can be enabled or disabled by PCRF, in case of pre-defined rule it is configure either on boxer configuration or CLI.

Important

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

When the license is not enabled, P2P continues to function as per its original behavior, that is, it monitors the traffic at the entire rulebase level. When the license is enabled, the P2P behavior changes such as to monitor traffic at per subscriber level.

The following types of ADC ruledefs are supported for this feature.

configure

    active-charging service service_name
    ruledef adc_rule_type1
    p2p protocol = protocol_name
    p2p protocol-group = protocol_group
    p2p behavioral = behavioral_list
    multi-line-or-all-lines
    exit
    ruledef adc_rule_type2
    p2p protocol = protocol_name
    p2p traffic-type = traffic-type
    exit
    ruledef adc_rule_type2
    p2p any-match = TRUE
    exit

Notes:

• For the ruledef adc_rule_type1 ruledef type, multiline-or all-lines is optional if rule contains only one line.
A limitation for the \texttt{p2p any-match = TRUE} rule def type is that only one rule containing this rule line can be configured. This rule line must not be configured with any other P2P rule line.

\textit{Limitations}

The limitations for the ADC over Gx feature are:

- ADC does not support group of rule defs.
- Registration of the duplicate application IDs are not supported.
- Readdress/Redirection for P2P flows will not be supported.
- Redirection happens only on transactions of GET/Response.
- Port based, IP Protocol based, and URL based applications are not supported.
- Pre-configured options (precedence, redirect-server-ip) for dynamic ADC Rules are not supported.
- Simultaneous instances of an application for the same subscriber are not distinguished.
- Flow recovery is not supported for application flows.

\textbf{Command Changes}

\texttt{action priority}

The \texttt{adc} and \texttt{mute} are new keyword options added to this command to support ADC rules over Gx.

\textbf{Important} The \texttt{p2p dynamic-flow-detection} CLI command must be enabled in rulebase for this feature to work.

\begin{verbatim}
cfg active-charging service service_name
rulebase rulebase_name
  action priority action_priority { [ dynamic-only { adc | mute } ] | static-and-dynamic | timedef timedef_name } { [ group-of-ruledefs ruledefs_group_name ] | ruledef ruledef_name } charging-action charging_action_name | [ monitoring-key monitoring_key ] | [ description description ] }
  no action priority action_priority
end
\end{verbatim}

Notes:

- The \texttt{adc} keyword option specifies the rule def to be given as ADC rule. This predefined rule can be activated from PCRF/Gx. This can be configured only with the \texttt{dynamic-only} keyword and optional along with rule def. Group-of-ruledefs is not supported in this release.

- The \texttt{mute} keyword is optional and can be configured only with the \texttt{adc} keyword. This keyword option will disable ADC application reporting to PCRF, that is, will mute the Application Start and Application Stop notifications to PCRF/Gx. Detection of protocols in the rule will still happen. Whenever the application traffic matches the specified rule def for the first time in that flow, it is considered as Application Start. At the end of flow, it is considered as Application Stop.
diameter encode-supported-features

A new keyword `adc-rules` has been introduced in this command to support configuration of ADC rules over Gx interface.

`configure`
```
    context context_name
    ims-auth-service service_name
    policy-control
        diameter encode-supported-features adc-rules
        [ default | no ] diameter encode-supported-features
    end
```

Notes:
- The new keyword "adc-rules" will be available only when the feature-specific license is configured.
- For ADC 6th bit of supported feature will be set.

show subscribers

The `adc` keyword is added to this command to display ADC readdress statistics for a given call ID.

`show subscribers callid call_id adc readdress statistics`

**Performance Indicator Changes**

**show active-charging service statistics**

The following fields are added to the output of this command. These are debug statistics visible only in the Debug mode and controlled by a separate feature license.

- Dynamic Rule Statistics:
  - ADC Rules Received
  - Total ADC Rules
  - ADC Install Succeeded
  - ADC Install Failed
  - ADC Start Received
  - ADC Stop Received

- Install Failure Reason:
  - ADC Invalid Rule
  - ADC Invalid Readdress

**show active-charging sessions full all**

The following fields are added to the output of this command.
• Total ADC Rules
• Dynamic Charging Rule Definition Statistics:
  ◦ TDF Application Id
  ◦ TDF Readdress Status
  ◦ TDF Readdress IP
  ◦ TDF Redirect URL

**show ims-authorization service statistics**

The following fields are added to the output of this command.
• Re-Authorization Triggers:
  ◦ Application Start
  ◦ Application Stop

**show ims-authorization sessions full all**

The following fields are added to the output of this command.
• Event Triggers:
  ◦ Application-Start
  ◦ Application-Stop

**show subscribers callid <callid> adc readdress statistics**

The following statistics will be displayed in the output of this command to show readdress statistics at subscriber level for a given call ID.
• Total Readdressed Flows
• Readdressed Upl Pkts
• Readdressed Dnl Pkts
• Total Readdressing Failures
• Non Syn Flow
• Duplicate Key
• Dropped Pkts
CSCuq05896 - ADC support over Gx
ECS Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from ECS in StarOS 18 software releases.

- ECS Enhancements for 18.4, page 49
- ECS Enhancements for 18.2, page 53
- ECS Enhancements for 18.1, page 59

ECS Enhancements for 18.4

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.

CSCuw12560, CSCuw33132 - IPv6-OS-Signature based Tethering solution

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

IPv6 OS-based Tethering Detection

The Tethering Detection feature enables detection of subscriber data traffic originating from devices tethered to mobile smartphones, and also provides effective reporting to enable service providers take business decisions on how to manage usage and bill subscribers accordingly.
This release supports tethering detection for IPv6 TCP flows based on OS signatures. This feature is configurable at the rulebase level and is enhanced to support IPv6 flows for all subscribers having IPv6 OS configuration within the rulebase.

Bulk statistics and EDR variables are added in support of this enhancement. If the signature format used for IPv6 OS based tethering detection needs to be modified, additional data must be collected to identify the contents of the new signature. The following new TCP parameters are added to EDRs:

- IPv6 OS signature string
- Sequence number from the TCP SYN packet of a flow
- 8 bytes of control parameters that include data offset, reserved, flags, window size, checksum and urgent pointer from TCP SYN header
- TCP options, if they are present in TCP SYN header

**Previous Behavior:** IPv6 Tethering Detection was supported only with TTL and UA signatures, and not supported with OS signatures.

**New Behavior:** OS-based tethering detection is supported for IPv6 TCP flows in this release.

**Customer Impact:** Customers will be able to detect tethering using IPv6 OS database.

### Command Changes

**tethering-database**

The `ipv6-os-signature` keyword is added to the `tethering-detection` command in support of the IPv6 OS signature-based tethering detection feature.

```plaintext
configure
  active-charging service service_name
  tethering-database [ipv6-os-signature ipv6_os_signature_db_file_name]
    { default | no } tethering-database
end
```

**Notes:**

- `tethering-database ipv6-os-signature ipv6_os_signature_db_file_name`: Specifies the IPv6 OS Signature database file to load. `ipv6_os_signature_db_file_name` must be the name of the IPv6 OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

  Default filename: `v6-os-db`

  The default filename can be changed by the user only during boot up. Once the system is up and running, the database file name cannot be modified. This is true for all tethering related database files.

**tethering-detection**

In support of the IPv6 OS-based Tethering Detection feature, the `os-db-only` and `os-ua-db` options are enhanced to support IPv6 OS based tethering detection.

```plaintext
configure
  active-charging service service_name
  rulebase rulebase_name
  tethering-detection { ip-ttl value ttl_value | os-db-only | os-ua-db | ua-db-only }
```


{ default | no } tethering-detection
end

Notes:

- **os-db-only**: Specifies to perform tethering detection using IPv4 and IPv6 OS signature databases.
- **os-ua-db**: Specifies to perform tethering detection using IPv4 OS, IPv6 OS, and UA signature databases.

**tethering-detection**

In support of the IPv6 OS-based Tethering Detection feature, the **os-ua** keyword option is enhanced to support IPv6 flows for OS-UA lookups.

```
configure
 active-charging service service_name
   ruledef ruledef_name
       tethering-detection | ip-ttl | os-ua | { flow-not-tethered | flow-tethered }
       no tethering-detection
end
```

Notes:

- **os-ua**: Specifies to select IPv4 and IPv6 flows that were tethered or not tethered as per OS-UA lookups.

**rule-variable**

In support of the IPv6 OS based tethering detection feature, new parameters — **syn-control-params**, **syn-options**, **syn-seq** and **v6-os-signature** are added to the **tcp** keyword.

```
configure
 active-charging service service_name
   edr-format format_name
   [ no ] rule-variable tcp { syn-control-params | syn-options | syn-seq | v6-os-signature } [ priority priority ]
end
```

Notes:

- **syn-control-params**: 8 bytes following the TCP Acknowledgement in the TCP SYN packet displayed as hexadecimal string of characters.
- **syn-options**: All TCP options received in the TCP SYN packet displayed as hexadecimal string of characters.
- **syn-seq**: The absolute 4 byte value of the sequence number received in the TCP SYN packet displayed as decimal value.
- **v6-os-signature**: OS signature string for IPv6 TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
- If tethering detection with current signature is not sufficient, then the three parameters **syn-control-params**, **syn-options** and **syn-seq** along with the existing **ip-control-param** parameter will be used (data collected from live nodes) to improve the IPv6 OS signature.
upgrade tethering-detection

This command is enhanced to upgrade IPv6 OS signature databases.

upgrade tethering-detection database { ipv6-os-signature } [ -noconfirm ]

Performance Indicator Changes

ECS Schema

The following new bulk statistics are added for IPv6 OS signature support:

- ecs-td-v6-os-signature-lookups – Total number of IPv6 OS signature lookups.
- ecs-td-v6-os-signature-matches – Total number of IPv6 OS signature matches.

show active-charging rulebase statistics name

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

- Tethering Detection:
  - IPv6 OS signature lookups
  - IPv6 OS signature matches

show active-charging tethering-detection statistics

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

- Tethering Detection Statistics (os-ua):
  - IPv6 OS signature lookups
  - IPv6 OS signature matches

CSCuw36228 - Incorrect tagging of TTL in the EDR records

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

IP TTL Value in EDR Records

Tethering detection for TCP OS and IP-TTL must be performed based on the same TTL value for accurate tethering of TCP flows.
**Previous Behavior:** IP TTL value was extracted from the first packet of TCP/UDP flows. Flows with a non-SYN packet might carry different values of IP TTL in OS signature and TTL EDR field.

**New Behavior:** IP TTL value is extracted from TCP SYN packets if the first packet of the flow is not TCP SYN. Flows with non-SYN packets will use the first packet TTL value till a TCP SYN packet is encountered on the flow.

**Customer Impact:** This change provides more accurate tethering for TCP flows and ensures that both TCP OS signature and IP-TTL based tethering is performed based on the same TTL value.

### ECS Enhancements for 18.2

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.

### CSCus80666 - Dis-engage TRM when a flow moves from one bearer to another

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

**Feature Changes**

**TRM Flows**

The Transactional Rule Matching (TRM) feature enables the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified. With this enhancement, TRM/Accelpath gets disengaged in case of any bearer movement for a particular flow.

**Previous Behavior:** When TRM/Accelpath gets enabled for a flow on a particular bearer and if flow moves from one bearer to another, TRM would not get disengaged. As a result, packets were being matched to rules present on the previous bearer, and not on the current bearer.

**New Behavior:** When TRM/Accelpath gets enabled for a flow on a particular bearer and if flow moves from one bearer to another, TRM will get disengaged. Packets will now be matched to rules present on the new bearer.

### CSCus96377 - Reset Flow-Bearer mapping is missed in certain scenarios

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

ACS Data Flow-Bearer Association

Previous Behavior: When a new bearer gets created from UE, ACS does not mark all existing data flow-bearer associations invalid. ACS uses existing bearer mapping to send a new downlink packet. Secondly when an uplink packet fails to match any rule on the bearer it came from, it is discarded and downlink packets for the same flow are also discarded.

New Behavior: When a new bearer gets created from UE, ACS marks all existing data flow-bearer association invalid. When a new downlink packet comes for the same flow, ACS queries SM for the correct bearer and sends the packet on the correct bearer. Secondly when an uplink packet fails to match any rule on the bearer it came from, it is discarded and the flow-bearer association is invalidated. If a downlink packet comes for the same flow, ACS now sends a bearer lookup query to SM and the packet goes on the correct bearer.

CSCut05534 - Per subscriber traffic steering/marking

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

Feature Changes

Per Subscriber Traffic Steering

Override Control feature can be activated for a subscriber using custom AVPs over the Gx interface. Override Control can be received from PCRF over Gx in CCA-I, CCA-U or RAR. This is a license controlled feature.

With this enhancement, customers will have the capability to dynamically route/mark traffic on a per subscriber basis. Override Control functionality will now support the policy parameters in charging action for post processing rules — Nexthop Address (IPv4 address only) and TOS.

Previous Behavior: In earlier releases, support to override Nexthop Address and TOS from PCRF was not provided.

New Behavior: Support to override Nexthop Address and TOS from PCRF is added in this release. The existing Override Control statistics in the output of the show active-charging rulebase statistics and show active-charging sessions full all commands will also include the new policy parameters.

The following new Diameter AVPs are introduced in support of this feature:

- Override-Nexthop-Address
- Override-Tos-Value
- Override-Tos-Direction
- Override-Tos-Value-Standard
- Override-Tos-Value-Custom

Limitations:

- Override Control supports only IPv4 Nexthop Address in this release.
If invalid value of Nexthop Address or TOS is received, then the complete Override Control message will be discarded.

Currently there is no way to withdraw an already applied Override Control message. This can only be modified.

This feature does not support Group-of-Rules in Override Control.

This feature enables customers to steer specific subscribers to different services using a unique Nexthop address. This could alternatively be accomplished using a unique VLAN ID as well. Due to the current implementation, this feature does not provide support of VLAN ID on Override Control even though VLAN ID can be received in OC message, and the packet can still be routed to default VLAN.

**Customer Impact:** Customers can now steer specific subscribers to different services using a unique Nexthop address and will be able to choose which traffic must be proxied and which should not be proxied.

**Performance Indicator Changes**

```
show active-charging subscribers callid <call_id> override-control
```

This CLI command is enhanced to include the additional policy parameters — TOS uplink/downlink and Nexthop Address.

**CSCut93985 - IP-TTL based Tethering solution**

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

**Feature Changes**

**IP-TTL based Tethering Detection**

The Tethering Detection feature enables detection of subscriber data traffic originating from PC devices tethered to mobile smartphones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly.

This release supports IP-TTL based Tethering Detection solution to detect tethering for all IP flows - both IPv4 and IPv6. This feature is configurable at the rulebase level and will be done for all flows of all subscribers having IP-TTL configuration within the rulebase. Bulk statistics and EDR variables are also added in support of this feature. Tethering Detection can now be done for IPv4, IPv6, TCP and UDP flows.

**Important**

IPv6 Tethering Detection is supported only with TTL and UA signatures, and not supported for OS signatures.
Command Changes

tethering-detection

With the IP-TTL feature, the \texttt{ip-ttl} value and \texttt{os-ua} keywords are added to the \texttt{tethering-detection} command in support of the IP-TTL based Tethering Detection feature.

```
configure
  active-charging service service_name
  rulebase rulebase_name
    tethering-detection \{ ip-ttl value \textit{ttl\_value} | os-db-only | os-ua-db | ua-db-only \}
    \[ default | no \] tethering-detection
end
```

Notes:

- \texttt{ip-ttl value \textit{ttl\_value}}: Specifies to perform tethering detection using IP-TTL configuration. \textit{ttl\_value} must be an integer from 1 through 255 to configure TTL values for tethered flows.
- \texttt{os-ua-db}: Specifies to perform tethering detection using only OS and UA signature databases.

\texttt{tethering-detection}

With the IP-TTL feature, the \texttt{ip-ttl} and \texttt{os-ua} keywords are added to the \texttt{tethering-detection} command to select flows that were tethered or not tethered.

```
configure
  active-charging service service_name
  ruledef ruledef_name
    tethering-detection \{ ip-ttl | os-ua \} \{ flow-not-tethered | flow-tethered \}
    no tethering-detection
end
```

Notes:

- \texttt{ip-ttl}: Specifies to select flows that were tethered or not tethered as per IP-TTL values.
- \texttt{os-ua}: Specifies to select flows that were tethered or not tethered as per OS-UA lookups.

\texttt{rule-variable}

With the IP-TTL and IPv6 EDR enhancement, \texttt{ip-control-param}, \texttt{tethered-ip-ttl} and \texttt{ttl} options are added to the \texttt{flow} keyword in this release.

```
configure
  active-charging service service_name
  edr-format format_name
    \[ no \] rule-variable flow \{ ip-control-param | tethered-ip-ttl | ttl \} \[ priority priority \]
end
```

Notes:

- \texttt{ip-control-param}: First 8 bytes of IPv6 header is inserted in EDRs.
- \texttt{tethered-ip-ttl}: IP-TTL based tethering detected on flow.
- \texttt{ttl}: Time To Live/Max hops value received in the first packet of the flow.
Performance Indicator Changes

ECS Schema

The following new bulk statistics are added in this release:

- ecs-td-osua-total-flows-scanned
- ecs-td-osua-tethered-flows-detected
- ecs-td-osua-non-tethered-flows-detected
- ecs-td-ipttl-total-flows-scanned
- ecs-td-ipttl-tethered-flows-detected
- ecs-td-ipttl-non-tethered-flows-detected
- ecs-td-ipttl-tethered-uplink-packets
- ecs-td-ipttl-tethered-downlink-packets

show active-charging rulebase name

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

- Tethering Detection (ip-ttl)
- Ip-ttl Values

show active-charging rulebase statistics name

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

- Tethering Detection (ip-ttl)
- Total flows scanned
- Tethered flows detected
- Tethered uplink packets
- Tethered downlink packets

show active-charging tethering-detection statistics

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

- Total flows scanned
- Total Tethered flows detected
- Tethering Detection Statistics (os-ua)
- Tethering Detection Statistics (ip-ttl)
- Total flows scanned
• Tethered flows detected
• Tethered uplink packets
• Tethered downlink packets

CSCut97261 - FAPA support for Customer

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

Feature Changes

Tethered Flows using FAPA

The FAPA feature is enhanced to accelerate tethered and blacklisted flows in this release. This functionality is extended for the active charging service with CF/ICAP/BL configured.

Previous Behavior: Currently if the active charging service has CF/BL/ICAP configured, all flows associated with the active charging service are marked not eligible for FAPA and not allowed at FAPA. All other flows of the service that do not have CF/BL/ICAP configured will be allowed on FAPA.

New Behavior: The FAPA functionality is extended for the active charging service with CF/ICAP/BL configured. The following enhancements are done for this feature.

• Packets for tethered flows will be counted on accelerated packets.
• Packets for blacklisted flows will be counted on fast-path packets.
• Simple TCP traffic will be eligible on accelerated path with content filtering configured in active charging service but not in rulebase.
• Only HTTP traffic will be blocked from accelerated path with ICAP configuration.

Customer Impact: More number of applicable flows will get accelerated using FAPA.

CSCut99876 - No CCR-U for rule-binding failure incase CBR was pending

Applicable Products: GGSN, P-GW

Feature Changes

Triggering of CCR-U for Reporting Rule Failure During Collision

Previous Behavior: P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during LTE to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received.

New Behavior: In this release, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.
Customer Impact: This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

ECS Enhancements for 18.1

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.

CSCui85235, CSCut15652 - Change-condition issue in Rf record when OCS/ Gy is down during CCR

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

**Feature Changes**

**New Change Condition for Rf Record in Gy Server Unreachable Scenario**

- **Previous Behavior:** When connection is terminated due to unavailability of Gy/OCS server, Rf STOP record used to be generated with change-condition as MGMT_INTERVENTION.
- **New Behavior:** Rf record will be generated with change-condition as ABNORMAL_RELEASE when Gy server is unreachable.
- **Customer Impact:** Different change condition will be observed in Rf STOP record generated due to unreachability of Gy server.

CSCun96897 - Simplification of ECS show CLIs- phase II

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

**Feature Changes**

**Enhancement for Ruledef Statistics**

ECS collects statistics for various reasons at many levels like flow, bearer, subscriber, rulebase, etc. to provide information like traffic patterns, system load, and so on. Enhancements are done in this release to cleanup some statistics, thereby reducing memory consumption.
The following enhancements are done in this release:

- A new CLI command `statistics-collection` is added at configuration level and execution level to dynamically enable ruledef statistics collection.

- TCP proxy statistics and current flow statistics are moved from bearer level to subscriber level. These statistics are deprecated from the `show active-charging sessions full` CLI command and available in the `show active-charging subscribers full` command. The current flow statistics are dynamically computed when the `show active-charging subscribers full` CLI is issued.

- Ruledef statistics are maintained and displayed at bearer level for individual bearers. These will now be maintained dynamically.

- The `show active-charging subscribers` command was a hidden command and is made visible in this release with the addition of current flow and TCP proxy statistics.

## Command Changes

### `statistics-collection`

The `statistics-collection` command is added in the ACS Configuration mode to dynamically enable statistics collection. This will collect specified ruledef statistics (Charging, Firewall, Post-processing) for all calls that start after the CLI is enabled.

```
configure
  active-charging service service_name
    statistics-collection { all | ruledef { all | charging | firewall | post-processing } } [no] statistics-collection
  end
```

Notes:

- By default, no statistics will be maintained.

- The `[ no ] statistics-collection all` and `[ no ] statistics-collection ruledef all` commands will result in the same output.

- If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the `show active-charging sessions full` CLI — "statistics collection disabled; not collecting <charging/firewall/postprocessing> ruledef stats".

### `statistics-collection` (Exec mode)

The `statistics-collection` command is added in the Exec mode to dynamically enable statistics collection. This will collect specified ruledef statistics (Charging, Firewall, Post-processing) for all calls that start after the CLI is enabled.

```
statistics-collection active-charging { all | charging | firewall | post-processing { callid call_id | imsi imsi_number } } [ no ] statistics-collection active-charging { callid call_id | imsi imsi_number }
```

Notes:

- The ruledef statistics will be maintained for a bearer only if this command is configured. By default, the statistics will not be maintained.
• If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the `show active-charging sessions full` CLI — "statistics collection disabled; not collecting <charging/firewall/postprocessing> ruledef stats".

`show active-charging subscribers`

The `show active-charging subscribers` command in the Exec mode is made customer visible. This CLI works at the PDN level.

`show active-charging subscribers { acsmgr instance instance_id | all | callid call_id | full | imsi imsi_number | rulebase rulebase_name }`

**Performance Indicator Changes**

**show active-charging sessions full**

The following counters have been deprecated from the output of this command, and added to the `show active-charging subscribers full` command.

• TCP Proxy:
  • TCP Proxy Flows Requests
  • TCP Proxy Flows Request Success
  • Disable TCP Proxy Flows Requests
  • Disable TCP Proxy Flows Success
  • Current TCP Proxy Flows
  • Total TCP Proxy Flows
  • TCP-proxy reset for non-SYN flows

• Current Flows:
  • Current IP Flows
  • Current ICMP Flows
  • Current IPv6 Flows
  • Current ICMPv6 Flows
  • Current TCP Flows
  • Current UDP Flows
  • Current HTTP Flows
  • Current HTTPS Flows
  • Current FTP Flows
  • Current POP3 Flows
  • Current SMTP Flows
show active-charging subscribers full

The following counters are added to the output of this command, and deprecated from the show active-charging sessions full command.

- TCP Proxy:
  - TCP Proxy Flows Requests
  - TCP Proxy Flows Request Success
  - Disable TCP Proxy Flows Requests
  - Disable TCP Proxy Flows Success
  - Current TCP Proxy Flows
  - Total TCP Proxy Flows
  - TCP-proxy reset for non-SYN flows

- Current Flows:
  - Current IP Flows
  - Current ICMP Flows
  - Current IPv6 Flows
  - Current ICMPv6 Flows
CSCuo23808, CSCup52344, CSCuq97903 - Enhancement for SIP Analyzer Statistics

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

Support for enhanced SIP Analyzer Statistics

Previous Behavior: The SIP analyzer currently supports only RFC 3261, and other limited statistics for UDP based SIP message analysis.
**New Behavior:** SIP analyzer is enhanced to support various SIP extension methods statistics, granular statistics for responses to RFC3261 including SIP extension and SIP calls statistics with TCP/UDP flows information. Rule-matching fields for new SIP Request messages are also added in this release.

**Command Changes**

`sip request method`

This command is enhanced to support rule-matching for new SIP request messages — INFO, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, SUBSCRIBE, UPDATE.

```
configure
  active-charging service service_name
  ruledef ruledef_name
      [no] sip request method operator { info | message | notify | prack | publish | refer | subscribe | update }
end
```

Notes:

**operator** must be one of the following to match the SIP method:

- `!=`: Does not equal
- `=:` Equals

**Performance Indicator Changes**

**ECS Schema**

The following bulk statistics are added in this release to display SIP analyzer statistics:

- `sip-valid-uplk-pkts`
- `sip-valid-dwnlk-pkts`
- `sip-uplk-err-pkts`
- `sip-dwnlk-err-pkts`
- `sip-curr-udp-flows`
- `sip-total-udp-flows`
- `sip-curr-tcp-flows`
- `sip-total-tcp-flows`
- `sip-info`
- `sip-prack`
- `sip-refer`
- `sip-update`
- `sip-message`
• sip-options
• sip-publish
• sip-subscribe
• sip-notify
• sip-1xx
• sip-2xx
• sip-3xx
• sip-4xx
• sip-5xx
• sip-6xx
• sip-retrans-invite
• sip-retrans-bye
• sip-retrans-ack
• sip-retrans-cancel
• sip-retrans-info
• sip-retrans-prack
• sip-retrans-refer
• sip-retrans-update
• sip-retrans-message
• sip-retrans-options
• sip-retrans-publish
• sip-retrans-subscribe
• sip-retrans-notify
• sip-retrans-1xx
• sip-retrans-2xx
• sip-retrans-3xx
• sip-retrans-4xx
• sip-retrans-5xx
• sip-retrans-6xx

The following bulk statistics are modified in this release:

• sip-total-uplk-bytes — This variable replaces sip-uplk-bytes.
• sip-total-dwnlk-bytes — This variable replaces sip-dwnlk-bytes.
• sip-total-uplk-pkts — This variable replaces sip-uplk-pkts.
• sip-total-dwnlk-pkts — This variable replaces sip-dwnlk-pkts.

The following bulk statistics are deprecated in this release:
• sip-uplk-bytes-retr
• sip-dwnlk-bytes-retr
• sip-inv-pkts

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

The following fields are added to the output of this command in this release.

• Total SIP calls
• Total SIP TCP flows
• Current SIP TCP flows
• Total SIP UDP flows
• Current SIP UDP flows
• SIP Request
  • INVITE Requests
  • ACK Requests
  • REGISTER Requests
  • BYE Requests
  • CANCEL Requests
  • PRACK Requests
  • MESSAGE Requests
  • OPTIONS Requests
  • SUBSCRIBE Requests
  • REFER Requests
  • UPDATE Requests
  • INFO Requests
  • PUBLISH Requests
  • NOTIFY Requests

• Total
• Retransmitted
• SIP Response
  • 1xx
  • 2xx
CSCuo61507 - Enhance EDR timestamps with 10ms granularity

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

**Feature Changes**

**New Timestamp Formats for more Granular EDRs**

This feature enables to record timestamps of the events at finer granularity. The timestamps will be populated according to the selected timestamp format whenever any of the predefined events/event triggers for generating EDRs is encountered.

This feature is implemented to help determine the flow durations to an accuracy of 10 milliseconds.

**Previous Behavior:** The current timestamps available in the EDR format configuration allow recording of time information only up to seconds level.

**New Behavior:** New timestamp formats are added to allow recording of time information up to milliseconds granularity.

**Command Changes**

```
attribute
```

New timestamp formats are added to the EDR attributes to record the timestamps of the events at 10 milliseconds granularity.

```
configure
  require active-charging
  active-charging service service_name
    edr-format format_name
          [ localtime ] | [ ip | tcp } { bytes | pkts } { downlink | uplink } | priority priority_value }
    end
```

**Notes:**

Feature Changes

Modification of TCP Flows

In some scenarios, UE initiates a new TCP connection request (SYN) reusing the existing source port number, received within the 2MSL time frame of the existing flow. The data flow pertaining to this old connection gets deleted after 2MSL timeout, if configured and till then the new TCP connection traffic goes on the same data flow. The TCP analyzer is not able to reopen existing TCP flow, in response to UE’s new behavior.

The TCP analyzer has been enhanced to support the optional behavior in RFC 1122, section 4.2.2.13. ECSv2 now clears the old data flow before 2MSL timeout and creates a new data flow, for UE’s new connection using the same port number. It will also generate and send last ack packet if not already sent. The CLI command has also been enhanced to control this feature at rulebase level. This feature can be enabled or disabled using the CLI command. New counters have also been modified to indicate the number of port reuse flows.

Command Changes

tcp 2msl-timeout

A new keyword **port-reuse** has been added to the tcp 2msl-timeout command at rulebase level to support the source port reuse.

configure

    active-charging service service_name
    rulebase rulebase_name
    tcp 2msl-timeout time_in_sec | port-reuse |
    { default | no } tcp 2msl-timeout
    end

Notes:

- **port-reuse**: Allows the source port reuse to reopen the TCP flow in 2msl timeout.
- When **port-reuse** keyword is configured along with tcp 2msl-timeout, reuse of the same source port number within 2msl timeout of previous flow is permitted.
- When **port-reuse** keyword is not configured along with the tcp 2msl-timeout, reuse of the same source port number within 2msl timeout of the previous flow is not supported and such a packet will be dropped.

Performance Indicator Changes

*show active-charging rulebase name*

This command has been modified to include the following field in the output:
show active-charging rulebase statistics name

This command has been modified to include the following field in the output:

- TCP 2msl port reuse

**CSCup42837, CSCup44247 - PMIPv6 Subscriber Continuity Support**

**Applicable Products:** 3G-CDMA, GGSN, 4G LTE/eHRPD

**Feature Changes**

**Support for PMIPv6 Analyzer**

The Proxy Mobile IPv6 (PMIPv6) protocol support is added for providing network-based IP mobility management support to a mobile node, without requiring the participation of the mobile node in any IP mobility related signaling. The mobile node may be an IPv4-only node, IPv6-only node, or a dual-stack (IPv4/v6). The core functional entities involved are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). This feature is implemented to leverage LTE service authorization and subscription for the PMIPv6-based MPN service authorization. This feature will be deployed to support PMIPv6 between external MAG and LMA (ASR9K) over 3G-CDMA, GGSN and 4G LTE/eHRPD.

In earlier releases, Mobile Private Network (MPN) utilized Network Mobility Services (NEMO) to provide wireless connectivity between enterprise core network and remote Enterprise sites over 3G/4G network, and supports only IPv4 addressing scheme. To expand the addressing scheme to IPv6, PMIPMv6 support is added.

**Previous Behavior:** PMIPv6 analyzer was not supported in ECS which is now required when ASR5000 is in XGW/eXGW mode. Proxy Binding Update messages (PBUs) were coming to ASR5000 over control path and were handled by SessMgr.

**New Behavior:** The PMIPv6 protocol analyzer is added to detect PMIPv6 traffic in ECS. Proxy Binding Update messages (PBUs) are now coming over data path and handled by MIPv6 protocol analyzer. PMIPv6 PBUs can come over IPv4, IPv6 or over dual stack IPv4/v6.

**Command Changes**

`clear active-charging analyzer statistics`

A new `mipv6` keyword is added to this command to clear the MIPv6 analyzer statistics.

`clear active-charging analyzer statistics [ name mipv6 ]`
**permission**

A new `pmipv6-interception` keyword is added to this command in the APN Configuration Mode to allow APN to access the external LMA over PMIPv6.

```configure
context context_name
  apn apn_name
    [ no ] permission { pmipv6-interception }
  default permission
end
```

**permission**

A new `pmipv6-interception` keyword is added to this command in the Subscriber Configuration Mode to allow subscribers to access the external LMA over PMIPv6.

```configure
context context_name
  subscriber { default | name subscriber_name }
    [ no ] permission { pmipv6-interception }
  default permission
end
```

**route priority**

A new `mipv6` option is added to the `analyzer` keyword in this release to configure route to the MIPv6 protocol in a rulebase.

```configure
active-charging service service_name
  rulebase rulebase_name
    route priority route_priority ruledef ruledef_name analyzer { mipv6 } [ description description ]
    no route priority route_priority
end
```

**Performance Indicator Changes**

**ECS Schema**

The following bulk statistics are added in this release to display statistics for MIPv6 flows:

- `mipv6-pbu`
- `mipv6-pbu-modified`
- `mipv6-pbu-discarded`

**show active-charging analyzer statistics name mipv6**

The following fields are added to the output of this command to display the current and total number of MIPv6 flows.
show active-charging subsystem all

The following fields are added to the output of this command to display the current and total number of MIPv6 flows.

- Total MIPv6 flows
- Current MIPv6 flows

CSCup44069, CSCup91558 - EDR enhancement to support NEMO MR Hosts

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

Feature Changes

EDR Enhancement to Support NEMO MR Hosts

This feature enables creating EDRs with configurable QCI attribute along with VRF name, source IP and destination IP tied to host behind the NEMO Mobile Router (MR). This feature is supported for both single-VRF and multi-VRF.

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important

This feature provides customers the option to separate offline charging based on VRF, source and destination. This enhancement is introduced to support multiple VRF (Enterprises/Departments) configuration for the NEMO MR host.

In the case of multi-VRF, this feature will provide the option to distinguish the Enterprises/Departments using different VRF on the same NEMO MR.

A new CLI command "edr nemo-call" is added at rulebase level to enable/disable this feature of populating the source IP, destination IP and vrf-name associated with UEs behind the NEMO MRs. By default this feature will be disabled.

Previous Behavior: ECS did not see the inner user packet i.e. it sees only MIP packet containing user data in both uplink and downlink direction. For example, it sees [IP header1][GRE header] [IP header2] [payload].

New Behavior: With this feature, ECS will see and analyze the inner IP packets i.e. [IP header2] [payload], and determine the source IP, destination IP and VRF name of the NEMO hosts.
Command Changes

attribute

A new attribute "\texttt{sn-nemo-vrf-name}" is added to EDR format to support NEMO sessions.

\begin{verbatim}
configure
  require active-charging
  active-charging service service_name
  edr-format format_name
  \[ \textbf{[no]} \textbf{attribute} \texttt{sn-nemo-vrf-name} \texttt{priority} priority_value \]
end
\end{verbatim}

Notes:

\begin{itemize}
  \item \texttt{sn-nemo-vrf-name}: This attribute indicates the VRF name associated with UE behind the NEMO MR. This is a customer-specific attribute, and is available only with NEMO license.
  \item The \texttt{sn-nemo-vrf-name} attribute will not be present in the EDR unless explicitly configured in the EDR format using this CLI command.
\end{itemize}

rule-variable

A new keyword "\texttt{qci}" has been added to this command to configure the new rule variable QCI in the EDR format.

\begin{verbatim}
configure
  require active-charging
  active-charging service service_name
  edr-format format_name
  rule-variable bearer qci priority priority
end
\end{verbatim}

dr nemo-call

\texttt{edr nemo-call} is a new command to control the feature of populating the source IP, destination IP and VRF name associated with UEs behind the NEMO MRs.

\begin{verbatim}
configure
  require active-charging
  active-charging service service_name
  rulebase rulebase_name
  \[ \textbf{[default|no]} \textbf{edr nemo-call} \]
end
\end{verbatim}

Notes:

\begin{itemize}
  \item The CLI command is available only with NEMO license.
  \item By default this CLI will be disabled i.e. this CLI should be configured if the feature needs to be turned ON.
\end{itemize}
CSCup77479 - ADC rule support over Gx interface as per Release 11

Applicable Products: P-GW

Related CDETS IDs: CSCuq75294, CSCup75820, CSCuq05896, CSCur84088

Feature Changes

ADC over Gx Interface

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard.

ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

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

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

Important

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

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- TDF-Application-Identifier – It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.

- Redirect-Information – This indicates whether the detected application traffic should be redirected to another controlled address.
• Mute-Notification – This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.

• Application Detection Information – If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers "APPLICATION_START" and "APPLICATION_STOP" are generated for reporting purpose.

**Limitations**

The limitations for the ADC over Gx feature are:

• ADC does not support group of ruledefs.

• Registration of the duplicate application IDs are not supported.

• Readdress/Redirection for P2P flows will not be supported.

• Redirection happens only on transactions of GET/Response.

• Port based, IP Protocol based, and URL based applications are not supported.

• Pre-configured options (precedence, redirect-server-ip) for dynamic ADC rules are not supported.

• Simultaneous instances of an application for the same subscriber are not distinguished.

• Flow recovery is not supported for application flows.

**Command Changes**

diameter encode-supported-features

A new keyword **adc-rules** has been introduced in this command to support configuration of ADC rules over Gx interface.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features adc-rules
          [ default | no ] diameter encode-supported-features
        end
  end
```

Notes:

• The new keyword "**adc-rules**" will be available only when the feature-specific license is configured.

• For ADC 6th bit of supported feature will be set.

**show subscribers**

The **adc** keyword is added to this command to display ADC readdress statistics for a given call ID.

```
show subscribers callid call_id adc readdress statistics
```
Performance Indicator Changes

show active-charging service statistics

The following fields are added to the output of this command. These statistics are visible only in the Debug mode and controlled by a separate feature license.

- Dynamic Rule Statistics:
  - ADC Rules Received
  - Total ADC Rules
  - ADC Install Succeeded
  - ADC Install Failed
  - ADC Start Received
  - ADC Stop Received

- Install Failure Reason:
  - ADC Invalid Rule
  - ADC Invalid Readdress

show active-charging sessions full all

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

- Total ADC Rules
- Dynamic Charging Rule Definition Statistics:
  - TDF Application Id
  - TDF Readdress Status
  - TDF Readdress IP
  - TDF Redirect URL

show ims-authorization service statistics

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

- Re-Authorization Triggers:
  - Application Start
  - Application Stop
show ims-authorization sessions full all

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

- Event Triggers:
  - Application-Start
  - Application-Stop

show subscribers callid <callid> adc readdress statistics

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

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

CSCup92630, CSCup82660, CSCup89677, CSCup89673, CSCup73076 - ECS support for ULI Enhancements

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

Feature Changes

Enhancements In Network Provided Location Information

The Network Provided Location Information (NPLI) feature is now supported for charging rule removal as well.

⚠️ Important

Use of NPLI feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

CSCup99498 - ECS support for IPv6 wildcards in "ip server-ip-address" CLI

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

IPv6 Wildcard Support

**Previous Behavior:** Wildcard support was not provided for rule-matching of IPv6 addresses.

**New Behavior:** ECS support for IPv6 wildcards is added in this release. If a wildcard is available in IPv6 rule-matching, then a single rule can be used to match all the server IPs and configuration can be considerably optimized. A combination of wildcard and specialized range input can also be supported in the same rule line configuration along with network mask.

Command Changes

**ip**

In this release, `address-group` is a new keyword added to configure a group of IPv6 addresses with wildcard input and/or specialized range input.

```plaintext
configure
  active-charging service service_name
  ruledef ruledef_name
  { no | ip { dst-address | server-ip-address | src-address | subscriber-ip-address } = address-group
  wildcard_address
end
```

**Notes:**

- The `address-group` keyword can be added only after the "=" operator.
- The IPv6 address with wildcard will be parsed and stored as a string.
- The range spans across a maximum of 2 bytes within ":" delimiters in a given IPv6 address.
- If no network mask is configured, it is considered as /128 mask.
- In the example — `2607:7700::*:[2020-3040]:ce1d:b083/128, *` is a wildcard input and `[2020-3040]` is a 2 byte specialized range input.

CSCuq04032 - [A-ECS] RTP flows can be accelerated after first rule-match

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

Feature Changes

Support for Accelerated RTP Flows

In this release, the Flow Aware Packet Acceleration (FAPA) feature is enhanced to accelerate RTP flows. These flows carry media traffic and can lead to significant performance improvement.

**Previous Behavior:** RTP flows were not accelerated. Only plain-TCP, plain-UDP, HTTP and HTTPS flows could be accelerated using FAPA.
**New Behavior:** RTP flows will be accelerated using FAPA.

**Performance Indicator Changes**

**ECS Schema**

The following bulkstat variable is added in this release to display the total number of accelerated RTP packets.

- rtp-accel-pkts

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

The following field is added to the output of this command to display the total number of accelerated RTP packets.

- Total Accel Pkts

---

**CSCuq12003, CSCuq11994, CSCup98379, CSCus94777 - ECS LTE/WiFi GTP S2b Make-Before-Break HO Compliance**

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

---

**Feature Changes**

**Support for Seamless Handoff from LTE to WiFi**

The current implementation during LTE to WiFi Handoff (HO) has been changed from "break and make" to "make and break" in order to be compliant with the 3GPP standard specification. That is, both the old and new access types (Wi-Fi and LTE) will remain active until the handoff is complete.

Old RAT policy (rules, OC, etc.) will remain active till HO is complete and Bearer Binding request (CBR with new RAT Policy) will be triggered on new RAT.

**Previous Behavior:** LTE to WiFi HO was "break and make" i.e. old connections (bearers) were dropped when HO was initiated even before new connection (bearer) is up.

**New Behavior:** First a connection in new RAT is made and then the old connections are dropped i.e. "make and break".

**Customer Impact:** This feature will help avoid handoff failures and data suspension during the handoff.

---

**CSCuq26322, CSCup89524 - Discontinue "if-protocol" CLI from ruledef config mode**

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

Deprecation of "if-protocol" CLI command

The `if-protocol` CLI command in the ACS Ruledef Configuration Mode was configured to associate different content IDs with the same ruledef, depending on the protocol being used. This content ID overrides the content ID specified in the charging action associated with the ruledef on the action priority line. This feature has been deprecated since this configuration was not being used by any customer.

Previous Behavior: The `if-protocol` CLI command was allowed to be configured in ruledef and when configured, the content ID defined in ruledef took precedence over the content ID in the charging-action.

New Behavior: The `if-protocol` CLI command is deprecated in this release. This command can be configured but will have no effect.

Command Changes

`if-protocol`

The `if-protocol` CLI command in the ACS Ruledef Configuration Mode is deprecated in this release.

```
configure
  active-charging service service_name
  ruledef ruledef_name
    if-protocol { http | wsp-connection-less | wsp-connection-oriented } content-id content_id
    no if-protocol { http | wsp-connection-less | wsp-connection-oriented } content-id
end
```

CSCuq46538, CSCup75969, CSCuq04720 - EDR to include PCRF correlation identifier

Applicable Products: GGSN, P-GW, SAEGW

Feature Changes

Inclusion of PCRF Correlation ID in EDRs

This feature provides CLI control for configuring a new EDR rule variable "pcrf-correlation-id". With this CLI option, it is possible to control the inclusion of PCRF correlation identifier in the generated EDRs.

The `pcrf-correlation-id` field contains the PCRF correlation identifier of the bearer flow sent through the Gx interface. The PCRF correlation ID can be included in the EDRs only when this information is obtained from Gx interface through the session setup request, session modify request or policy change request.
Command Changes

rule-variable bearer

A new keyword "pcrf-correlation-id" is introduced in this CLI command to control the inclusion of PCRF Correlation Identifier in the generated EDRs.

configure
require active-charging
active-charging service service_name
edr-format format_name
[ no ] rule-variable bearer 3gpp pcrf-correlation-id priority priority
end

Performance Indicator Changes

show active-charging edr-format all

This show command has been updated to display the new EDR rule variable if configured.

show configuration

This show command has been updated to display the new EDR rule variable if configured.

CSCuq73688 - Debug CLI to show subscriber map info

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

Support for Subscriber Map Information

In support of the Override-Control feature, a new debug CLI command is added in hidden mode to provide complete subscriber map information as output for a given Call ID.

Command Changes

depth acsmgr

This is a new debug CLI command added in Exec hidden mode to provide complete subscriber map information as output for a given Call ID.

depth acsmgr override-control subscriber-map callid call_id
CSCuq89417 - Allow use of TAB character as EDR delimiter rather than COMMA

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

**Feature Changes**

**New Delimiter for EDRs**

The comma character is currently used as the delimiter between EDR fields. But comma is a valid character for URLs. Thus when a EDR URL contains a comma, the downstream parser encounters issues.

Hence, this feature has been developed to allow TAB as an additional character to be used as the delimiter in the EDR file. For backward compatibility reasons, a new CLI configuration is provided to choose the delimiter character between both comma and TAB.

**Command Changes**

```
delimiter
```

This is a new CLI command added to EDR format configuration to allow configuration of EDR delimiters.

```
configure
  require active-charging
  active-charging service service_name
  edr-format format_name
  delimiter { comma | tab }
  no delimiter
end
```

**Notes:**

- **comma**: Comma is used as an EDR delimiter, and this is the default configuration.
- **tab**: Tab is used as an EDR delimiter.

CSCur31337 - vrf-name attribute in EDR and UDR

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

**Feature Changes**

**UDR Enhancement to Support NEMO Hosts**

New attribute is added to FDR/EDR and UDR formats to populate the vrf-name associated with the base session of NEMO setup.

The VRF name attribute in the FDR/EDR and UDR will enable the customer to correlate the NAT binding records with the FDR/EDR and UDR in the gateway.
**Command Changes**

attribute

A new attribute "sn-vrf-name" is added to EDR format to support NEMO sessions.

```markdown
configure
  require active-charging
  active-charging service service_name
  edr-format format_name
    | no | attribute sn-vrf-name priority priority_value
  end
end
```

Notes:

• **sn-vrf-name**: This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.

attribute

A new attribute "sn-vrf-name" is added to UDR format to support NEMO sessions.

```markdown
configure
  require active-charging
  active-charging service service_name
  udr-format format_name
    | no | attribute sn-vrf-name priority priority_value
  end
end
```

Notes:

• **sn-vrf-name**: This attribute indicates the VRF name associated with the base session of NEMO. This is a customer-specific attribute.

**CSCur65367 - HO trigger handling needed in populate_edr_field_sgsn for GGSN PGW calls**

Applicable Products: GGSN, P-GW

**Feature Changes**

**Handling Inter SGSN and Inter S-GW Handoff Triggers**

**Previous Behavior**: New SGSN/S-GW addresses used to get populated when the EDR gets generated during Handoff (HO) scenario.

**New Behavior**: Now the old SGSN and S-GW addresses are getting populated in the EDRs generated for HO triggers on inter SGSN handoff and inter S-GW handoff respectively.
CSCus28519 - Incorrect UL/DL byte count when non-wsp traffic routed to WSP analyzer

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

**Feature Changes**

**Non-WSP traffic to WSP analyzer**

**Previous Behavior:** When TCP packets with WAP port number 9200/9201 are routed to WAP analyzers, the packets are matched to WSP-Any rule and charged against it.

**New Behavior:** When TCP packets with WAP port number 9200/9201 are routed to WAP analyzers, the packets will not be passed to WAP analyzer and will match to defined L4/L3 rule.

CSCus77206 - Rule level volume is reported as 0 in CCR-T for CCA-U delay

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

**Feature Changes**

**Rule Level Usage Monitoring for CCA-U Delay**

**Previous Behavior:** If the `reset-usage` CLI command is not configured and usage reporting is done and if PCRF does not rearm monitoring-keys by explicitly sending monitoring-key, then the monitoring-keys were not getting disabled.

**New Behavior:** Now the monitoring-keys will get disabled after usage reporting and no additional data is sent in the CCR-T message.

This behavior is aligned to the 3GPP standard specification 29.212, section 4.5.16.

**Customer Impact:** Reporting is done only for the Usage Monitoring Information (UMI) which is re-armed in CCA-U for which usage has been reported in corresponding CCR-U. So, the usage reporting will be done in a correct manner.

CSCus78756 - Need to add support for override control license

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

New License for Override Control Feature

Previous Behavior: The override-control CLI command introduced in rulebase configuration mode was customer-specific in the previous release.

New Behavior: Now the usage of override-control CLI command is made generic and available to all customers with a common feature license instead of a customer-specific feature license.

Customer Impact: Customers should install the new license in order to use the Override Control feature.

CSCut05601 - Signal Aborted at libc.so.6/__strncmp_ia32

Applicable Products: GGSN, PDSN, P-GW

Feature Changes

Maximum SIP Calls Per Subscriber

Previous Behavior: The number of SIP calls supported per subscriber were unlimited.

New Behavior: A limit is defined to support 100 SIP calls per subscriber at a given point of time.

CSCuu00275 - unlink_ca_prime_for_sub() Sessmgr crash seen on Customer Ares DxGW Setup

Applicable Products: GGSN, P-GW

Feature Changes

Use of "update active-charging override-control rulebase-config" Command on Standby Chassis

Previous Behavior: There was no restriction on the usage of the command "update active-charging override-control rulebase-config" on a standby chassis.

New Behavior: Now when this CLI command is executed on standby chassis, the following error message "Failure: CLI executed on Standby Chassis, No Changes Done." will be displayed.

Customer Impact: Customers should be aware that this CLI command will not be allowed to run on a standby chassis.
CSCuu05981 - [acsmgr 91300 info] debug logs printed only once with update act-chg CLI

Applicable Products: GGSN, P-GW

Feature Changes

Change in Error Log Display

Previous Behavior: For any failure, the CLI command "update active-charging override-control rulebase-config" used to print the following error message "Failed to Update Rulebase Change for Active Calls".

New Behavior: In this scenario, this CLI command now displays "Failed to apply Inheritance/Override values for any changes done in configuration".
CSCuu05981 - [acsmgr 91300 info] debug logs printed only once with update act-chg CLI
ePDG Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from ePDG in StarOS 18 software releases.

• ePDG Enhancements for 18.4, page 87
• ePDG Enhancements for 18.2, page 90
• ePDG Enhancements for 18.0, page 94

ePDG Enhancements for 18.4

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

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

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

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

Important

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

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

CSCux26495 - Configurable EBI range on ePDG

As part of this release a new command **ebi range start xx end xx** is added to ePDG Service Config Mode.

**Important**
This enhancement is applicable to 18.4.3 and later releases.

Feature Changes

Configuring EBI range

Configures EBI related parameters for bearer-id allocation (applicable only for GTPv2-S2b).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration
`configure > context context_name > epdg service service_name`

Entering the above command sequence results in the following prompt:
`{context_name}@host_name(config-epdg-service)#`

**Syntax**

`ebi range start value end value [-noconfirm ]`
`default ebi range [-noconfirm ]`

**Important**
The EBI range change to configuration is not supported and will result in service restart that deletes all existing sessions. A CLI prompt with warning is provided to avoid accidental configuration change.

`default`
Sets the default EBI related parameters for bearer-id allocation.
range
Configures EBI range for bearer-id allocation.

start value
This is the start value of EBI range.
value is an integer between 5 and 15.

end value
This is the end value of EBI range that can be greater than or equal to start value.
value is an integer between 5 and 15.

-noconfirm
Change EBI range for EPDG service without prompting for confirmation.

Usage
Use this command to configure the EBI related parameters for bearer-id allocation (applicable only for GTPv2-S2b).

Example
The following command configures the EBI related parameters for bearer-id allocation with start value as 5 and end value as 12:
ebi range start 5 end 12

Monitoring and Troubleshooting the Configurable EBI range for Bearers in ePDG
This section provides new monitoring show command outputs introduced as part of ePDG Configurable EBI range for Bearers Support.

Configurable EBI Range for Bearers Support Show Command Outputs

show epdg-service all
A new show out put variable is introduced for show epdg-service all for Configurable EBI Range monitoring and troubleshooting support:

• EBI: Allowed Range xx to xx

CSCuu32592 - AAA-Failure-Indication AVP support
Refer the AAA Enhancements for 18.4 section for more information on this feature.
CSCuv73157 - UE Local IP Address IE in the S2b Interface over GTPv2

Feature Changes

SUE Local IP Address IE in the S2b Interface over GTPv2

With this release EPDG sends UE Local IP (SWu interface) to the PGW in CSR. This is encoded in the IP Address IE present in the Create Session Request as per the 3GPP spec 29.274. EPSG also sends UE UDP port to the PGW in CSR when NAT is detected for the subscriber.

ePDG Enhancements for 18.2

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

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

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

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

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
CSCuu24382 - Support for IPSEC Integrity algorithm HMAC-SHA2

**Applicable Products:** ePDG

**Feature Changes**

**SHA2 HMAC algorithms support**

With this release ePDG supports all flavours of SHA2 HMAC algorithms as defined in RFC 4868. This is in addition to IPSEC integrity algorithms support including HMAC-SHA1-96, HMAC-MD5-96 and AES-XCBC-96.

CSCut20186 - Fast reauth support for ePDG

**Feature Changes**

The UEs accessing through ePDG can perform multiple reattach due to movement across/within WLAN Network and can also access multiple PDN at the same time. In these cases, the UE authentication is performed frequently with AAA-server involving HSS node interaction for EAP-AKA algorithm.

The operator providing the untrusted WLAN access solution through ePDG can enable fast-reauthentication in AAA-server and UE in order to perform faster authentication and reduce the load in HSS. This is because the fast-reauthentication uses the keys derived in the previous full-authentication. Also fast-reauthentication helps the operator to enable local-policy in UE node to authenticate itself to AAA server periodically for enhanced security.

**Applicable Products:** ePDG

**Performance Indicator Changes**

**Monitoring and Troubleshooting the ePDG Fast Re-Auth Support**

This section provides new monitoring show command outputs introduced as part of ePDG Fast Re-Auth Support.

**ePDG Fast Re-Auth Support Show Command Outputs**

```plaintext
show crypto statistics ikev2
```

New show out put variables are introduced for `show crypto statistics ikev2` under EAP-AKA-Fast-Reauthentication:

- **Current:**
- **Attempt:**
- **Success:**
CSCut20186 - Support for DSCP marking in SWu interface downlink packets

Applicable Products: ePDG

Feature Changes

DSCP marking in SWu interface downlink packets
The ESP IP header of the downlink packet in SWu interface sent out of ePDG has the TOS value copied from the inner IP payload of the ESP packet. But as per the customer requirement the TOS value should be taken from the configuration or GTPU IP header received on S2B side.

Previous Behavior: The TOS value is copied from inner ip-payload of ESP packet to ESP-IP-Header.
New Behavior: The TOS value is obtained from configuration or GTPU-IP-header. The configuration is available inside qi-cqi-qos-mapping table, which is associated to epdg-service configuration.
Customer Impact: None

vPC-DI for ePDG

Applicable Products: ePDG

Feature Changes

QvPC-DI for ePDG
With this release, ePDG supports QvPC-DI.

CSCut20141 - Offline Charging (CDR) support for ePDG

Applicable Products: ePDG

Feature Changes

Data buffering support for DL pkts for DL pkts before session establishment
Offline charging is a process where charging information is collected concurrently with that resource usage. The charging information is then passed through a chain of logical charging functions. At the end of this process, CDR files are generated by the network, which are then transferred to the network operator's Billing Domain(BD).

Charging information like amount of data transmitted in uplink and downlink direction are collected as part of ePDG-CDR are used to inter-operator settlements.

Previous Behavior: CDR feature support unavailable in ePDG service.
New Behavior: CDR feature introduced in ePDG service.
Customer Impact: ePDG customer can enable CDR accounting and charge the end users based on resource usage.

Performance Indicator Changes

GTPP Schema

Below are the new monitoring bulkstats introduced as part of ePDG Offline Charging support.

- total-epdgcdr-xmit
- total-epdgcdr-rexmit
- total-epdgcdr-accept
- total-epdgcdr-fail

CSCuu51841 - Unable to scale when OCSP is not reachable

Feature Changes

Scale up issue

On ePDG DI system tests, when OCSP is enabled on crypto template and made unreachable, sessions are not able to scale up not more than 12 for cert based authentication.

Previous Behavior:

- If OCSP responder is unreachable, non-blocking system call-connect-takes time to return error (due to TCP retransmission exponential backoff mechanism), which is delaying session establishment time.
- With this configuration, irrespective of time taken by connec-to-return-error, if there is no response from kernel, within the configured timeout, TCP socket will be closed and session will proceed with alternate fallback mechanism for cert validation. (ca-crl)
- The configuration is in Sec and range 1 to 60 Sec.

New Behavior:

- Added a CLI under Crypto Template as [default] timeout cert-server <value>.

Customer Impact: None

Command Changes

timeout

New command timeout is introduced to configure Certificate Server timeout in seconds.

configure
context context_name
timeout cert-server timeout_value
default timeout cert-server
end

ePDG Enhancements for 18.0

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.

**CSCun88535 - Data buffering support for DL pkts before session establishment**

**Applicable Products:** ePDG

**Feature Changes**

**Data buffering support for DL pkts for DL pkts before session establishment**

For ePDG call establishment, once the PGW sends the create session response message to ePDG the call setup is complete at PGW and Downlink traffic may come. However on ePDG processing of create session response and setting up of IPsec tunnel may take small duration so it is required that before bearer establishment and IPsec tunnel establishment is completed ePDG should have capability to buffer the data. In case of handover especially when the LTE bearer is torn down after sending create session response the downlink traffic shall be sent over the WLAN so this becomes important to buffer data on ePDG avoiding any traffic loss.

**Previous Behavior:** ePDG was dropping the DL packets in connecting state.

**New Behavior:** ePDG will buffer the data packets in connecting state and will release the buffered packets in connected state. Shared buffer is 10 MB as system level.

**Customer Impact:** ePDG will become more reliable as seen by the customer.

**Command Changes**

`data-buffering`

The `data-buffering` command has been introduced in the ePDG Service Configuration Mode to allow downlink packets to be buffered, while session is in connecting state. By default it is enabled.

configure context profile_name
    [ no ] default ] data-buffering
end

CSCup26465 - Non VoLTE data outage improvements

Applicable Products: ePDG

Feature Changes

Non VoLTE data outage improvements

ePDG does allow the data for non-voLTE calls during ICSR switchover to reduce the data-outage for non-voLTE calls and is configuration controlled to either allow data traffic for both VoLTE and non-VoLTE calls or only VoLTE calls.

CSCup35998 - IPSec scale and performance improvement on SSI

Applicable Products: ePDG

Feature Changes

IPSec scale and performance improvement on SSI

ePDG needs to be supported on the SCALE (qvEPC - DI). This feature is mainly for IPsec infrastructure support.

Previous Behavior: No of Ipsecmgr was constant
New Behavior: it will be dynamic based on memory/CPu core
Customer Impact: None

CSCup38880, CSCup38881, CSCup38882 - Custom SWm to SWu error code mapping

Applicable Products: ePDG

Feature Changes

Custom SWm to SWu error code mapping

The Communication service providers (CSP) would like the ability to take different actions depending on the severity of the error received from the AAA (SWm interface). If there is a temporary congestion in the network, a retry is appropriate. If the UE is blacklisted or has no valid APN then ePDG should not continue to retry.

In compliance with RFC 5996 2.21.2 ePDG sends AUTHENTICATION_FAILED/24 as Notify Error message type in IKE_AUTH_RESP message on SWu interface for all the SWm interface error codes.
The ePDG needs mapping of SWm to SWu error codes for communicating different error codes to device, enabling device to identify whether its temporary failure or permanent and can accordingly try connecting to the ePDG.

The ePDG continues to release the call while notifying the UE about the SWm error, however the UE based on error code shall take decision when to try connecting again.

**Previous Behavior:** All diameter errors were mapped as AUTH_FAIL towards UE.

**New Behavior:** Now a mapping exists (CLI enabled), where different sets of diameter error produces a different SWu notify error code.

**Customer Impact:** Yes. This is a customer requirement. And it can be disabled through CLI.

**Command Changes**

custom-sw-m-sw-u-error-mapping  
The custom-sw-m-sw-u-error-mapping command has been introduced in the Crypto Temp Config Mode to enable Customized mapping of SWm errors with SWu Notify Error Type.

```plaintext
configure
    context profile_name
        [ no ] allow { custom-sw-m-sw-u-error-mapping | duplicate-prec-in-tft }
    end
```

**CSCup44422 - Session Audit Removal from demuxmgr ePDG**

**Applicable Products:** ePDG

**Feature Changes**

**Session Audit Removal from demuxmgr ePDG**

Currently EGTPC demuxmgr keeps the session list in its database. This database supports add, update, delete session. Due to heavy database, these operations consume good amount of CPU cycles, significant memory is used to store the sessions. This feature is about removal of the session list from the demux & to make sure that current functionality does not get affected.

**CSCup90380 - ePDG bearer duration KPIs**

**Applicable Products:** ePDG

**Feature Changes**

**ePDG bearer duration KPIs**

Service providers require monitoring VoWiFi dedicated bearer and would like to have more granular session duration. Therefore its important to support following show command.
Performance Indicator Changes

**show session duration apn**

ePDG supports APN and dedicated bearer level view for "show subscriber statistics" and for "show session duration".

- 5 seconds call number during time period
- 10 seconds call number during time period
- 30 seconds call number during time period
- 30min call number during time period
- 1hr call number during time period
- 2 days call number during time period
- 4 days call number during time period

**ePDG Schema**

The following new bulksts Schema is added for this release to enable providing the apn-qci duration details for custom swm to swu mapping:

- aaa-network-failure
- aaa-network-too-busy
- aaa-roaming-not-allowed
- aaa-rat-disallowed
- aaa-no-subscription

The following new bulksts Schema is added for this release to enable providing the apn-qci duration details for DL data buffering:

- tx-buffered-pkts
- tx-buffered-bytes
- tx-curr-buffered-pkts
- tx-curr-buffered-bytes

**ePDG APN QCI Duration Schema**

The following new bulksts Schema is added for this release to enable providing the apn-qci duration details.

- apn-name
- qci-value
- qci-calldur-5sec
ICSR based upgrade and downgrade between N and N-2 Release Support

Applicable Products: ePDG

Feature Changes

Upgrade and Downgrade between N and N-2 Release

The ePDG supports upgrade or downgrade capability from N to N-2 release and vice versa and upgrade/downgrade from release 18 (N) to 16 (N-2).
CHAPTER 5

GGSN Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from GGSN in StarOS 18 software releases.

- GGSN Enhancements for 18.5, page 99
- GGSN Enhancements for 18.4, page 101
- GGSN Enhancements for 18.2, page 102
- GGSN Enhancements for 18.1, page 107

GGSN Enhancements for 18.5

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

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

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

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

---

**Important**

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

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
CSCuw08643 - v6 support on newcall duplicate subscriber requested addr accept

Feature Changes

Duplicate Address Support for IPv6

This feature supports IPv6 PDN establishment with duplicate static IPv6 address from same user for an already existing PDN. This makes the PDN re-establishment successful and avoids enterprise users from experiencing service outage due to duplicate IP address request. A new CLI has been introduced at P-GW and GGSN service level to control this behavior. To support duplicate IPv4v6 address request, the existing CLI for duplicate address support for IPv4 and the newly added CLI for IPv6 need to be configured. Once the CLI is configured and the feature is enabled, the old session is terminated to accept the new connection with the same IPv6 address. If the feature is not enabled and the CLI is not configured then the new connection request is rejected if the requested address is already in use.

A new disconnect reason "dup-static-ipv6-addr-req" has also been added for the existing PDN, whenever the session is terminated due to a duplicate IPv6 address request.

Command Changes

duplicate-subscriber-requested-v6-address

A new CLI has been introduced at P-GW and GGSN service level to support duplicate IPv4v6 address request. This CLI supports IPv6 PDN establishment with duplicate static IPv6 address from same user for an already existing PDN. This makes the PDN re-establishment successful and avoids enterprise users from experiencing service outage due to duplicate IP address request.

configure
  context context_name
ggsn-service <ggsn-service-name>
    newcall duplicate-subscriber-requested-v6-address { accept | reject }
default newcall duplicate-subscriber-requested-v6-address { accept | reject }
end

Notes:

• duplicate-subscriber-requested-v6-address: Configures the support to accept or reject a duplicate address request with same IPv6 address.

• accept: Accepts the duplicate sessions with same IPv6 address request.
• **reject**: Rejects the duplicate sessions with same IPV6 address request.
• **default**: Disables the support to accept a duplicate address request.

**Performance Indicator Changes**

**show configuration**

The following field has been added to the output of this command under the GGSN service:

- duplicate-subscriber-requested-v6-address accept
- duplicate-subscriber-requested-v6-address reject

**show configuration verbose**

The following field has been added to the output of this command under the GGSN service:

- duplicate-subscriber-requested-v6-address accept
- duplicate-subscriber-requested-v6-address reject

**show ggsn-service name <ggsn-service-name >**

The following field has been added to the output of this command under the GGSN service:

- Duplicate Subscriber Addr Request IPv6: Accept
- Duplicate Subscriber Addr Request IPv6: Reject

**GGSN Enhancements for 18.4**

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

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

---

**Important**

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

- **AAA Enhancements**
- **CF Enhancements**
CSCuv49840 - Non standard QCI modification fails when mapped to same pre-rel8 QCI

Feature Changes

Pre-Release 8 QoS Mapping

Previous Behavior: When multiple non-standard QCIs were associated with the same pre-release 8 QoS value (such as the following example) and there was a change between those non-standard QCI, QCI was not updated.

```configure
qci-qos-mapping name
operator-defined-qci 190 non-gbr pre-rel8-qos-mapping 7
operator-defined-qci 254 non-gbr pre-rel8-qos-mapping 7
end
```

New Behavior: Now, when multiple non-standard QCIs are associated with the same pre-release 8 QoS value and there is change between those non-standard QCIs, the non-standard QCIs will be updated and no UPC will be triggered towards the access side for the same.

GGSN Enhancements for 18.2

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.
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

CSCuc83409 - 'show gtpc summary' not able to filter on imsi, ip-address, callid, username

Feature Changes

Change to the 'show gtpc' CLI Command

Unwanted filter command options have been removed from the CLI commands show gtpc and show gtpc summary.

Previous Behavior: The CLI commands show gtpc and show gtpc summary had many filter options.

New Behavior: The CLI commands show gtpc and show gtpc summary have been modified to remove the following keywords and their associated options:

- callid
- imsi
- user-address

Performance Indicator Changes

show gtpc

This command has been modified as follows:
Previous Command: show gtpc { all | apn | callid | counters | full | ggsn-service | imsi | sgsn-address | smgr-instance | statistics | summary | user-address | username }

New Command: show gtpc { all | apn | counters | full | ggsn-service | sgsn-address | smgr-instance | statistics | summary }

show gtpc summary

This command has been modified as follows:

Previous Command: show gtpc summary { all | apn | callid | ggsn-service | imsi | sgsn-address | smgr-instance | user-address | username }

New Command: show gtpc summary { all | apn | ggsn-service | sgsn-address | smgr-instance }

**CSCur80803 - Supporting Counters to Report 2G & 3G PDP Numbers in GTP-C Schemas**

**Feature Changes**

**New Counters to Report 2G and 3G PDP Numbers in GTP-C Schema**

This enhancement adds a bulkstat counter to the GGSN function to measure the number of 2G and 3G PDP contexts at GGSN. Counter support has been added in the GTP-C schema to report the 2G PDP and 3G PDP numbers at the GGSN function/node.

**Previous Behavior:** Counters to display the number of active and setup 2G and 3G PDP contexts at GGSN were not available.

**New Behavior:** New counters have been added in GTP-C schema and in the **show gtpc statistics** command output to display the number of active and setup PDP contexts on the basis of RAT type.

**Performance Indicator Changes**

**GTP-C Schema**

Following counters have been added to the GTP-C schema to display the total number of active/inactive 2G and 3G PDP contexts:

- setup-2g-pdp
- current-2g-pdp
- setup-3g-pdp
- current-3g-pdp
show gtpc statistics

Output of this command has been modified to display the total current session statistics and total setup session statistics of 2G and 3G PDP contexts at GGSN.

• Session Stats:
  • Total Current
  • 2G
  • 3G
  • Total Setup
  • 2G
  • 3G

CSCur85219 - New GGSN counter to measure connected subscribers

Feature Changes

New GGSN Counter to Measure Connected Subscribers

New bulkstat gauges have been added to measure the amount of connected subscribers.

Previous Behavior: Gauges the unique number of subscribers for GGSN were not available.

New Behavior: New gauges have been added in GTP-C schema and in the `show gtpc statistics` command output to display the number of unique GGSN subscribers per RAT type.

Performance Indicator Changes

GTP-C Schema

The following gauges have been added to the GTP-C Schema to measure the connected subscribers:

• num-ggsn-active-ue
• num-ggsn-active-2g-ue
• num-ggsn-active-3g-ue

show gtpc statistics

This command now includes the following information:

• Active Subscribers:
  • Total
Feature Changes

Licensing Bulkstats Enhancements

To enforce pricing based on per active sessions for 2G/3G and 4G subscribers, new counters have been added to the APN schema to count the number of active sessions per RAT type per APN. The CLI commands `show apn statistics` and `show bulkstats` have been modified to display the active sessions per APN for 2G, 3G, and 4G per RAT type per APN.

Performance Indicator Changes

APN Schema

The following new gauges on active sessions per 2G, 3G, and 4G have also been modified.

- active-eutran-sessions
- active-geran-sessions
- active-utran-sessions
- active-wlan-sessions
- active-hspa-sessions
- active-other-sessions

`show apn statistics name <apn_name> | all`

This command output has been modified to include the following new fields:

- Active Sessions per RAT Type
- EUTRAN
- UTRAN
- GERAN
- WLAN
- HSPA
- OTHER
CSCus11708 - L2TP support with Demux on MIO

Feature Changes

L2TP Support with Demux on MIO (ASR 5500)

Please see "System and Platform Enhancements" chapter for more details.

GGSN Enhancements for 18.1

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.

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
CSCun23280 - GTP Throttling Stats plugging to RLF Stats

Feature Changes

Support for GTP-C RLF Statistics

The existing CLI commands have been enhanced to display GTP-C statistics.

Performance Indicator Changes

show rlf-context-statistics sessmgr gtpc-context-name ingress

This command displays the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress

This command displays the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress summary

This command displays the summary of the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress verbose

This command displays the RLF-Context statistics verbose level for GTP-C services like PGW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-memcache-statistics sessmgr

This command displays the cumulative RLF memory cache statistics for all session managers.

show rlf-memcache-statistics sessmgr instance 1

This command displays the RLF memory cache statistics for session manager instance 1.

clear rlf-context-statistics sessmgr gtpc-context-name ingress

This command clears the RLF context statistics in the VPN-Context/GTPC-Context-name "ingress".
CSCus07270 - [GGSN]: CLI 'show subscribers ggsn-only full all' having incorrect value

Feature Changes

Correction In The Output Text of CLI Command

Previous Behavior: When the data rate exceeds the MBR, earlier only drop counters for UL data in the show subscribers ggsn-only full all command was incremented. Drop counters in the DL data were not incremented.

New Behavior: When the data rate exceeds the MBR, drop counters in the DL traffic is also incremented in the show subscribers ggsn-only full all command.

Customer Impact: Drop counters for DL data in the show subscribers ggsn-only full all command would be incremented when the data rate exceeds the MBR.

Performance Indicator Changes

show subscribers ggsn-only full all

The show subscribers ggsn-only full all command has been modified to display the incremented values of the drop counters for the DL data when data rate exceeds the MBR.

CSCus25086 - Incorrect qosNegotiated seen in custom6 GCDR

Feature Changes

Change in Peak Throughput in QoS

In case of GGSN, if UPC request is received with a QoS, which has peak throughput not set according to the MBR value, then it will be adjusted appropriately and sent back in the UPC response, even if the response contains the NQN (no qos negotiated flag) in the common flags.

Previous Behavior: In case of GGSN, if UPC request is received with a QoS, which has peak throughput not set according to the MBR value and if NQN flag is set in the common flags, UPC response will have the peak throughput same as that received in UPC request.

New Behavior: In case of GGSN, if UPC request is received with a QoS, which has peak throughput not set according to the MBR value and if NQN flag is set in the common flags, then the peak throughput would be adjusted according to the MBR value and only then sent in the UPC response.

Customer Impact: Peak throughput in QoS can be seen changing in UPC response even if NQN flag is set in the UPC request.
CSCus25086 - Incorrect qosNegotiated seen in custom6 GCDR
GTPP Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from GTPP in StarOS 18 software releases.

- GTPP Enhancements for 18.4, page 111
- GTPP Enhancements for 18.2, page 112
- GTPP Enhancements for 18.1, page 114

GTPP Enhancements for 18.4

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.

**CSCux26716 - Not able to specify GTPP data record format on using custom48 dictionary**

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

Data Record Format Version for CDRs

The `gtpp data-record-format-version` CLI command was earlier applicable only to custom24 and custom35 GTPP dictionaries for S-GW. In this release, this command is applicable to all GTPP dictionaries for all products including GGSN, P-GW and SGSN.

**Important** This behavior change is applicable to 18.4.3 and later releases.

**Previous Behavior:** When custom48 GTPP dictionary is used and the `gtpp data-record-format-version` CLI command is configured, the default version number is applied irrespective of the value being configured.

**New Behavior:** The 3GPP version number configured through the `gtpp data-record-format-version` CLI command is encoded in the GTPP request irrespective of the GTPP dictionaries being used.

GTPP Enhancements for 18.2

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.

CSCut20167 - [ePDG] AAAMGR support for Offline Charging (CDR) feature in ePDG

**Applicable Products:** ePDG

**Related CDETS ID** = CSCut20141

Feature Changes

**New GTPP Dictionary to Support ePDG CDRs**

With this release, ePDG supports CDR generation for charging the UEs for their network resource usage. To support the customized charging requirements, a new GTPP dictionary "custom38" has been created for ePDG CDRs based on the standard GTPP dictionary "custom24". The CDRs generated by ePDG node are compliant to 3GPP TS 32.298 V12.6.0.
In ePDG, the accounting mode should be set to GTPP in order to enable the ePDG-CDR generation for the subscribers.

**Performance Indicator Changes**

**IMSA Schema**

The following new bulkstatistic variables are added to this schema in support of ePDG CDRs.

- total-epdgcdr-xmit
- total-epdgcdr-rexmit
- total-epdgcdr-accept
- total-epdgcdr-fail

**show gtpp counters all**

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

- Outstanding ePDG CDRs
- Possibly Duplicate Outstanding ePDG CDRs
- Archived ePDG CDRs
- ePDG CDRs buffered with AAAPROXY
- ePDG CDRs buffered with AAAMGR

**show gtpp statistics**

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

- Total ePDG-CDR transmission
- Total ePDG-CDR retransmission
- Total ePDG-CDR accepted
- Total ePDG-CDR transmission failures
- ePDG-CDR transmission failure percent

**show session subsystem facility aaaproxy all**

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

- Total ePDG-C DRs
- Current ePDG-C DRs
CSCuu25810 - Add AF-Charging-Identifier to new custom CDR dictionary

Applicable Products: P-GW

Feature Changes

New GTPP Dictionary to Support AF-Charging-Identifier AVP

A new GTPP dictionary "custom50" is created based on custom24 to support the AF-Charging-Identifier AVP for the customer to be able to support VoLTE roaming. The fields "aFRecordInformation" and "aFChargingIdentifier" are added to the PGW-CDRs when the AF-Charging-Identifier AVP is received from PCRF.

GTPP Enhancements for 18.1

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.

CSCua96527 - SP WiFi - LMA support for P-GW CDR

Applicable Products: P-GW

Feature Changes

CDR Support for Trusted/Untrusted WLAN

Previous Behavior: Currently there was no CDR support for GTP based WLAN calls (both S2a and S2b).

New Behavior: With this feature, support is provided to generate PGW-CDRs for offline billing purpose for GTP based WLAN calls also. A new GTPP dictionary "custom48" has been added to support the PGW-CDRs generated for GTP based WLAN calls.

For ECS to support offline charging on Gz interface for Trusted WLAN access type, a new field "TWAN ULI" is added to the PGW-CDR. As this an optional parameter, operator can choose whether or not to include the attribute in the CDR. Hence, this attribute is CLI configurable.

Customer Impact: Customers should be aware that CDRs will be generated for WLAN access type.
Command Changes

gtp attribute
A new keyword "twan-uli" has been introduced in this command to control the inclusion of the optional field "TWAN User Location Information" in PGW-CDRs.

configure
  context  context_name
    gtp group  group_name
      | default | no | gtp attribute twan-uli
end

Notes:
• By default, this attribute is disabled.

Performance Indicator Changes

show gtp group all
The following field is newly added to the output of this show command to indicate whether or not the TWAN ULI field is configured.
• TWAN User Location Information present

CSCup88805, CSCur35107, CSCuq08380 - Abnormal bearer termination info in CDR for Customer

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

Feature Changes

Support for Abnormal Bearer Termination Cause in CDR
This feature provides more granular disconnect reasons in CDRs when bearer gets terminated due to abnormal release.

P-GW/S-GW application will provide additional information (disc-reason) with 'abnormalrelease' in 'Delete-Bearer-Indication' and 'Session-Release-Request' to ECS and these information are added to the CDRs.

This additional information will be of type enum and will be added as part of "NAS management extension" in the CDR. This attribute will be populated in PGW-CDR for custom35 dictionary, and SGW-CDR for custom34 and custom35 GTPP dictionaries when the cause for record closing is "Abnormal Release".

The causeForRecordClosing is "Abnormal Release" when a call is dropped because of any one of the following disconnect reasons:
• gtpc-path-failure
• path-failure
• path-failure-s5
• path-failure-s11
• path-failure-s4
• gtpu-err-indication
• gtpu-err-indication-s5u
• gtpu-err-indication-s1u
• gtpu-err-indication-s4u
• gtpu-err-indication-s12
• gtpu-path-failure
• gtpu-path-failure-s5u
• gtpu-path-failure-s1u
• gtpu-path-failure-s4u
• gtpu-path-failure-s12

Previous Behavior: Abnormal Release in CDRs indicated only in cause for record closing.

New Behavior: Detailed disconnect reasons are now included in the NAS management extension part of P-GW/S-GW CDRs for abnormally terminated VoLTE bearers.

Customer Impact: The detailed disconnect reasons will provide the customers the ability to perform gateway/network wide analysis for failures in the network.

CSCuq08380, CSCup88805 - Diagnostic field to be updated in SGWCDR for custom34/35

Applicable Products: S-GW, SAE-GW

Feature Changes

Abnormal Bearer Termination Cause in Diagnostic Field for SGW-CDRs

The reason for abnormal bearer termination is now being included in the S-GW/P-GW CDRs. This information will provide additional visibility to call quality.

The abnormal disconnect reason is added in Diagnostics field of SGW-CDR for custom34 and custom35 dictionaries. The presence of this trigger in the CDR field is CLI controlled.
Command Changes

gtp attribute diagnostics

A new keyword "abnormal-release-cause" has been introduced in this command to indicate the reasons for abnormal bearer termination in VoLTE network.

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute diagnostics [ abnormal-release-cause ]
      | default | no | gtpp attribute diagnostics
    end
end
```

Notes:

• abnormal-release-cause: This keyword controls the inclusion of abnormal bearer termination information in diagnostics field of SGW-CDR. Note that the CLI command "gtpp attribute diagnostics" will disable abnormal-release-cause and enable the diagnostics field. The no gtpp attribute diagnostics command will disable both abnormal-release-cause and diagnostics field.

Important

The Abnormal Bearer Termination feature is currently applicable only to custom34 and custom35 GTPP dictionaries. That is, the bearer termination cause is populated in PGW-CDR for custom35 dictionary, and SGW-CDRs for custom34 and custom35 GTPP dictionaries.

CSCuq15013 - Removing the limitation of one Service Data container per CDR for Customer

Applicable Products: GGSN, P-GW

Feature Changes

Configurable Service Data Container for CDR

Currently the customer-specific GTPP dictionaries "custom38" and "custom39" have restriction of one Service Data Container per CDR. In this release, this restriction is removed and the number of containers per CDR is configurable through the CLI "gtppegcdr losdv-max-containers".

Previous Behavior: Default value of max_losdv was 1 and max_losdv attribute was not configurable for custom38 and custom39 dictionaries.

Default value of max_lotv in gtpp group is 1 and max_lotv is not configurable for custom39.

New Behavior: Default value of max_losdv is 10 and max_losdv attribute is configurable for both custom38 and custom39 dictionaries.

Default value of max_lotv in GTPP group is 8 and max_lotv is now configurable.
**CSCuq51466 - [ECS] Release closure CDRs handling with NPLI feature**

**Applicable Products:** P-GW

**Feature Changes**

**Applying New ULI/Tz across all Bearers**

*Previous Behavior:* If the User Location Information (ULI)/UE Timezone information in the Delete Bearer Command (DBC) / Delete Session Request (DSR) is changed, then the new value of ULI/UE_Tz was not getting reflected in the subsequent CDRs for the remaining bearers of the same PDN.

There were no billing records (Gz/Rf/Gy) triggered for the changed value of ULI/UE_Tz.

*New Behavior:* If the ULI/UE_Tz received as part of DBC/DSR is changed, then the new value is applied to all other bearers.

---

**CSCus30283 - PGW-Gz Redesign Cust35: Cause sequence reversed in PGWCDR**

**Applicable Products:** P-GW

**Feature Changes**

**Cosmetic Change to PGW-CDR Fields**

*Previous Behavior:* The cause code information was printed in the reverse order in the PGW-CDR for GTPP custom35 dictionary.

*New Behavior:* Now the cause code information is printed in the order it is present in Hex Dump for custom35 dictionary.
 CHAPTER 7

HA Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from HA in StarOS 18 software releases.

- HA Enhancements for 18.2, page 119
- HA Enhancements for 18.1, page 120

HA Enhancements for 18.2

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

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

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

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

CSCup91515 - Enhancement for Additional AVPs in MIP Tunnel

Feature Changes

MIP RRQ Enhancement

**Important**  This MIP RRQ is a customer-specific enhancement. For more information, contact your Cisco account representative.

For billing to be done for native and Proxy MIP call based on location information and access technology, the following attributes will be passed on MIP-Registration-Request message from FA to HA.
• IMSI
• BSID
• Subnet-Id
• PCF IP address
• Service Option

Previous Behavior: Supported basic functionality of mobile-ip.
New Behavior: Additional AVPs in MIP RRQ from FA to HA is supported.
Customer Impact: Yes

Command Changes

mobile-ip send

The subnet-id, pcf-address, and service-option keywords have been introduced and the bsid is modified in the mobile-ip send command, under the Subscriber Configuration Mode to support additional MVPs in MIP RRQ from FA to HA.

configure
context context_name
  subscriber { default | name variable }
    mobile-ip send { bsid | custom-2 | subnet-id { custom-2 } | pcf-address { custom-2 } | service-option { custom-2 } }
end

Notes:
• custom-2: Use customer-specific NVSE to send PCF address attribute in the RRQ.

show subscribers configuration username

While displaying subscriber related configuration, if the attribute is configured to send, it will display the NVSE type. Otherwise, it will show as disabled.

• mobile-ip send imsi: Custom-2
• mobile-ip send bsd: Custom-2
• mobile-ip send pcf-address: Custom-2
• mobile-ip send subnet-id: Disabled
• mobile-ip send service-option: Disabled

HA Enhancements for 18.1

This section identifies all of the HA enhancements included in this release:
Feature Changes - new or modified features or behavior changes. For details, refer to the HA Administration Guide for this release.

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

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

CSCur58242, CSCup29785, CSCup56949 - Support for 3G HA stats in show session summary and historical CLIs

Feature Changes

Show Command Enhancements

The current implementation of show session historical command does not provide a breakdown of access technology type. New keywords have been added to this command to display more precise output regarding access technology. The show subscribers CLI commands provides the session information instead of subscriber information. This command has been modified to give more precise output for the subscriber information.

Command Changes

show session counters historical

Following new keywords have been added to the command show session counters historical so that the session information can be displayed as per access-type.

- all
- 2g
- 3g
- 3g-ha
- 4g
- ehrpd
- wifi

show session counters historical { all | arrived | callops | connected | disconnected | failed | handoff | rejected | renewal } | all-intervals | cumulative | graph | incremental | recent-intervals | table | | all | 2g | 3g | 3g-ha | 4g | ehrpd | wifi

Notes:
- all: Displays session counters for all access-types (2g/3g/4g/ehrpd/wifi)
- 2g: Displays session counters for 2G (GERAN, GPRS) calls [GGSN, P-GW/S-GW and S4 SGSN] calls
• **3g**: Displays session counters for 3G (GERAN, GPRS) calls [GGSN, P-GW/S-GW and S4 SGSN] calls
• **3g-ha**: Displays session counters for 3G-HA calls
• **4g**: Displays session counters for 4G (EUTRAN, LTE) calls [P-GW, S-GW] calls
• **ehrpd**: Displays session counters for EHRPD (evolved High Rate Packet Data) calls
• **wifi**: Displays session counters for Wireless LAN (WiFi) calls [P-GW, CGW]

**Performance Indicator Changes**

**show session counters historical**

This command has been modified to support the following new keywords for filtering output by access technologies:

- **all**: display counters for all access technology types
- **2g**: display counters for 2G (GERAN, GRPS) access technology
- **3g**: display counters for 3G (UTRAN, UMTS) access technology
- **3g-ha**: display counters for 3G-HA sessions
- **4g**: display counters for 4G (EUTRAN, LTE) access technology
- **ehrpd**: display counters only for eHRPD access technology
- **wifi**: display counters only for Wireless LAN access technology

When an access technology filter is specified, the output of this command separates session counters by category.

**show session summary**

This new command displays session types by access technology categories. The following information appears in the output of this command:

- **4G LTE (EUTRAN)**
- **2G (GERAN)**
- **3G (UTRAN)**
- **WiFi (WIRELESS LAN)**
- **ehrpd**
- **Others**
- **Total sessions**
- **Active**
- **Dormant**
- **pdsn-simple-ipv4**
CSCup91558, CSCup44069 - EDR enhancement to support NEMO MR Hosts-SM Changes

Feature Changes

Change in Session Manager (SM) for EDR enhancement to Support NEMO MR Hosts

This feature enables creating EDRs with configurable QCI attribute along with NEMO MNP's VRF name, source IP and destination IP tied to a flow. This feature is supported for both single-VRF and multi-VRF.

Important

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Previous Behavior: For a data packet, ECS will see [IP header1] [GRE header] [IP header2] [payload].

New Behavior: Changes were compiled in SM to support the feature. With this feature, ECS will now see only inner IP packets i.e. [IP header2] [payload], and determine the source IP, destination IP and VRF name of the NEMO hosts.
CSCup91558, CSCup4069 - EDR enhancement to support NEMO MR Hosts-SM Changes
CHAPTER 8

HeNBGW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from HeNBGW in StarOS 18 software releases.

- HeNBGW Enhancements for 18.2, page 125

HeNBGW Enhancements for 18.2

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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
CSCul28128 - HeNB-GW: Support for show subscribers henbgw-only ebi | qci.

Performance Indicator Changes

show henbgw session qci
   Below variable is introduced as part of this release:
   • qci

show henbgw session full qci
   Below variable is introduced as part of this release:
   • qci

show henbgw session summary qci
   Below variable is introduced as part of this release:
   • qci

CSCuo65686 - Support R12 CMAS PWS Restart Indication Message

Performance Indicator Changes

henbgw-access schema
   Below variables are introduced to support CMAS PWS restart.
   • s1ap-transdata-wrwreq
   • s1ap-recdata-wrwrsp
   • s1ap-recdata-restartind

henbgw-network schema
   Below variables are introduced to support CMAS PWS restart.
   • s1ap-transdata-wrwresp
CSCuo78931 - HeNBGW MOCN support

MOCN is a network sharing technology that allows different core network operators to connect to a shared radio access network. One HENB can handle more than one core network operator. In this scenario, HENB broadcasts a list of PLMN IDs to UE's. UE's supporting MOCN functionality decode the broadcast system information sent by HENB and are able to select a core network operator as the serving operator within a shared network.

Performance Indicator Changes

show henbgw-access-service henb-association full

New show output variables are introduced for show henbgw-access-service henb-association full

- Supported TAI(s)

show henbgw henb-association full

New show output variables are introduced for show henbgw henb-association full:

- Supported TAI(s)

CSCup47037 - HeNBGW: Default and configured Overload params show support is needed

Feature Changes

Overload parameters show support

Previous Behavior: There was no option "HeNBGW" with "lte-policy" config mode.

New Behavior: Added new option "HeNBGW" introduced in "show lte-policy".

Customer Impact: They can see overload-control and session recovery information with "lte-policy".
**CSCup68855 - HeNBGW support on Virtual Platform (QvPC-DI)**

**Feature Changes**

**Virtual platform support**

With this release, HeNBGW supports QvPC-DI.

**CSCup68867 - HeNBGW support on ASR5500**

**Feature Changes**

**ASR 5500 platform support**

With this release, HeNBGW supports ASR 5500 platform.

**CSCup71541 - HeNBGW Support for X2 proxy**

As part of E-UTRAN architecture a X2 Gateways are deployed to allow the indirect X2-C interface between (H)eNBS

**Feature Changes**

**X2 proxy GW support**

**Command Changes**

A new configuration mode X2-GW Service Configuration Mode is introduced to for X2 Proxy Gateway support. Below are the new commands introduced as part of X2 Proxy Gateway support.

```
bind
  configure
    context context_name
  bind x2-c ipv4-address IPv4_address
  no bind x2-c
end
```
configure
context context_name
x2-c sctp port value
default x2-c sctp port
end

associate x2gw-service

The below command is introduced to support CMAS PWS reset.

configure
context context_name
associate x2gw-service associate_x2gw-service_name context context_name
no associate x2gw-service
end

Performance Indicator Changes

show x2gw-service

This command is introduced as part of X2 Proxy Gateway support.

show x2gw-service { all | enb-association [ all ] | statistics [ sctp | x2ap ] } [ | { grep grep_options | more } ]

CSCuq06852 - HENBGW - Bulkstats var missing for WRWReq WRWResp in access and network

Performance Indicator Changes

henbgw-access schema

Below variables are introduced to support CMAS PWS reset.

• s1ap-transdata-wrreq
• s1ap-recdata-wrresp
• s1ap-recdata-restartind

henbgw-network schema

Below variables are introduced to support CMAS PWS reset.

• s1ap-transdata-wrresp
• s1ap-transdata-restartind
Feature Changes

Handling 10k pws msg

Time when RSP is dispatched

*Previous Behavior:* All rsp will be cumulated and dispatched after configured timeout.

*New Behavior:* A rate limiting function is used, which sends the response before the timeout, if the number of broadcasted IDs in response is > 1000. TAI will be dispatched in batches of 130 IDs. If it is less than 1000, all responses will go after timeout.

*Customer Impact:* None

Duplicate GUMMEI handling

Handling of duplicate GUMMEIs

*Previous Behavior:* When ever duplicate GUMMEI is received from another MME in the same LeNB, SCTP abort will be sent from HeNBGW MGR.

*New Behavior:* When ever duplicate GUMMEI received from another MME in the same LeNB, unusual log message is displayed.

*Customer Impact:* Whenever there is mis-configuration with MME, operator has to correct the configuration.

HeNBGW support on Virtual Platform (QvPC-SI)

Feature Changes

HeNBGW QvPC-SI support

With this release, HeNBGW supports QvPC-SI.
CSCur84827 - HENBGW: Bulkstats support required for PWS Restart message.

Performance Indicator Changes

henbgw-access schema
Below variables are introduced to support CMAS PWS reset.
  • s1ap-transdata-wrwreq
  • s1ap-recdata-wrwresp
  • s1ap-recdata-restartind

henbgw-network schema
Below variables are introduced to support CMAS PWS reset.
  • s1ap-transdata-wrwresp
  • s1ap-transdata-restartind
  • s1ap-recdata-wrwreq

CSCut40006 - HENBGW:DI: drvctrl process in warn state on loading build 18.2.0.59380

With this release this issue is resolved.

CSCut55898 - S1 Full/Partial Reset for MOCN

Command Changes
A new configuration mode X2-GW Service Configuration Mode is introduced to for X2 Proxy Gateway support. Below are the new commands introduced as part of X2 Proxy Gateway support.

s1-reset
This command is introduced as part of s1 Full/Partial Reset for MOCN feature.

configure
    context context_name
henbgw  s1-reset
no henbgw  s1-reset
end
CSCuu12717 - Handling of RESET messages from MME and HENB

Feature Changes

Handling RESET messages from MME and HENB

RESET messages are not forwarded to the peers nodes

Previous Behavior: RESET messages received from HeNB/MME are dropped.

New Behavior: RESET messages received from HeNB/MME is forwarded to the peer nodes.

Customer Impact: No Impact to customers. RESET messages can be disabled.

CSCuu24106 - S1AP Cause based stats based on TAI for MOCN

Feature Changes

TAI for MOCN

TAI Based cause Stats will be maintained at the Access Service level for those S1AP messages which contain the cause IE and unique TAI for which the message is sent can be identified.

Previous Behavior: TAI Based cause Stats will be maintained at the Access Service level for all S1AP messages which contain the cause IE and even if unique TAI that message is intended is not known since a single HENB will serve only one TAI.

New Behavior: Now for those S1AP messages containing cause IE and for those unique TAI cannot be determined TAI based cause Stats will not be maintained. With the support of MOCN in HeNBGW, since a single HENB can serve up to 6 TAI's, we cant maintain TAI level Stats for messages for which the message intended for a particular TAI cannot be known.

Customer Impact: Customer cannot track TAI based cause Stats for messages for which unique TAI the message is intended cannot be known.
HNBGW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from HNBGW in StarOS 18 software releases.

- HNBGW Enhancements for 18.2, page 133

HNBGW Enhancements for 18.2

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

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

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

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

---

**Important**

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

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

**CSCts49192 - ASR5K-HNBGW-00040 - Enhancements to Access Control List (ACL)**

**Feature Changes**

With HNBGW Hybrid and ACL Phase I support HNBGW returns the membership status of the UE with respect to the HNB in the UE Register accept message. Also max length of the list of IMSI (white-list) representing the UEs that can register with an HNB is increased to 150 from 27.

**Command Changes**

```bash
hnb-access-mode closed
```

Below is the new command introduced as part of HNBGW Hybrid and ACL Phase I support:

```bash
configure
  context context_name
    hnb-access-mode closed [ max-registered-ue value ]
  default hnb-access-mode closed
end
```

**Performance Indicator Changes**

```bash
show hnbgw-service
```

`show hnbgw-service hnbgw-svc_name` will show the following output for Closed mode HNB:

- Closed HNB support
- UEs allowed per Closed HNB
- Maximum UEs

`show hnbgw-service hnbgw-svc_name` will show the following output for Hybrid mode HNB:

- Hybrid HNB support
- UEs allowed per Hybrid HNB
- Maximum non-access-controlled UEs
- Maximum UEs
**CSCup01809 - [CBS] Incorrect value of CLI "sabp timer <timer_value>"**

**Feature Changes**

`sabp timer <timer_value>`

- **Previous Behavior:** SABP timer default value - 10 sec, Range - 1 to 300 sec
- **New Behavior:** SABP timer default value - 10 sec, Range - 1 to 30 sec
- **Customer Impact:** None

**CSCup96215 - RTCP enhancements to support RTCP on Iu interface**

**Feature Changes**

**RTCP on Iu interface support**

HNBGW creates another RTCP entity on the Iu-interface between HNBGW and Media-GW. So, there will be two separate RTCP entity per Call, i.e. one on the Iuh-interface and another on Iu-interface. This provides added advantage of MGW independence.

- **Previous Behavior:** HNBGW was supporting RTCP over Iuh interface only.
- **New Behavior:** HNBGW now supports RTCP over Iuh-interface as well as over Iu-interface. These two RTCP-streams are independent of each other.
- **Customer Impact:** None.

**CSCup96781 - HNBAP Configuration transfer procedure support**

**Feature Changes**

**HNBAP Configuration transfer procedure**

HNBGW supports Femto-to-Femto handover using the SRNS-Relocation, which involves the Core-Node entities, and a direct Iurh-based handover, which doesn't involve the Core-Node entities.

For direct IURH connectivity, HNB should know the details of other HNBs to communicate, like the IURH interface IP address. To achieve the same, a new HNBAP procedure HNB Configuration Procedure is added in the specifications. An addition of IURH TNL IP address of HNB in HNBAP HNB registration Procedure helps the HNBGW to build the knowledge of IURH interface IP address of HNBs. And the HNB Configuration Transfer Procedure helps to convey this information to HNBs who require it.
Command Changes

**hnb-config-transfer**

This command **hnb-config-transfer** enables/disables inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

```
configure
   context  context_name
      | default | no | hnb-config-transfer add-inner-ip
end
```

CSCup97007 - Emergency call behavior overhaul

HNBGW already supports emergency calls and provides priority to them. Emergency calls are not subject to Access control checks and restrictions due to congestion control, newcall policy etc. Few changes in behavior of HNBGW with respect to emergency calls and UE registrations are made due to various Internet of Things (IOTs) performed and from interaction with various HNB vendors.

CSCur55959 - 10k UEs per HNB support for HNBGW

Feature Changes

10k UEs per HNB support

New CLIs keyword options are introduced in HNBGW-Service Config Mode to enable HNB Aggregation and specify the maximum number of simultaneously registered UEs to be allowed per HNB-aggregator.

Command Changes

**hnb-aggregation**

New CLIs keyword options **hnb-aggregation max-registered-ues-per-hnb** is introduced in HNBGW-Service Config Mode to enable HNB Aggregation and specify the maximum number of simultaneously registered UEs to be allowed per HNB-aggregator.

```
configure
   context  context_name
      hnb-aggregation max-registered-ues-per-hnb value [-noconfirm]
      | no | default | hnb-aggregation [-noconfirm]
end
```
Performance Indicator Changes

show configuration

The show commands in this section are available in support of the Configuring 10K UE Support. show configuration will show the following output if hnb aggregation is enabled:

- hnb-aggregation max-registered-ues-per-hnb

show configuration will show the following output if hnb aggregation is disabled:

- hnb-access-mode open max-registered-ue
- hnb-access-mode hybrid max-non-access-controlled-ue
- hnb-access-mode hybrid max-registered-ue

show configuration verbose

show configuration verbose will show the following output regardless of the value of hnb-aggregation:

- hnb-access-mode closed max-registered-ue
- hnb-access-mode open max-registered-ue
- hnb-access-mode hybrid max-non-access-controlled-ue
- hnb-access-mode hybrid max-registered-ue
- hnb-aggregation max-registered-ues-per-hnb

show hnbgw-service all

show hnbgw-service all will show the following output if hnb aggregation is enabled:

- hnb-aggregation max-registered-ues-per-hnb

show hnbgw-service all will show the following output if hnb aggregation is disabled:

- hnb-access-mode open max-registered-ue
- hnb-access-mode hybrid max-non-access-controlled-ue
- hnb-access-mode hybrid max-registered-ue
CSCur79073 - F2F SRNS relocation fails due to access control failure for emergency IU

**Feature Changes**

**Relocation failure due to access control failure**

Emergency behavior changed in SRNS relocation.

**Previous Behavior:** If HNBGW gets a Relocation Request message from CN with IMSI present, it registers the UE as Normal UE. Here if we have an emergency UE relocating, it is registered as Normal in tHNB, and hence is subject to access-control-checks, license checks, etc, and relocation may be dropped if any of these fails.

**New Behavior:**

- During F2F SRNS relocation, we establish the UE and IU in tHNB according to the Registration types in sHNB.
- During SRNS relocation, if a normal UE containing 1 or more emergency IUs fails access control checks in tHNB, we change the UE-type to emergency. If this UE contains any normal IU, the IU is disconnected after we received Reloc-Complete for it.
- Hidden CLI in hnbgw-global: additional-emergency-ues, to configure the % of extra emergency UEs to be allowed per HNB.

**Customer Impact:** None

CSCut18057 - [16.1.7] CLI o/p is not correct when phase2/3 timers are disabled

**Feature Changes**

**CLI Output when Phase 2/3 timers are disabled**

**Previous Behavior:**

- Page last known HNB timeout: 0 Secs
- Paging Grid Fanout timeout: 0 Secs
- Paging Area Fanout timeout: 0 Secs

**New Behavior:**

- Page last known HNB timeout: Disabled
- Paging Grid Fanout timeout: Disabled
- Paging Area Fanout timeout: Disabled
Customer Impact: Instead to paging value as "0Secs" they will see it as "Disabled", if a paging phase is disabled.

CSCus25924-[18.0] HNB accept msg is coming with different Cell-access-mode in ACL

Feature Changes

Accept msg is coming with different Cell-access-mode in ACL

Previous Behavior: Reject the whitelist if the access mode is not same in all occurrences of white-list in AAA message.

New Behavior: Access mode is picked only from the first occurrence of whitelist in AAA Accept message, and it is ignored in subsequent occurrences of whitelist in the same message from AAA

Customer Impact: None.
CSCus25924 -[18.0] HNB accept msg is coming with different Cell-access-mode in ACL
HSGW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from HSGW in StarOS 18 software releases.

- HSGW Enhancements for 18.2, page 141

HSGW Enhancements for 18.2

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

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

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

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

Important

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

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements


- **SNMP MIB Enhancements**
- **System and Platform Enhancements**

**CSCut74593 - MEID in PBU**

**Feature Changes**

**Hardware ID Support in Proxy Binding Update (PBU) Messages**

The changes related to functionality will be in the MAG driver module.

**MAG Driver:**

- The MAG driver encodes the MEID extensions and decodes at LMA.
- The MEID is maintained at the driver call line level.
- MEID is informed during initial-call/Re-reg/De-reg.
- The MEID is recovered along with the driver callline.

**Previous Behavior:** Hardware id mobility option was not supported for `information element set custom2` in mag-service.

**New Behavior:** Hardware ID mobility option is now supported with the configuration of `information element set custom2` in mag-service in PBU messages (Reg, Re-reg, De-reg) from MAG to LMA. Also, it is now possible to only disable the hardware-id mobility option in PBU with the configuration `information element set custom2 disable-ie hardware-id` in mag-service.

If a MEID is not available in the initial registration and a MEID is sent in a re-registration, then the message should be sent to the LMA.

---

**Important**

When the feature is disabled and the MAG receives a "MEID" option in the PBU, then the PBU should be forwarded to the LMA without a MEID.

**Command Changes**

`information-element-set`

New keywords `disable-ie` and `hardware-id` are added to disable information elements in PBU and disable the hardware ID in PBU.

`configure`

```
context mag_context_name -noconfirm
  mag-service mag_service_name -noconfirm
    information-element-set custom2 [ disable-ie hardware-id ]
end
```

**Notes:**
• When **information-element-set custom2** is enabled, all of the supported mobility options are enabled including hardware ID for a specific customer.

• The above **disable-ie** keyword only disables the hardware ID mobility option in PBU.

---

**Important**

The **hardware-id** mobility option format is supported like **custom1**.

---

**Performance Indicator Changes**

**show configuration**

This show command has been updated to display the disable IE list if **custom2** and **hardware-id** is configured.

**show configuration context mag**

This show command has been updated to display the disable IE list if **custom2** and **hardware-id** is configured.

**show lma-service session full**

This show command already supports displaying the MEID value.

**show mag-service all**

This show command has been updated to display the disable IE-list if **custom2** and **hardware-id** is configured.
MME Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from the MME in StarOS 18 software releases.

Corrections have been made to the following items:

- In the section for 18.2, please check revised content for:
  - CSCus96030
  - CSCup66691, CSCuq25983

- MME Enhancements for 18.5, page 145
- MME Enhancements for 18.4, page 153
- MME Enhancements for 18.2, page 157
- MME Enhancements for 18.1, page 165

MME Enhancements for 18.5

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**
**CSCuv27053 - Purge-request towards only one HSS after sessmgr crash**

**Feature Changes**

**Purge Request Behavior**

**Previous Behavior:** After a Session Manager recovers from a crash, the MME sends the Purge Request to the default home HSS identified in the MME service configuration for any UE (homer or roamer) that had detached.

**New Behavior:** After a Session Manager recovers from a crash, the MME sends the Purge Request to the default home HSS identified in the MME service configuration for any IMSI (homer) that had detached. The MME does not send any Purge Requests for detached roamer IMSIs post session recovery.

**CSCuw29857 - M-TMSI Allocation algorithm enhancement**

**Feature Changes**

**P-TMSI/M-TMSI Allocation Algorithm Enhancements**

**New Behavior:**

The MME's algorithm for generating M-TMSI has been modified. The change helps increase the number of uniquely mapped P-TMSIs to avoid possible P-TMSI overlapping during handovers during IRAT changes. The MME dynamically determines the size of the local ID based on the platform: 21-bit local ID for the M-TMSI on ASR5K/ASR5500(DPC)/SSI and 19-bit local ID in M-TMSI for ASR5K (DPC2) and VPC-DI.

**Customer Impact:**

This will increase the unique number of P-TMSI IDs allocated by the MME, resulting in a reduction of collisions during IRAT changes.
Feature Changes

Operator Policy Selection Based on IMEI-TAC

Operator policies (proprietary Cisco functionality) empower the carrier/network operators to configure preferred call handling controls not typically used in all applications and to determine the granularity of the implementation of any operator policy; to groups of incoming calls or simply to one single incoming call.

Previous Behavior: The MME selects an operator policy to guide call handling based on the UE's international mobile subscriber identity (IMSI) and PLMN-ID.

New Behavior: Now, the MME can select/re-select an operator policy based on the UE's IMSI or based on the UE's unique international mobile equipment identity - type allocation code (IMEI-TAC). Including the type allocation code (TAC) in the operator policy selection process results in the network access restrictions based on the type of wireless device as identified by the TAC.

This IMEI-TAC-based selection functionality is configured with the new command changes (see Command Changes below) then, except for emergency calls, the MME will select/re-select the operator policy whenever the MME retrieves the IMEI or IMEI-SV in one of the following scenario:

- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Identity-Request with IMEI.
- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (policy attach imei-query-type under MME service must be enabled).
- normal 4G TAU when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (policy tau imei-query-type under MME service must be enabled).
- inbound handover when IMEI/IMEI-SV is received with IMSI via the Forward-Relocation-Request.
- S10 and S3 Attaches when IMEI/IMEI-SV is retrieved with IMSI via EGTP-Identification-Request.
- Inter-RAT TAU and Intra-RAT TAU with MME change when IMEI/IMEI-SV is received with IMSI in Context-Response.

Command Changes

precedence

Important

The operator policy(s) and call control profile(s) must first be configured according to the instructions in the section on Operator Policy in the MME Administration Guide.
To setup IMEI-TAC based operator policy selection, use the new `imei-tac` keyword to configure either a particular IMEI-TAC value or a range of IMEI-TAC values as matching criteria. As well, associate an operator policy and assign an order of precedence for this IMEI-TAC value or range.

```
configure
  lte-policy
  subscriber-map map_name
    precedence precedence_number match-criteria imei-tac { range start_tac_value to end_tac_value | value tac_value } operator-policy-name policy_name
    no precedence precedence_number
  end
```

Notes:

- `tac_value` is an 8 digit number that identifies a specific type allocation code. The TAC, the first eight digits of the 15-digit IMEI or 16-digit IMEI-SV, identifies the equipment manufacturer, the device type and the model number (if there is one).

---

**CSCux04060 - Non-delivery of Modify Bearer Msg leads to loss of PDN**

**Feature Changes**

**NAS-NON-DELIVERY for Modify Bearer Msg**

By default, the MME suspends a modification procedure when NAS-NON-DELIVERY is received from the eNodeB in response to the MME's MODIFY EPS BEARER CONTEXT REQUEST with cause X2-HO triggered or S1-HO triggered. The MME does not restart a suspended modification procedure to send UPDATE BEARER RESPONSE to the PGW when PATH SWITCH REQUEST is not received from the target eNB or when HANDOVER REQUIRED is not received from the source eNB. Such a suspension leads to the deletion of bearers and detaching of the UE.

It is now possible to configure a new MME timer to instruct the MME to resume a suspended modification procedure to avoid detaching UE in the noted scenario.

**Command Changes**

```
policy
```

A new configurable "modify-procedure-timer" instructs the MME to resume a modification procedure that has been suspended due to reception of NAS-NON-DELIVERY with cause X2-HO/S1-HO triggered.

If configured, the new timer starts when NAS-NON-DELIVERY is received for EPS MODIFY BEARER CONTEXT REQUEST with cause X2-HO/S1-HO triggered and the timer stops if HANDOVER REQUIRED or PATH SWITCH REQUEST is received prior to expiry.

Upon expiry of the new timer the suspended procedure is resumed to complete the modification procedure and the MME sends UPDATE BEARER RESPONSE with cause.
EGTP_CAUSE_TEMP_REJECTED_DUE_TO HO_IN PROGRESS without re-trying EPS Modify Bearer Context Request to the eNB.

```
configure context context_name
  mme-service service_name
  policy nas-non-delivery
modify-procedure-timer seconds
end

configure context context_name
  mme-service service_name
  no policy nas-non-delivery
modify-procedure-timer end
```

- **no** - Disables the timer configuration.
- **seconds** - Enter an integer from 1 through 100 to enable the timer and to define the number of seconds the MME waits before resuming the modification procedure that has been suspended in response to receipt of a NAS_NON_DELIVERY for an EPS_MODIFY_BEARER_CONTEXT_REQUEST with cause X2/S1 HO triggered.

### CSCux13166 - MME releases UE context with Category NAS Unspecified for non-TAU

#### Feature Changes

**Previous Behavior:** By default, an MME initiated the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME received a TAU Request over Initial-UE if the UE was in the connected state.

CLI was available which allowed the operator to specify the cause code mapping for MME-initiated S1-UE-CONTEXT-RELEASE whenever the MME received a TAU over Initial-UE message from the eNodeB.

**New Behavior:** Now by default, the MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a request over Initial-UE (for all TAU and non-TAU scenarios such as Service Request, Attach, and Extended-Service-Request), if the UE is in the connected state.

The existing CLI has been modified to enable the operator to specify the cause code mapping for the MME-initiated S1-UE-CONTEXT-RELEASE whenever the MME receives an Initial-UE request message from the eNodeB, irrespective of the procedure if the UE is in the connected state. CLI changes are explained in the following section.

#### Command Changes

`s1-ue-context-release`

The original `init-ue-from-enodeb-for-tau` keyword name and functionality have been modified. The new keyword is `init-ue-from-enodeb`. New functionality allows the MME to send the configured cause code
mapping in the MME-initiated UE-CONTEXT-RELEASE in response to *any unexpected procedure* over Initial-UE from the eNodeB, such as TAU, Service Request, Extended Service Request, Attach Request.

**Important**

In support of backward compatibility, the MME will accept configurations with either form of the keyword. When the operator explicitly saves the configuration, the configuration will save using the new form of the keyword.

```
class configure

context context_name

  mme-service service_name

  s1-ue-context-release reason init-ue-from-enodeb cause type { nas_value nas_value | radio_value }

default s1-ue-context-release reason init-ue-from-enodeb cause

end
```

Notes:

**Important**

*service_name* must be unique across all contexts.

- The configured cause code will be sent in the UE-CONTEXT-RELEASE message whenever the MME releases the existing S1AP connection in response to unexpectedly receiving an Initial-UE message for any procedure such as TAU, Service Request, Extended Service Request, Attach Request.
- Currently, the only release reason possible is *init-ue-from-enodeb*.
- There are two cause options for which cause code values can be assigned:
  - *nas value nas_value* options are:
    - 0 - Normal Release (default value)
    - 1 - Authentication Failure
    - 2 - Detach
    - 3 - Unspecified
    - 4 - CSG Subscription Expiry
  - *radio value radio_value* must be an integer from 0 to 38.

**CSCux26819 - MME should intimate dedicated bearer its default bearer will be deleted**

**Feature Changes**

**Previous Behavior:** The MME does not support dedicated bearer cleanup so that the eNB is informed when a Default Bearer Release Request is sent from an eNB.
Also, when the MME receives a RAB Release Response (from the eNB) that includes an unknown eRAB-ID, then an S1-App Error Indication is generated by the MME.

**New Behavior:** Modifications have been made such that the MME now supports dedicated bearer cleanup so that the eNB is informed when a Default Bearer Release Request is sent from an eNB.

**Customer Impact:** Reduced number of S-1App Error Indications.

### CSCux33388, CSCur41900 - CLI Control for Target Access Restriction

CSCux33388 - InterSGSN 3G to 2G HO fails
CSCur41900 - Rollback Behavior in EPC during TAU/RAU Needs to be Corrected

#### Feature Changes

**Target Access Restriction**

Target Access Restriction feature was added to the SGSN and MME in release 17.4. The purpose of this feature is to avoid rollback behavior that exists in RAU and TAs by checking target RAT Type IE present in the Context Request at the source node, and then rejecting the TAU/RAU based on the subscriber's ARD profile earlier in the cycle if the target RAT is restricted for the subscriber. Rollback behavior caused late TAU/RAU rejection, resulting in PDP/bearer deletion for the MME, PGW, and the SGSN, requiring the UE to reattach and reactivate lost PDP/bearer.

**Previous Behavior:** As a part of this functionality, the target access restriction feature instructs the source-SGSN or the source-MME to reject outbound RAU when the target access was restricted for the subscriber. Rejection was performed without checking "access-restriction-data no-check" in the call control profile configuration.

**New Behavior:** With release 17.6.1, a new command keyword `target-access-restriction` has been introduced to the call control profile configuration to control (enable/disable) target access restriction functionality. Target access restriction is now disabled by default on both the SGSN and the MME. Refer to the Command Changes section below for the command information to enable/disable this functionality.

The default behaviors for the SGSN and the MME now differ:

- **New Behavior for the MME only:** "target-access-restriction" keyword configuration will control the target access restriction feature for the MME without other consideration:
  
  - **No Rejection:** if "target-access-restriction" is not enabled, then the source-MME will not reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
  
  - **Rejection:** if "target-access-restriction" is enabled, then the source-MME will reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

- **New Behavior for the SGSN only:** "target-access-restriction" keyword configuration enables/disables the target access restriction feature. The SGSN also considers "access-restriction-data no-check" in the call control profile configuration prior to rejecting outbound RAU when target access restriction
functionality is enabled. The SGSN's target access restriction behavior is dependent upon the SGSN's "access-restriction-data no-check" configuration:

◦ **No Rejection**: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

◦ **Rejection**: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will ignore the "target-access-restriction enabled" configuration and the source-SGSN will reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

### Command Changes for the MME

**access-restriction-data**

With release 17.6.1, the MME has access to this command in the call-control-profile configuration mode. The new keyword `target-access-restriction` enables or disables rejection of the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

```plaintext
configure
call-control-profile ccp_name
  access-restriction-data target-access-restriction
  remove access-restriction-data [ target-access-restriction ]
end
```

**Notes:**

- Including the `target-access-restriction` keyword with the command enables the target access restriction feature.
- Including the `remove` command filter disables the target access restriction feature. Inclusion of the `target-access-restriction` keyword in the remove command is currently optional.

### Command Changes for the SGSN

**access-restriction-data**

With release 17.6.1, the new keyword `target-access-restriction` enables or disables the Target Access Restriction feature.

```plaintext
configure
call-control-profile ccp_name
  access-restriction-data [ eutran-not-allowed | failure-code | no-check | target-access-restriction
  access-restriction-data no-check
  remove access-restriction-data [ target-access-restriction ]
end
```

**Notes:**
• Including the **target-access-restriction** keyword with the command enables the target access restriction feature.

• With the target access restriction feature enabled, including the **no-check** keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

• Including the **remove** command filter with the **target-access-restriction** keyword disables the target access restriction feature.

• With the target access restriction feature enabled, including the **remove** command filter with the **no-check** keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

### Performance Indicator Changes

**show call-control-profile**

The Target Access Restriction field will display in the output with Enabled or Disabled and it will appear similar to the following:

```
[local]test# show call-control-profile full name ccprof1
...
Authentication Detach : Not configured
Regional Subscription Restriction Failure Code Value : 13
ARD-Checking : Enabled
ARD Failure Code : Disabled
Access Restriction Data : EUTRAN Allowed
Target Access Restriction : Enabled
Zone-Code Check : Enabled
...
```

**show configuration verbose**

The access-restriction-data target-access-restriction field displays in the output without the "remove" prefix to indicate it is Enabled or with the "remove" prefix to indicate the feature is Disabled. The output will appear similar to the following when the feature is enabled:

```
[local]test# show configuration verbose
...
call-control-profile ccprof1
remove rau-inter ctxt-xfer-failure
   no subscriber-control-inactivity
...
   access-restriction-data target-access-restriction
...
```

### MME Enhancements for 18.4

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

**Feature Changes** - new or modified features or behavior changes. For details, refer to the *MME Administration Guide* for this release.
Command Changes - changes to any of the CLI command syntax. For details, refer to the ASR 5x00 Command Line Interface Reference for this release.

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

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

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

CSCuu94088, CSCuu87580 - A-MSISDN / MSIM for VoLTE

Feature Changes

A-MSISDN Flag Support in Features List AVP for ULR

These changes to the MME behavior are in compliance with 3GPP TS 3GPP 29.274 v11.10.0

Previous Behavior: The MME did not set the Additional-MSISDN (A-MSISDN) flag in the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time of UE attaches.

New Behavior: Now it is possible to configure the MME to set the A-MSISDN flag in the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time of UE attaches. Configuration information is identified in the Command Changes section below.

If the MME indicates support of the A-MSISDN feature in ULR messages and if A-MSISDN is available in the subscription data, then the HSS sends the provisioned A-MSISDN together with the MSISDN in Update Location Answer (ULA) and in / Insert-Subscription-Data-Request (ISDR) messages. The MME receives the A-MSISDN as Correlation MSISDN (C-MSISDN) and sends the information in SRVCC PS-to-CS Request and in Forward Relocation Request messages to the HSS.
Customer Impact: This new configurable behavior makes it possible to use A-MSISDN as C-MSISDN during SRVCC PS to CS handover.

Command Changes
diameter update-dictionary-avps

Use the new 3gpp-r11 keyword to instruct the MME to support AVPs defined by 3GPP 29.274 v11.10.0 which will allow MME to support use of A-MSISDN information sent in the Feature List AVP for ULR.

configure
  context context_name
  hss-peer-service service_name
    diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }
    no diameter update-dictionary-avps
  end

Notes:

• no Sets the command to the default value where Release 8 ('standard') dictionary is used for backward compatibility of previous releases.

• 3gpp-r11 Configures the MME to support signaling additional AVPs to an HSS in support of Release 11 of 3GPP 29.272. Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile Station ISDN (A-MSISDN) flag of the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time a UE Attaches.

a-msisdn

Use this new command to enable the MME to advertise A-MSISDN functionality support to the HSS.

configure
  call-control-profile profile_name
    a-msisdn
    remove a-msisdn
  end

Notes:

• remove Disables support for A-MSISDN functionality and returns the MME to default state.

• a-msisdn Enables the MME to notify the HSS of support for Additional-MSISDN for the PLMN associated with this call-control profile.

• Configure the 3GPP R11 support with the diameter update-dictionary-avps command in the HSS Peer Service configuration mode to complete the configuration required to support A-MSISDN.

Performance Indicator Changes

show call-control-profile full all

Use the output of this command to verify the configuration status of the A-MSISDN functionality:

Call Control Profile Name = cp1
  SAMOG Web-Authorization Multiple Device Support : NO
CSCuv53725, CSCuv14176 - Enforce License for SBc

Feature Changes

SBc License Enforced

With this release, an SBc interface feature license is enforced. The license controls access to the commands that configure the SBc interface parameters for the MME.

**Previous Behavior:** A feature license was not required to access and configure the commands in the SBc service configuration mode or to use `associate sbc-service` in the MME service configuration mode.

**New Behavior:** Beginning with Release 18.4, a valid feature license is required to access and use the following commands in the SBc service configuration mode:

- `associate`
- `bind`
- `cbc-associations`
- `sbc-mme`

As well, without the SBc license, it is not possible to associate an SBc service with an MME service using the `sbc-service` keyword and the `associate` command in the MME service configuration mode.

**Customer Impact:** If interested in SBc functionality, please contact your Cisco Representative to obtain a feature license for SBc.

CSCuv73207 - MME not compliant with 3GPP 24.301 CR 2098

Feature Changes

**Cause Code in Attach Reject when EPS Subscription Not Present**

**Previous Behavior:** EMM cause code #19 (ESM failure) and ESM cause as #8 are sent in the Attach Reject when the subscriber does not have an LTE/EPS subscription.

**New Behavior:** EMM cause code #15 (No suitable cells in tracking area.) and ESM cause as #31 are sent in the Attach Reject when the subscriber does not have an LTE/EPS subscription. The significant change is the change of EMM cause code as the ESM cause can be anything as long as the EMM cause code is not #19.

**Customer Impact:** Reduced signaling between UE and MME because the UE does not retry the Attach.
Performance Indicator Changes

MME Schema

A new counter helps the operator to track Attach Rejects due to the subscriber not having an EPS subscription:

- **emmdisc-noepssubscription**
  - **Description:** Total number of 4G Attaches rejected because the subscriber did not have an EPS subscription.
  - **Triggers:** Counter increments when a subscriber without a subscription for 4G packet-oriented services tries to Attach to the MME.
  - **Availability:** per MME service
  - **Type:** Counter
  - **Data Type:** Int32

CSCuw17197 - PLA dropped by DRA when sent from another PSC card

Feature Changes

**PLA and PLR Using Same Connection**

**Previous Behavior:** When the MME received a Provide Location Request (PLR) on one connection (e.g., PSC-a), if the MME is maintaining a subscriber session on another connection (e.g., PSC-b) then the MME sends the Provide Location Answer (PLA) incorrectly via the maintained connection (i.e., PSC-b).

**New Behavior:** The MME now sends the PLA via the same diamproxy connection (i.e., card) through which the PLR is received.

MME Enhancements for 18.2

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

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

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

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

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

CSCug17478, CSCui29064 - Support for Mis-Spelled APN Name Correction

Feature Changes

Default APN for DNS Failures

Previous Behavior: The MME discontinued support of configurable default APN with a "require-dns-fail-wildcard" option because

- in 2G/3G, there is no default-APN option available in the HLR's subscriber profile,
- however, in LTE, a default-APN setting is included in the UE Subscription Data returned from the HSS via the Update_Location_Response.

Therefore, configuring a default APN option on the MME was deemed unnecessary.

New Behavior: With Release 18.2, allowing the operator to configure a default APN option on the MME is deemed useful. Now, the MME allows the operator to configure the use of a default APN when DNS resolution fails for the subscriber-requested APN, when the subscriber-requested APN is not present in the subscription record and wildcard subscription is present in the subscription record. The operator can configure use of a default APN with the require-dns-fail-wildcard CLI keyword, so the MME retries the DNS query and proceeds with activation.

Customer Impact: The operator can ensure that calls and PDP context activation are not rejected because of possible UE errors, such as, the UE requested a misspelled APN name.
Command Changes

apn-selection-default

The MME can now use the existing CLI keyword, require-dns-fail-wildcard, to enable use of a default APN when there is a wildcard subscription in the subscription record and there is a situation where the DNS query fails to resolve with the UE-requested APN.

Configuration of this default APN functionality is done in the APN Remap Table configuration mode.

configure
   apn-remap-table table_name
   apn-selection-default network-identifier net_id require-dns-fail-wildcard
   no apn-selection-default network-identifier net_id require-dns-fail-wildcard
   end

Notes:

• no prefix included with the command disables the use of a default APN in situation where the DNS query fails due to a problem with the UE-requested APN.

• By default, the default-APN functionality is not enabled.

Performance Indicator Changes

show apn-remap-table full all

This command displays the status of the default APN configuration, for example:

[local]asr5000# show apn-remap-table full all
APN Remap Table Name        : test-table
Default APN                   : star.com
Require Subscription APN      : Not Configured
Use Default APN when no APN is requested : Yes
Use Default APN when DNS Query fails : Yes
Fallback APN to use when Default APN not present in subscription : Not Configured

CSCus24510 - MME support for EMERGENCY_CALL_RELEASE event in lcs service

Feature Changes

MME Notifies GMLC of Emergency Call Release

Important This functionality was initially available in 17.3 as Lab Quality but in Release 17.3.2 it was made available as fully qualified Deploy Quality.
The call release event enables the GMLC to clear the cache for existing calls and to correctly log the duration of an emergency call. Without call release facilitating the clearing of the cache, the location platform could send the old (erroneous) location information in response to a new location request for an E-911 call.

**Previous Behavior:** The GMLC was not notified when the MME performed an Emergency Call Release as part of a location service procedure.

**New Behavior:** In compliance with 3GPP TS 29.172, the MME LoCation Services (LCS) feature supports sending the EMERGENCY_CALL_RELEASE event in a subscriber location report (SLR) request message, to the GMLC to notify the GMLC of the call release, when an emergency call is released or when an emergency PDN is disconnected at the MME.

Note, this is not configurable functionality.

**Customer Impact:** Notifying the GMLC of the emergency call release event allows the GMLC to delete all information previously stored for the emergency call in accordance with regulations.

---

**CSCus32031 - Separate Authentication Message routing from MME to AuC**

**Feature Changes**

**Additional Routing for Authentication Messages from MME to AuC**

**Previous Behavior:** Currently, all S6a/S6d messages (AIR, ULR, Notify, CLR) are routed to a peer that has been configured as the originating Diameter HSS endpoint for the HSS peer service. This configuration creates a Diameter-based S6a or S6d (SGSN) interface association to provide AAA functionality.

**New Behavior:** The `diameter hss-endpoint` command (see below) in the HSS peer service configuration mode now gives the operator the option to create routing to a different set of endpoint HSS servers - authentication centers (AuC). This AuC-endpoint routing can be used to send only a specific message type, the Authentication-Information-Request (AIR) messages, to the AuC.

If this optional AuC-endpoint functionality is not enabled, then AIRs are routed, along with all other S6a/S6d messages, to the configured HSS server endpoint.

**Command Changes**

```
diameter hss-endpoint
```

A new keyword option, `auc-endpoint`, has been added to this command to enable the operator to define endpoint routing to an authentication center.

```
configure
  context  context_name
  hss-peer-service  service_name
    diameter hss-endpoint  endpoint_name | eir-endpoint | eir_endpoint_name | auc-endpoint | auc_endpoint_name
  end
no diameter hss-endpoint
end
```

Notes:
• **auc-endpoint** Including this keyword option enables routing to an authentication center (AuC) as the endpoint in place of the hss-endpoint. If configured, all AIR messages are routed to this AuC-endpoint. If not configured, all AIR messages are sent to the configured HSS endpoint. **auc_endpoint_name** Must be a unique endpoint name comprised of a string of 1 to 63 alphanumeric characters.

• It is possible to configure either or both optional endpoints with the same command entry.

• Reminder: The configuration of the auc-endpoint is only valid when all necessary endpoint configuration has been completed. This auc-endpoint must also be defined as a valid endpoint using the commands in the Diameter Endpoint configuration mode (refer to the appropriate chapter in the *Command Line Interface Reference* manual).

• **no diameter hss-endpoint** Disables all Diameter HSS endpoint configuration entries for the HSS peer service.

**Performance Indicator Changes**

**show hss-peer-service service all**

This command generates a display of the configuration for the HSS peer service, including names of any configured Diameter hss, eir, or auc endpoints. The following is an example of what could be generated:

```
[local]asr5000# show hss-peer-service service all
Service name : hss1
Context : plmn1
Status : STARTED
Diameter hss-endpoint : s6d
Diameter eir-endpoint : n/a
Diameter auc-endpoint : AuC1
```

**CSCus96030 - CSFB support for CDMA Network enhancements - lab quality**

**Feature Changes**

---

**Important**

In a previous release of this document, this feature was incorrectly referred to as eCSFB. The correct feature identification is CSFB for 1XRTT.

---

**CSFB for 1XRTT**

---

**Important**

This functionality is released as Trial/Test Quality and should only be used in a test environment.

The primary purpose of enhanced CSFB for 1XRTT is to take the CDMA2000 messages received from the UE and relay them to the MSC (or vice-versa) through S1-APP and S102 interfaces.

With the 18.0 release, the MME expanded support of circuit-switched fall back (CSFB) to include enhanced circuit-switched fall back for CDMA 1x (single-carrier) radio transmission technology (RTT) networks. The
MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWF/MSC to support the following CS services:

- MO/MT Voice calls
- MO/MT SMS
- Emergency calls

With release 18.2, the commands to configure and manage the S1-APP and the S102 interface are now license controlled. Speak with your Cisco Representative for information about this license.

**Command Changes**

**Performance Indicator Changes**

**S102 Schema**

A new bulk statistics schema has been created and it currently includes the following variables:

- vpnname
- vpnid
- servname
- servid
- s102ap-tx-a21-air-signal-msg
- s102ap-tx-a21-ack-msg
- s102ap-tx-a21-evt-ntfy-msg
- s102ap-tx-unknown-msg
- s102ap-retx-a21-air-signal-msg
- s102ap-retx-a21-ack-msg
- s102ap-retx-a21-evt-ntfy-msg
- s102ap-retx-unknown-msg
- s102ap-rx-a21-air-signal-msg
- s102ap-rx-a21-ack-msg
- s102ap-rx-a21-evt-ntfy-msg
- s102ap-rx-unknown-msg
- s102ap-encode-errors
- s102ap-missing-mandatory-ies
- s102ap-corelation-mismatch
- s102ap-decode-errors
CSCut68757 - Need support of 'Change to Report Flags' IE in EGTP

Feature Changes

'Change to Report Flags' IE

3GPP has introduced 'Change to Report Flags' in 29.274 for delayed reporting of change of SN/TZ during inter-CN node mobility.

New Behavior: The MME now supports the 'Change to Report Flags' IE which reports changes of serving network or UE time zone in Forward Relocation Request or Context Response messages.

Inclusion of the 'Change to Report Flags' IE is not CLI controlled (enabled/disabled). Serving Network / UE Time Zone IE is automatically included on the S4/S11 interface during a TAU/RAU/Handover with MME change, if the source MME supports NITZ (network identity and time zone) which enables the MME to set the SNCR/TZCR bit in the Change to Report Flags IE in the Forward Relocation Request or Context Response message.

CSCuu02102 - eSRVCC Implementation for 1XRTT

Feature Changes

eSRVCC for CDMA

Important

This functionality is released as Trial/Test Quality and should only be used in a test environment.

The MME already supports single radio voice call continuity (SRVCC) for UTRAN/GERAN. With this release, the MME has expanded support to enhanced SRVCC (eSRVCC) for CDMA 1x (single-carrier) radio transmission technology (1x-RTT) networks.

The primary purpose of eSRVCC - SRVCC for 1xRTT - is to enable a VoLTE UE to move between LTE and 3G/UMTS or 2G/GSM coverage areas with smooth handovers so that CDMA2000 messages are received from the UE and then relayed to the MSC (or vice-versa) through S1-AP and S102 interfaces.

The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWF/MSC to support the following CS services:

- MO/MT Voice calls
- MO/MT SMS
- Emergency calls
The commands to configure and manage the S1-AP and the S102 interfaces are license controlled. Speak with your Cisco Representative for information about this license.

**Command Changes**

**Performance Indicator Changes**

**S102 Schema**

This new schema includes the following variables

- `vppname`
- `vppid`
- `servname`
- `servid`
- `s102ap-tx-a21-air-signal-msg`
- `s102ap-tx-a21-ack-msg`
- `s102ap-tx-a21-evt-ntfy-msg`
- `s102ap-tx-unknown-msg`
- `s102ap-retx-a21-air-signal-msg`
- `s102ap-retx-a21-ack-msg`
- `s102ap-retx-a21-evt-ntfy-msg`
- `s102ap-retx-unknown-msg`
- `s102ap-rx-a21-air-signal-msg`
- `s102ap-rx-a21-ack-msg`
- `s102ap-rx-a21-evt-ntfy-msg`
- `s102ap-rx-unknown-msg`
- `s102ap-encode-errors`
- `s102ap-missing-mandatory-ies`
- `s102ap-correlation-mismatch`
- `s102ap-decode-errors`
- `s102ap-syntax-errors`
- `s102ap-misc-errors`
MME Enhancements for 18.1

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

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

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

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

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

**CSCtx81747 - MME Integration to IPNE to activate Location Report Procedures**

This feature, with its CLI commands, counters, and statistics, are all under development for future use and are not yet fully qualified.

**Feature Changes**

**IPNE Service Support**

The MME now supports IP Network Enabler (IPNE), a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. The MINE cloud
service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services.

With support of the IPNE interface and IPNE Service, the MME is able to export the following information to the CSB (Cisco Service Bus):

- UE Location Information
- UE Mobility Information

This functionality makes it possible for operators to design and/or implement solutions and services for network optimization, congestion, troubleshooting and monetization with the information exported from the MME. Implementation of this feature requires configuration of an IPNE Service that is then associated with the MME Service.

IPNE is a licensed Cisco feature. Contact your Cisco account representative for information on licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section in the System Administration Guide.

Command Changes

ipne-service

A new command has been added to the MME CLI to create and configure an IPNE service.

```
configure
context context_name
    [no] ipne-service ipne_service
end
```

Notes:

- It is recommended that the IPNE Service be configured in the same context in which the MME Service has been configured.

- `ipne_service` enter 1 to 63 alphanumeric characters to create a unique IPNE service within the context and enter the IPNE Service configuration mode.

- `no` included as a prefix of the command disables the feature when it has been enabled with this command and removes the IPNE service definition from the MME's configuration. If an IPNE service is to be removed and the service has active handles, then the handles are deleted using a timer-based approach and then the IPNE service is removed.

ipne-endpoint

A new command has been added to the suite of MME CLI that creates and configure an IPNE endpoint and enters the IPNE Endpoint configuration mode. An IPNE endpoint is a combination of a local IP address, a peer address and, optionally, a port.

```
configure
context context_name
    ipne-service ipne_service
    ipne-endpoint
        bind { ipv4-address | ipv6-address } ip_address
        no bind
```
peer { ipv4-address | ipv6-address } ip_address
no peer
end

Notes:

• { ipv4-address | ipv6-address } ip_address: Identify the type of IP address - either IPv4 or IPv6 and then enter either an IPv4 dotted-decimal or an IPv6 colon-separated hexadecimal notation.
  ◦ as part of the bind command, the IP address identifies the IPNE client socket as the local address.
  ◦ as part of the peer command, the IP address identifies the MINE server as the peer address.

• no included as a prefix of either the bind or peer command removes the bind address or the peer address from the IPNE endpoint configuration.

associate

A new ipne-service keyword has been added to the associate CLI to associate the created IPNE service with the MME service

configure
  context context_name
    mme-service mme_service
    associate ipne-service ipne_service
    no associate ipne-service
  end

Notes:

• ipne_service enter 1 to 63 alphanumeric characters to identify a unique IPNE service name within the context.

• no included as a prefix of the command disassociates the IPNE service definition from the MME's service configuration.

Performance Indicator Changes

MME Schema

The following bulk statistics have been added to the MME schema to enable the operator to track the MME's IPNE-related paging messaging:

• signaling-ipne-paging-init-events-attempted
• signaling-ipne-paging-init-events-success
• signaling-ipne-paging-init-events-failures
• signaling-ipne-paging-last-enb-success
• signaling-ipne-paging-last-tai-success
• signaling-ipne-paging-tai-list-success
show ipne peers { all | service | summary }

This command generates a display of information for the IPNE service(s) and the TCP connection status for associated Session Manager(s). The following are sample displays:

```
[local]asr5000# show ipne peers all
SESSMGR : 1
Service Name: ipne-service  Context id: 3
Version : n/a
Local Address : 192.168.120.1:45161
Peer Address : 192.168.120.7:5222  State : [OPEN 0/1] [TCP]
```

```
[local]asr5000# show ipne peers summary
Service Name: ipne-service  Context id: 3
Version : n/a
Local Address : 192.168.120.1:45161
Peer Address : 192.168.120.7:5222  State : [OPEN 144/144] [TCP]
```

Notes:

- **all** lists all of the peers of each IPNE service and the state of the TCP connections for every SessMgr. This command with **all** option is part of support details (SSD).
- **service** requires the inclusion of an IPNE service name and displays information only for that service.
- **summary** generates a display similar to the all display but provides only summary TCP connection information for the SessMgrs.

show ipne statistics { all | service | summary }

This command generates a display of information regarding the number of IPNE handles of each IPNE service and count information for query/response/subscription/feed messages for the SessMgrs. The command generates a display similar to the following:

```
[local]asr5000# show ipne statistics all
SESSMGR : 1
Service Name: ipne-service  Context id: 3
Total handles: 0
Local Address : 192.168.120.1:0
Peer Address : 192.168.120.7:5222
Total query : 0
Total query response : 0  Success : 0  Failure : 0
Total update : 0
Total update response: 0  Success : 0  Failure : 0
Total subscription : 0  Add : 0  Delete : 0
Total feed : 0  Add : 0  Delete : 0
Total notification : 0
Total XML parser error: 0
IPNE messages discarded on tx queue:
Total discards : 0
Total Feed : 0  Notify : 0  Response : 0
```

```
[local]asr5000# show ipne statistics summary
Service Name: ipne-service  Context id: 3
Total handles: 0
Local Address : 192.168.120.1:0
Peer Address : 192.168.120.7:5222
Total query : 0
Total query response : 0  Success : 0  Failure : 0
Total update : 0
Total update response: 0  Success : 0  Failure : 0
Total subscription : 0  Add : 0  Delete : 0
Total feed : 0  Add : 0  Delete : 0
Total notification : 0
Total XML parser error: 0
IPNE messages discarded on tx queue:
```

Release Change Reference, StarOS Release 18
Total discards : 0
Total Feed : 0 Notify : 0 Response : 0

Notes:

- all lists all of the peers of each IPNE service and the state of the TCP connections for every SessiMgr. This command with all option is part of support details (SSD).
- service requires the inclusion of an IPNE service name and displays information only for that service.
- summary generates a display similar to the all display but provides only summary TCP connection information for the SessMgrs.

CSCui82362, CSCum50067, CSCur31142, CSCup89617 - MME to select the co-located SGSN in case of handoffs from MME to SGSN

SGSN-MME Combo Optimization

The SGSN and MME can be enabled simultaneously in the same chassis and, though co-located, they each behave as independent nodes. This Combo Optimization feature enables the co-located SGSN and MME to co-operate with each other in order to achieve lower memory utilization, lower CPU utilization, and reduced signaling towards other nodes in the network. When functioning as mutually-aware co-located nodes, the SGSN and MME can share UE Subscription data.

This feature is enabled with a new CLI command, see the Command Changes section below.

- If the operator intends the MME to use DNS to dynamically discover the Target SGSN, then the DNS Server must be configured with an entry for the co-located SGSN for the RAN FQDN with service-parameter "x-3gpp-sgsn:x-s3" or "x-3gpp-sgsn:x-gn".
- If the operator intends the MME to use location configuration to select the Target SGSN, then the MME Service configuration is required to have a peer-sgsn entry for the co-located SGSN.

For detailed Combo Optimization feature and implementation description see the SGSN-MME Combo Optimization section in the MME Administration Guide, StarOS Release 18.

Combo Optimization functionality for both the SGSN and the MME is a licensed Cisco feature. Contact your Cisco account representative for information on acquiring this separate feature license or for any other licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section in the System Administration Guide.

Command Changes

sgsn-mme

The new sgsn-mme subscriber-data-optimization command in the LTE Policy configuration mode enables/disables this SGSN-MME Combo Optimization feature.

config
  lte-policy
  | no | sgsn-mme subscriber-data-optimization
end
Notes:

- By default the SGSN-MME Combo Optimization feature is disabled. Enter the command to enable the feature.
- `no` included as a prefix of the command disables the feature when it has been enabled with this command.

Performance Indicator Changes

MME Schema

The following new bulk statistics in the MME schema facilitate tracking MME optimization functionality for the SGSN-MME nodes when co-located in the same chassis with the Combo Optimization functionality enabled:

- optimized-out-rau-ho-4gto2g3g-attempted
- optimized-out-rau-ho-4gto2g3g-success
- optimized-out-rau-ho-4gto2g3g-failures
- optimized-in-tau-ho-2g3gto4g-attempted
- optimized-in-tau-ho-2g3gto4g-success
- optimized-in-tau-ho-2g3gto4g-failures
- optimized-out-s1-ho-4gto2g3g-attempted
- optimized-out-s1-ho-4gto2g3g-success
- optimized-out-s1-ho-4gto2g3g-failures
- optimized-in-s1-ho-2g3gto4g-attempted
- optimized-in-s1-ho-2g3gto4g-success
- optimized-in-s1-ho-2g3gto4g-failures

show lte-policy sgsn-mme summary

The following parameter indicates if data optimization on SGSN-MME combo node is "Enabled" or "Disabled":

- subscriber-data-optimization

show hss-peer-service statistics all

The following new fields are added to the show output to display the subscription data statistics:

- Subscription-Data Stats
- Skip Subscription Data
- Subscription-Data Not Received
The Skip Subscription Data statistic is incremented when the ULR is sent with the skip-subscription-data flag set. The Subscription-Data Not Received statistic is incremented if the HSS does not send the subscription data in the ULA when skip-subscription-data flag is set in ULR. The difference between the Skip Subscription Data and Subscription-Data Not Received gives us the number of times HSS does not honour the skip-subscription-data flag.

**show mme-service statistics handover**

The following new statistics are added to the show output to display the information about Inter-RAT Optimized Handoffs between the co-located SGSN and MME:

- Inter-RAT Optimized Handoffs Between Co-located MME and SGSN
- Outbound MME to SGSN RAU procedure
- Attempted
- Success
- Failures
- Inbound SGSN to MME TAU procedure
- Attempted
- Success
- Failures
- Outbound MME to SGSN Connected Mode Handover
- Attempted
- Success
- Failures
- Inbound SGSN to MME Connected Mode Handover
- Attempted
- Success
- Failures

**CSCul07975 - Splitting up of points of failure when the MME signals Network failure.**

**Feature Changes**

**Counters Focusing on Points of Failure**

With this release, the MME further splits up tracking of the reasons for network failures by providing new segregated counters for various conditions that could result in network failure.
Performance Indicator Changes

MME Schema

The following new bulk statistic variables have been added to the MME schema to facilitate network failure debugging:

- emm-msgtx-attach-rej-network-fail-session-recovery
- emm-msgtx-attach-rej-network-fail-smgr-resource-unavailable
- emm-msgtx-attach-rej-network-fail-egtp-connection
- emm-msgtx-attach-rej-network-fail-auth-proc
- emm-msgtx-attach-rej-network-fail-hss-unavailable
- emm-msgtx-attach-rej-network-fail-pgw-selection
- emm-msgtx-attach-rej-network-fail-sgw-selection
- emm-msgtx-attach-rej-network-fail-hss-subscription-fail
- emm-msgtx-attach-rej-network-fail-s1-connection
- emm-msgtx-attach-rej-network-fail-congestion
- emm-msgtx-attach-rej-network-fail-gateway-unreachable
- emm-msgtx-attach-rej-network-fail-newcall-restrict
- emm-msgtx-attach-rej-network-fail-other-reasons
- emm-msgtx-tau-network-fail-session-recovery
- emm-msgtx-tau-network-fail-smgr-resource-unavailable
- emm-msgtx-tau-network-fail-egtp-connection
- emm-msgtx-tau-network-fail-auth-proc
- emm-msgtx-tau-network-fail-hss-unavailable
- emm-msgtx-tau-network-fail-sgw-selection
- emm-msgtx-tau-network-fail-hss-subscription-fail
- emm-msgtx-tau-network-fail-s1-connection
- emm-msgtx-tau-network-fail-congestion
- emm-msgtx-tau-network-fail-gateway-unreachable
- emm-msgtx-tau-network-fail-max-retx-tau-accept
- emm-msgtx-tau-network-fail-guard-timer-expiry
- emm-msgtx-tau-network-fail-detch-event
- emm-msgtx-tau-network-fail-congestion
- emm-msgtx-tau-network-fail-gateway-unreachable
• emm-msgtx-tau-network-fail-newcall-restrict
• emm-msgtx-tau-network-fail-no-active-bearer
• emm-msgtx-tau-network-fail-peer-node-fail
• emm-msgtx-tau-network-fail-other-reasons
• emm-msgtx-tau-inter-network-fail-session-recovery
• emm-msgtx-tau-inter-network-fail-smgr-resource-unavailable
• emm-msgtx-tau-inter-network-fail-egtp-connection
• emm-msgtx-tau-inter-network-fail-auth-proc
• emm-msgtx-tau-inter-network-fail-hss-unavailable
• emm-msgtx-tau-inter-network-fail-sgw-selection
• emm-msgtx-tau-inter-network-fail-hss-subscription-fail
• emm-msgtx-tau-inter-network-fail-s1-connection
• emm-msgtx-tau-inter-network-fail-unexpected-tau
• emm-msgtx-tau-inter-network-fail-max-retx-tau-accept
• emm-msgtx-tau-inter-network-fail-guard-timer-expiry
• emm-msgtx-tau-inter-network-fail-detach-event
• emm-msgtx-tau-inter-network-fail-congestion
• emm-msgtx-tau-inter-network-fail-gateway-unreachable
• emm-msgtx-tau-inter-network-fail-newcall-restrict
• emm-msgtx-tau-inter-network-fail-no-active-bearer
• emm-msgtx-tau-inter-network-fail-peer-node-fail
• emm-msgtx-tau-inter-network-fail-other-reasons
• emm-msgtx-tau-intra-network-fail-session-recovery
• emm-msgtx-tau-intra-network-fail-auth-proc
• emm-msgtx-tau-intra-network-fail-hss-unavailable
• emm-msgtx-tau-intra-network-fail-sgw-selection
• emm-msgtx-tau-intra-network-fail-hss-subscription-fail
• emm-msgtx-tau-intra-network-fail-s1-connection
• emm-msgtx-tau-intra-network-fail-unexpected-tau
• emm-msgtx-tau-intra-network-fail-periodic-tau
• emm-msgtx-tau-intra-network-fail-guard-timer-expiry
• emm-msgtx-tau-intra-network-fail-detach-event
• emm-msgtx-tau-intra-network-fail-congestion
show mme-service statistics

The following counters have been introduced to the generated display to better track network failures:

### Attach Reject > Network Failure:

<table>
<thead>
<tr>
<th>Counter Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recovery</td>
<td>0</td>
</tr>
<tr>
<td>S11 EGTP Connection</td>
<td>0</td>
</tr>
<tr>
<td>HSS Unavailable</td>
<td>0</td>
</tr>
<tr>
<td>PGW Selection Fail</td>
<td>0</td>
</tr>
<tr>
<td>S1 Connection</td>
<td>0</td>
</tr>
<tr>
<td>Gateway Unreachable</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>SMgr Resource Unavail</td>
<td>0</td>
</tr>
<tr>
<td>Auth Procedure Fail</td>
<td>0</td>
</tr>
<tr>
<td>HSS Subscription Fail</td>
<td>0</td>
</tr>
<tr>
<td>SGW Selection Fail</td>
<td>0</td>
</tr>
<tr>
<td>Congestion Policy</td>
<td>0</td>
</tr>
<tr>
<td>New Call Restrict</td>
<td>0</td>
</tr>
</tbody>
</table>

### TAU Reject > Network Failure:

<table>
<thead>
<tr>
<th>Counter Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recovery</td>
<td>0</td>
</tr>
<tr>
<td>S11 EGTP Connection</td>
<td>0</td>
</tr>
<tr>
<td>HSS Unavailable</td>
<td>0</td>
</tr>
<tr>
<td>Detach Event</td>
<td>0</td>
</tr>
<tr>
<td>Periodic TAU Fail</td>
<td>0</td>
</tr>
<tr>
<td>Max Retx TAU Accept</td>
<td>0</td>
</tr>
<tr>
<td>S1 Connection</td>
<td>0</td>
</tr>
<tr>
<td>Gateway Unreachable</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>SMgr Resource Unavail</td>
<td>0</td>
</tr>
<tr>
<td>Auth Procedure Fail</td>
<td>0</td>
</tr>
<tr>
<td>HSS Subscription Fail</td>
<td>0</td>
</tr>
<tr>
<td>SGW Selection Fail</td>
<td>0</td>
</tr>
<tr>
<td>Congestion Policy</td>
<td>0</td>
</tr>
<tr>
<td>Guard Timer Expiry</td>
<td>0</td>
</tr>
<tr>
<td>New Call Restrict</td>
<td>0</td>
</tr>
</tbody>
</table>

### TAU Reject Intra MME > Network Failure:

<table>
<thead>
<tr>
<th>Counter Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recovery</td>
<td>0</td>
</tr>
<tr>
<td>S1 Connection</td>
<td>0</td>
</tr>
<tr>
<td>HSS Unavailable</td>
<td>0</td>
</tr>
<tr>
<td>Detach Event</td>
<td>0</td>
</tr>
<tr>
<td>Periodic TAU Fail</td>
<td>0</td>
</tr>
<tr>
<td>Gateway Unreachable</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>SMgr Resource Unavail</td>
<td>0</td>
</tr>
<tr>
<td>Auth Procedure Fail</td>
<td>0</td>
</tr>
<tr>
<td>HSS Subscription Fail</td>
<td>0</td>
</tr>
<tr>
<td>SGW Selection Fail</td>
<td>0</td>
</tr>
<tr>
<td>Congestion Policy</td>
<td>0</td>
</tr>
<tr>
<td>Guard Timer Expiry</td>
<td>0</td>
</tr>
<tr>
<td>New Call Restrict</td>
<td>0</td>
</tr>
</tbody>
</table>

### TAU Reject Inter MME > Network Failure:

<table>
<thead>
<tr>
<th>Counter Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recovery</td>
<td>0</td>
</tr>
<tr>
<td>S11 EGTP Connection</td>
<td>0</td>
</tr>
<tr>
<td>HSS Unavailable</td>
<td>0</td>
</tr>
<tr>
<td>Detach Event</td>
<td>0</td>
</tr>
<tr>
<td>Periodic TAU Fail</td>
<td>0</td>
</tr>
<tr>
<td>Gateway Unreachable</td>
<td>0</td>
</tr>
<tr>
<td>Other Reasons</td>
<td>0</td>
</tr>
<tr>
<td>SMgr Resource Unavail</td>
<td>0</td>
</tr>
<tr>
<td>Auth Procedure Fail</td>
<td>0</td>
</tr>
<tr>
<td>HSS Subscription Fail</td>
<td>0</td>
</tr>
<tr>
<td>SGW Selection Fail</td>
<td>0</td>
</tr>
<tr>
<td>Congestion Policy</td>
<td>0</td>
</tr>
<tr>
<td>Guard Timer Expiry</td>
<td>0</td>
</tr>
<tr>
<td>New Call Restrict</td>
<td>0</td>
</tr>
<tr>
<td>Unexpected TAU Request</td>
<td>0</td>
</tr>
</tbody>
</table>
Performance Indicator Changes

TAI Schema

The MME can now collect 98 new bulk statistics for ESM procedures based on TAI:

- tai-esm-msgtx-act-ded-brr
- tai-esm-msgtx-act-ded-brr-retx
- tai-esm-msgtx-act-dflt-brr
- tai-esm-msgtx-act-dflt-brr-retx
- tai-esm-msgtx-brralloc-rej
- tai-esm-msgtx-brralloc-rej-pti-inuse
- tai-esm-msgtx-brralloc-rej-semantic-errtft
- tai-esm-msgtx-brralloc-rej-syntactic-errtft
- tai-esm-msgtx-brralloc-rej-invalid-brid
- tai-esm-msgtx-brralloc-rej-collision-nwop
- tai-esm-msgtx-brralloc-rej-pgw-rej
- tai-esm-msgtx-brralloc-rej-invalid-qty
- tai-esm-msgtx-brralloc-rej-insuff-resource
- tai-esm-msgtx-brralloc-rej-auth-failed
- tai-esm-msgtx-brrmod-rej
- tai-esm-msgtx-brrmod-rej-pti-inuse
- tai-esm-msgtx-brrmod-rej-semantic-errtft
- tai-esm-msgtx-brrmod-rej-syntactic-errtft
- tai-esm-msgtx-brrmod-rej-invalid-brid
- tai-esm-msgtx-brrmod-rej-collision-nwop
- tai-esm-msgtx-brrmod-rej-pgw-rej
- tai-esm-msgtx-brrmod-rej-invalid-qty
- tai-esm-msgtx-brrmod-rej-insuff-resource
- tai-esm-msgtx-brrmod-rej-auth-failed
• tai-esm-msgtx-brrmod-rej-svc-not-supported
• tai-esm-msgtx-brrmod-rej-svc-not-subscribed
• tai-esm-msgtx-deactbrr
• tai-esm-msgtx-deactbrr-retx
• tai-esm-msgtx-deactbrr-esm-info-req
• tai-esm-msgtx-deactbrr-esm-info-req-retx
• tai-esm-msgtx-deactbrr-modbrr
• tai-esm-msgtx-deactbrr-modbrr-retx
• tai-esm-msgtx-pdncon-rej
• tai-esm-msgtx-pdncon-rej-pti-inuse
• tai-esm-msgtx-pdncon-rej-apn-unk
• tai-esm-msgtx-pdncon-rej-pdntype-unk
• tai-esm-msgtx-pdncon-rej-inv-brrid
• tai-esm-msgtx-pdncon-rej-inv-pti
• tai-esm-msgtx-pdncon-rej-pgw-rej
• tai-esm-msgtx-pdncon-rej-auth-failed
• tai-esm-msgtx-pdncon-rej-svc-not-supported
• tai-esm-msgtx-pdncon-rej-svc-not-subscribed
• tai-esm-msgtx-pdncon-rej-opr-determined-barring
• tai-esm-msgtx-pdncon-rej-insuff-resources
• tai-esm-msgtx-pdncon-rej-activation-reject
• tai-esm-msgtx-pdncon-rej-svc-temp-out-of-order
• tai-esm-msgtx-pdncon-rej-protocol-errors
• tai-esm-msgtx-pdncon-rej-apn-restrict-incompatible
• tai-esm-msgtx-pdndiscon-rej
• tai-esm-msgtx-pdndiscon-rej-pti-inuse
• tai-esm-msgtx-pdndiscon-rej-lastpdn
• tai-esm-msgtx-pdndiscon-rej-inv-pti
• tai-esm-msgtx-pdndiscon-rej-inv-brrid
• tai-esm-msgrx-ded-brr-accept
• tai-esm-msgrx-ded-brr-reject
• tai-esm-msgrx-dflt-brr-accept
• tai-esm-msgrx-dflt-brr-reject
MME Changes in Release 18

- tai-esm-msgrx-deactivate-brr-accept
- tai-esm-msgrx-brr-rsrc-alloc-req
- tai-esm-msgrx-brr-rsrc-modify-req
- tai-esm-msgrx-esm-info-resp
- tai-esm-msgrx-em-status
- tai-esm-msgrx-mod-brr-accept
- tai-esm-msgrx-mod-brr-reject
- tai-esm-msgrx-pdn-con-req
- tai-esm-msgrx-pdn-discon-req
- tai-emergency-pdn-connect-attempted
- tai-emergency-pdn-connect-success
- tai-emergency-pdn-connect-failures
- tai-esmevent-pdncon-attempt
- tai-esmevent-pdncon-success
- tai-esmevent-pdncon-failure
- tai-esmevent-pdncon-ipv4-attempt
- tai-esmevent-pdncon-ipv4-success
- tai-esmevent-pdncon-ipv4-failure
- tai-esmevent-pdncon-ipv6-attempt
- tai-esmevent-pdncon-ipv6-success
- tai-esmevent-pdncon-ipv6-failure
- tai-pdn-disconnect-ue-attempted
- tai-pdn-disconnect-ue-success
- tai-pdn-disconnect-ue-failures
- tai-esmevent-defbearact-attempt
- tai-esmevent-defbearact-success
- tai-esmevent-defbearact-failure
- tai-dedi-brr-activation-ue-attempted
- tai-dedi-brr-activation-ue-success
- tai-dedi-brr-activation-ue-failures
- tai-ded-brr-deactivation-ue-attempted
- tai-ded-brr-deactivation-ue-success
- tai-ded-brr-deactivation-ue-failures
• tai-dflt-brr-deactivation-ue-attempted
• tai-dflt-brr-deactivation-ue-success
• tai-dflt-brr-deactivation-ue-failures
• tai-brr-modification-ue-attempted
• tai-brr-modification-ue-success
• tai-brr-modification-ue-failures

CSCul63403 - MME S6a: Skip-Subscriber-Data when UE moves to 4G from a colocated SGSN

Feature Changes

Skip-Subscriber-Data Bit Reduces Signaling

Previous Behavior: The MME did not set the 'skip-subscriber-data' bit in the ULR flag.

New Behavior: As part of the SGSN-MME Combo Optimization re-architecture (CSCui82362), the MME now sets the 'skip-subscriber-data' bit in the ULR flag as a part of the signalizing optimization when a UE moves to 4G from a co-located SGSN. By setting this bit, the MME avoids requests for subscription data in a ULR to reduce the signaling load on the S6d and S6a interfaces towards the HSS. According to the 3GPP TS 29.272, when the 'skip-subscriber-data' bit is set in the ULR it indicates that the HSS may skip subscription data in the ULA. If the last successful update of either the MME or the SGSN causes a change in the subscription data at the HSS, then the HSS ignores the 'skip-subscriber-data' bit and sends the updated subscription data.

CSCup66362, CSCup66417 - MME: Scale IMSIMgr

Feature Changes

IMSI Manager Scaling

The IMSIMgr is the de-multiplexing process that selects the SessMgr instance to host a new session based on a demux algorithm logic to host a new session by handling new calls requests from the MMEMgr, EGTPC Mgr, and the (e)SGTPCMgr (New MME handoffs). The new call requests or signaling procedures include Attach, Inter-MME TAU, PS Handover, and SGs, all of which go through the IMSIMgr. The IMSIMgr process also maintains the mapping of the UE identifier (e.g., IMSI/GUTI) to the SessMgr instance.

Previous Behavior: In earlier releases, there was a single IMSIMgr per MME.

New Behavior: In Release 18.0, with support for the expanded capacities of the VPC-DI and ASR5500, the IMSIMgr has become a bottleneck. The IMSIMgr Scaling feature increases the number of IMSI managers that can be made available on the MME. - from 1 to a maximum of 4. The number is configurable (see below).
IMSIMgr Scaling is only available on the ASR5500 and VPC-DI platforms.

By increasing the number of IMSIMgr instances, the new call handling capacity (primarily for Attach and SGs procedures) of the MME is increased as the calls are distributed across multiple instances. The call distribution logic across IMSIMgrs utilizes a simple hash operation on IMSI/GUTI to select the IMSIMgr instance.

It is the MMEMgr/EGTPC Mgr/SGTPC Mgr that selects an IMSIMgr instance to be contacted for session setup. Each subscriber session in a SessMgr will maintain the IMSIMgr instance number that 'hosts' the mapping for the IMSI. The SessMgrs now remembers the IMSIMgr instance Ids per subscriber for the target IMSIMgr instance number (IMSIMgr instance Id calculated by hash on the IMSI).

As a result of IMSIMgr Scaling, a second behavior change has been implemented. Now all IMSIMgr instances will send the current count of sessions per MME service to the MMEMgr via existing response messaging. The MMEMgr shall send the same data received from multiple IMSIMgr instances back to the IMSIMgr in existing request messaging. As a result, each IMSIMgr shall know the session count per MME service for all IMSIMgr instances. Given this information, the per MME service session limits can now be enforced by each IMSIMgr instance.

Customer Impact: Customers will notice the following when the number of IMSI managers is set for more than 1:

- It is possible to initiate an audit request for a single, specific IMSIMgr instance; for details see CSCur34618.
- Increased tolerance for configurable MME per service session limits. This can be visualized when configuring commands such as `bind` in the MME Service configuration mode.
- Increased tolerance forAttach rate control as the MME Attach rate control will be independently enforced by each IMSI Mgr instance.

Command Changes

task facility imsimgr

This command has been modified with the addition of a new keyword, `max`, that sets the maximum number of IMSIMgrs that can be spawned on the MME. This keyword is only visible when the MME is running in an ASR5500 or a VPC platform.

Important This is a boot-time configuration and must be added in the configuration file to be implemented at startup and before any MME related configuration takes effect, that is before any IMSIMgr is started. The run-time configuration of this CLI does not have any impact but is recorded in the configuration and will take effect only after a system reboot.

configure
  task facility imsimgr max number_imsimgrs
end

Notes:

- `number_imsimgrs` must be an integer from 1 to 4. The original setting is 4 on ASR5500 and VPC-DI.
Performance Indicator Changes

**show task resources facility imsimgr all**
This command displays the number of configured IMSIMgrs per chassis.

**show subscribers mme-only full all**
This command displays IMSIMgr instance information for subscriber session(s).

**show mme-service session full all**
This command displays IMSIMgr instance information for MME service session(s).

**show mme-service db record call-id**
This command displays IMSIMgr instance information based on call-id records.

**show demux-mgr statistics sgtpcmgr instance <instance>**
This command updates to display IMSI Mgr selection counter information.

**show demux-mgr statistics egtpemgr all**
This command updates to display IMSI Mgr selection counter information.

**show session subsystem facility mmemgr instance <instance>**
This command updates to display IMSI Mgr selection counter information.

**show snmp trap history**
SNMP trap now includes the IMSIMgr instance information

- Internal trap notification 1249 **Imsimgr instance: 1**, (MMENewConnectionsDisallowed) MME new connections disallowed, initial reason test
- Internal trap notification 1249 **Imsimgr instance: 1**, (MMENewConnectionsDisallowed) MME new connections allowed
CSCup66691, CSCuq25983 - eCSFB support for CDMA Network

Feature Changes

Important In a previous release of this document, this feature was incorrectly referred to as eCSFB. The correct feature identification is CSFB for 1XRTT.

CSFB-SRVCC for CDMA and for S102

Important This functionality is in Development and is Trial Quality for this release.

With this release, the MME expands support of circuit-switched fall back (CSFB) to enhanced circuit-switched fall back (CSFB) for CDMA 1x (single-carrier) radio transmission technology (1x-RTT) networks. The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWF/MSC to support the following CS services:

- MO/MT Voice calls
- MO/MT SMS
- Emergency calls

When released as production quality, implementation of this functionality will require a feature license.

Command Changes

Performance Indicator Changes

S102 Schema

A new bulk statistics schema has been created and it currently includes the following variables:

- vpnname
- vpnid
- servname
- servid
- s102ap-tx-a21-air-signal-msg
- s102ap-tx-a21-ack-msg
- s102ap-tx-a21-evt-ntfy-msg
CSCup66766 - MME support on VPC-DI

Feature Changes

MMEMgr Scaling to Support VPC-DI

With this release, MME has undergone architectural changes to allow enhanced operations on Cisco's Virtual Packet Core (VPC)- Distributed Instance (DI) platform. VPC (Cisco's brand name for StarOS VM instances) is StarOS running as a virtual machine (VM). Multiple VMs act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management.

For more information about the VPC platform, ask your Cisco Representative.

For the MME to take advantage of next generation platforms, such as the VPC, the MME architecture has been changed to allow:

- Linear capacity (memory) growth to support greater numbers of UEs and ENBs
- Signaling performance growth in term of CEPS
- Improved redundancy for RAN connections

To allow for VPC-DI Support, the MME has undergone the following changes:

- MMEMgr tasks are distributed across session PSC/DPC/SF-VM
- MMEDemux task are moved to demux PSC/DPC/SF-VM
IMSIMgr tasks are increased, refer to CSCup66362

Increase in number of MMEMgrs
  - maximum of 12 MMEMgrs in an ASR5K platform
  - maximum of 24 MMEMgrs in either an ASR5500 and a VPC

Two models of configuration, normal density and high density, have been introduced for the increased MMEMgrs:

**Command Changes**

task facility mmemgr

This new command scales up or down the number of MMEMgrs per PSC3/DPC/SF-VM:

---

**Important**

At this time, this command continues to be in development. The command is qualified for MMEs on the ASR 5000 platform with Normal Density as the current recommended setting.

configure
  task facility mmemgr per-sesscard-density { high | normal }
  default task facility mmemgr per-sesscard-density
end

Notes:

- Normal Density - represents the default model and supports:
  - a max of 1 MMEMgr per active session card

- High Density - allows for eNB scaling and provides for a lower number of session cards
  - a max of 2 MMEMgr per active session card

---

**Important**

This is a boot-time configuration and should be added in the configuration file before any MME service related configuration is created or any MME Manager is started. Run-time (dynamic) configuration should be saved and will take effect only after reboot.

**congestion-control threshold**

A new keyword `mmemgr-average-cpu-utilization` has been added to this command to configure MMEMgr specific thresholds.

configure
  [ default | no ] congestion-control threshold mmemgr-average-cpu-utilization { critical | major | minor }
end

Notes:
• The **mmemgr-average-cpu-utilization** type threshold uses the average CPU utilization of all the MMEMgrs in the system and is currently the recommended threshold measure for gauging MME service utilization.

• **default** as a command prefix, instructs the MME to reset the critical congestion-control threshold for the MMEMgr. The critical default is 80.

• **no** as a command prefix instructs the MME to remove the threshold settings from the MME’s configuration.

**Performance Indicator Changes**

**show congestion-control configuration**

This command has been enhanced to display the configured MMEMgr average CPU utilization threshold.

**CSCur24765 - Instance number should be included in the snmp trap generated by imsimgr**

**Feature Changes**

**Support for Multiple IMSIMgr Instances**

**Previous Behavior:** In earlier releases, the MME only supported a single IMSIMgr instance.

**New Behavior:** With the 18.0 release, the MME supports multiple IMSIMgr instances simultaneously with a maximum of four IMSIMgr instances at one time (see CSCup66362). Each IMSIMgr instance is identified by an instance number, which is included in the snmp trap (MMENewConnectionsAllowed or MMENewConnectionsDisallowed) notification generated by the IMSIMgr.

**CSCur34618 - [MME] IMSI Mgr Audit and show CLI**

**Feature Changes**

**IMSIMgr Audit**

**Previous Behavior:** When an audit is initiated with a CLI command an audit request is sent to the IMSIMgr, which in turn sends a request to all the SessnMgrs. Each SessnMgr sends a list of sessions back to the IMSIMgr.

**New Behavior:** With more than one IMSIMgr instance (see CSCup66362), it is now possible to initiate an audit request for just one IMSIMgr instance at a time.
Command Changes

mme imsimgr

The new mme imsimgr command triggers an MME IMSIMgr audit for IMSI, IMEI, MSISDN information for a specific SessMgr instance associated with a specific IMSIMgr instance. This is useful when the MME has been configured to support more than one MME IMSIMgr.

mme imsimgr instance instance_id audit-with sessmgr { all | instance instance_id }

Notes:

• imsimgr instance instance_id: Enter an integer from 1 to 4 to identify the specific IMSIMgr instance for which the audit is to be performed.

• all | instance instance_id: Select all to initiate audit for all SessMgr instances or select instance and for instance_id enter an integer from 1 to 1152 to identify a specific SessMgr for the audit.

CSCus32182 - MME doesn't store the ARD related info under any CLI output

Feature Changes

New Fields Display ARD-related Data

Previous Behavior: The MME does not display ARD of subscribers in any of the MME show commands.

New Behavior: This behavior change makes it possible for the MME to do two new functions:

• The MME can verify the UE Access-Restriction-Data (ARD) data, particularly in situations where the data is shared between the MME and an SGSN.

• The MME can display information for ARD of a subscriber using the existing show mme-service db record command (see Performance Indicator Changes section below for details).

Performance Indicator Changes

show mme-service db record

When the imsi keyword and IMSI value are added to the show mme-service db record command, then new fields are displayed to indicate ARD-related data:

• ARD:
  • UTRAN-not-allowed : True
  • GERAN-not-allowed : True
  • GAN-not-allowed : True
  • I-HSPA-Evolution-not-allowed : False
CSCus34861 - MME is not using NAPTR with least preference first for MSC selection

Feature Changes

Enabling Weight-based MSC Selection

Previous Behavior: By default, the MME selection of the peer MSC for the Sv interface is 'weight' based.

New Behavior: By default, the MME selection of the peer MSC for the Sv interface is now 'preference' based. A new CLI command has been provided to enable the operator to disable the default and use 'weight' based load balancing.

Customer Impact: The customer will need to explicitly configure weight-based selection to disable the new preference-based selection scheme.

Command Changes

peer-msc

This new command makes it possible for the operator to enable/disable weight-based selection of a peer MSC during MSC lookup. By default, this functionality is not enabled.

configure
call-control-profile profile_name
  peer-msc interface-type sv weight
remove peer-msc interface-type sv weight
end

Notes:

• remove removes the previously configured peer-MSC configuration and disables weight-based selection of a peer MSC.

Performance Indicator Changes

show configuration

When the default is overridden with the new peer-msc command, the output of the show configuration command will indicate:

• peer-msc interface-type sv weight
Feature Changes

Subscription Sharing Issues for MME/SGSN Combo

The following issue and behavior change are only applicable to the MME and SGSN when they are co-located in a single chassis and the SGSN & MME Combo Optimization functionality (described in CSCui82362) is enabled.

**Previous Behavior:** The mme-db stores AMBR values in bits per sector (bps). When the values are sent, in any message via a GTPv-2 interface, then these values are converted to kilo bits per section (kbps) - values are simply divided by 1000, which rounds to a lower value. For example, if AMBR was stored as 55555, it would be sent as 55 kbps on a GTPv-2 interface.

**New Behavior:** While converting AMBR values from bps to kbps, if there is a fractional remainder then the value is rounded up rather than down. For example, if AMBR was stored as 55555, it would be sent as 56 kbps via GTPv-2 interface.

This new behavior is in accordance with 3GPP spec. 29.274 Rel-12 which indicates that "The APN-AMBR for uplink and the APN-AMBR for downlink may require converting values in bits per second to kilo bits per second when the APN-AMBR for uplink and the APN-AMBR for downlink are received from an interface other than GTPv2 interface. If such conversions result in fractions, then the value of APN-AMBR for uplink and the APN-AMBR for downlink shall be rounded upwards."

As the SGSN already complies (prior to Release 18.0), changes are being made only for the MME.
CSCut28685 - SGSN - Issue with Combo subscription sharing wrt ambr values
CHAPTER 12

NAT Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from NAT in StarOS 18 software releases.

- NAT Enhancements for 18.1, page 189

NAT Enhancements for 18.1

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.

CSCuo78207 - [NAT]Stats to display MAX port usage of subscribers

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

Feature Changes

Port Utilization by Subscribers

In a NAT call, ports are allocated to a subscriber in chunks. The size of the chunk is configured at the NAT pool from which the NAT IP is allocated. In this enhancement, statistics are added to find out the number of ports utilized by a subscriber. The maximum number of ports that were required by a subscriber at any point of time is recorded.

The port utilization data of subscribers is aggregated at the NAT pool level. The number of ports are grouped into buckets of size 8. There are 9 defined port buckets — [0-8], [9-16], [17-24], [25-32], [33-40], [41-48],...
[49-56], [57-64] and [>=65]. The first bucket [0-8] includes not-on-demand calls, that is, subscribers who are allocated a port chunk without using any ports at all will fall into the first bucket. The last bucket [>=65] includes all subscribers using greater than 64 ports.

**Previous Behavior:** The `show active-charging nat statistics` CLI command does not display statistics for maximum port usage by a subscriber.

**New Behavior:** The following enhancements have been done in this release.

- The `show active-charging nat statistics` CLI command has been enhanced to display the distribution of maximum port usage by subscribers at NAT pool level.
- The `show active-charging firewall statistics verbose` CLI command has been enhanced to display more granular statistics for packets dropped due to non-availability of port chunks and due to maximum usage limit of port chunks.

### Performance Indicator Changes

**show active-charging firewall statistics verbose**

The following counters are added to the output of this command:

- Packets dropped due to MAX port chunks reached
- Packets dropped due to non-availability of port chunks

**show active-charging nat statistics**

The following counters are added to the output of this command:

- Ports distribution:
  - Max no. of ports used
  - Total no. of Subscribers

### CSCup47715 - Pilot Packet Format and Trigger Update

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

### Feature Changes

**Support for Pilot Packet Format and Trigger**

Pilot Packet is a feature which provides key pieces of information about subscriber session to an external element. As part of this enhancement, the current pilot packet format is modified to include additional attributes — Serving network identifier, Foreign agent IP address, NAI, and RAT Type. The Pilot Packet trigger is also enhanced to send a pilot packet when RAT type changes. The new pilot packet attributes and RAT type trigger are configurable.
The Pilot Packet feature is customer-specific. Contact your Cisco account representative for more information.

## Command Changes

### pilot-packet

In this release, the `attribute` and `trigger` keywords are added to this command in the Context Configuration mode. The `attribute` keyword configures the optional attributes to be sent in pilot packet. The `trigger` keyword configures triggers for pilot packet. This command must be configured in the destination context.

```plaintext
configure
  context context_name
    pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | trigger
      rat-change generate { nat-info-only | user-info-and-nat-info | user-info-only } }
    [ default | no ] pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | trigger rat-change }
end
```

**Notes:**

The optional attributes can be configured to be sent in pilot packet:

- **foreign-agent-ip-address**: Specifying this option includes the optional field "Foreign Agent IP Address" in pilot packet.
- **nai**: Specifying this option includes the optional field "NAI" in pilot packet.
- **rat-type**: Specifying this option includes the optional field "RAT Type" in pilot packet.
- **serving-nw-id**: Specifying this option includes the optional field "Serving Network Identifier" in pilot packet.

## Performance Indicator Changes

### APN Schema

The following bulk statistics are new in the release:

- rat-change-user-info-pilot-packet-sent-per-apn
- rat-change-nat-info-pilot-packet-sent-per-apn

### System Schema

The following bulk statistics are new in the release:

- rat-change-user-info-pilot-packet-sent
- rat-change-nat-info-pilot-packet-sent
show apn statistics name

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

- RAT-Change-User-Info
- RAT-Change-NAT-Info

show pilot-packet statistics all

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

- RAT-Change-User-Info
- RAT-Change-NAT-Info

show session subsystem facility sessmgr all

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

- RAT-Change-User-Info
- RAT-Change-NAT-Info

CSCup49820 - [NAT] Support for forcible NAT IP release CLI as part of MOP

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

Feature Changes

Forcible NAT IP Release

A new CLI command is added in support of this feature to release NAT IP addresses from SessMgr to VPNMgr for NAT pools by forcibly releasing the IP addresses from the subscriber calls.

**Previous Behavior:** In order to release a NAT IP address from a SessMgr, the calls in the system using the NAT IP will have to be cleared and the NAT binding timer has to expire before the NAT IPs are released back to VPNMgr. The `clear nat-ip` CLI command was present in the Debug mode.

**New Behavior:** CLI support is provided to release the NAT IP addresses from SessMgr to VPNMgr by forcefully releasing the IP addresses from the subscriber. The `clear nat-ip` CLI command is present in the Exec mode.

**Customer Impact:** An additional option is provided to forcibly clear the IP address from subscribers and NAT pools.
**Command Changes**

**clear nat-ip**

The `nat-ip` keyword is added to the `clear` command in the Exec mode, to clear NAT IP addresses forcibly from NAT pools.

`clear nat-ip { ip_address | pool pool_name } context context_name [ -noconfirm ]`

Notes:

- `ip_address`: Specifies the NAT IP address to be released from subscribers, in IPv4 dotted-decimal notation.
- `pool pool_name`: Specifies the NAT pool name, that is an existing IP pool or IP pool group, specified as an alphanumeric string of 1 through 31 characters.
- `context context_name`: Clears statistics for the VPN context name where the NAT pool belongs to, specified as an alphanumeric string of 1 through 79 characters.
- `-noconfirm`:Executes the command without any additional prompt and confirmation from the user.
- The following possible outputs can be seen on issuing this CLI command:
  - Success: <number-of-ips> NAT IP(s) are released from the using <number-of-subscribers> subscribers. For example: Success: 1 NAT IP(s) are released from the using 1 subscribers.
  - Failure: Invalid Pool Name.
  - Failure: NAT IP not found.
  - Failure: Invalid Context Name.
CSCup49820 - [NAT] Support for forcible NAT IP release CLI as part of MOP
PDSN Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from PDSN in StarOS 18 software releases.

- PDSN Enhancements for 18.1, page 195

PDSN Enhancements for 18.1

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

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

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

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

CSCup44247, CSCup42837 - SM support for PMIPv6 Subscriber Continuity Support

Applicable Products: 3G-CDMA, GGSN, 4G LTE/eHRPD

Feature Changes

Session Manager (SM) support for PMIPv6 Subscriber Continuity

The PMIPv6 Subscriber Continuity feature is implemented to leverage the LTE service authorization and subscription for the PMIPv6-based MPN service authorization. The Proxy Mobile IPv6 protocol is intended for providing network-based IP mobility management support to a mobile node, without requiring the participation of the mobile node in any IP mobility related signaling. The core functional entities involved
are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). This feature will be deployed to support PMIPv6 between external MAG and LMA (ASR9K) over 3G-CDMA, GGSN and 4G LTE/eHRPD.

**Previous Behavior:** Mobile Private Network (MPN) utilized Network Mobility Services (NEMO) to provide wireless connectivity between Enterprise Core Network and remote Enterprise sites over 3G/4G network, and supported only IPv4 addressing scheme.

**New Behavior:** To expand the addressing scheme to IPv6, PMIPv6 support is added.

### CSCus41228 - PDSN not to terminate PPP session when handoff within a restricted zone

#### Feature Changes

**PDSN not to terminate PPP session when handoff is within a restricted zone.**

**Previous Behavior:** PDSN terminates the subscriber session if subscriber performs an inter pcf-handoff, where both PCF exists in the same restricted zone.

**New Behavior:** PDSN accepts the PPP session when handoff is within the same restricted zone.
P-GW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from P-GW in StarOS 18 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 18.1
  
  "CSCus30437 - Std QCI(Non-GBR) wrngly incrmntd whn traffic dropd for GBR bearer in OCP"  
  - The fix implemented for CSCus30437 has resulted in a behavior change associated with some statistics at the P-GW subscriber level.

- P-GW Enhancements for 18.5, page 197
- P-GW Enhancements for 18.4, page 200
- P-GW Enhancements for 18.3, page 202
- P-GW Enhancements for 18.2, page 204
- P-GW Enhancements for 18.1, page 222

P-GW Enhancements for 18.5

This section identifies all of the P-GW enhancements included in this release:

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

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

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

CSCuw08643 - v6 support on newcall duplicate subscriber requested addr accept

Feature Changes

Duplicate Address Support for IPV6

This feature supports IPv6 PDN establishment with duplicate static IPv6 address from same user for an already existing PDN. This makes the PDN re-establishment successful and avoids enterprise users from experiencing service outage due to duplicate IP address request. A new CLI has been introduced at P-GW and GGSN service level to control this behavior. To support duplicate IPv4v6 address request, the existing CLI for duplicate address support for IPv4 and the newly added CLI for IPv6 need to be configured. Once the CLI is configured and the feature is enabled, the old session is terminated to accept the new connection with the same IPv6 address. If the feature is not enabled and the CLI is not configured then the new connection request is rejected if the requested address is already in use.

A new disconnect reason "dup-static-ipv6-addr-req" has also been added for the existing PDN, whenever the session is terminated due to a duplicate IPv6 address request.

Command Changes

duplicate-subscriber-requested-v6-address

A new CLI has been introduced at P-GW and GGSN service level to support duplicate IPv4v6 address request. This CLI supports IPv6 PDN establishment with duplicate static IPv6 address from same user for an already
existing PDN. This makes the PDN re-establishment successful and avoids enterprise users from experiencing service outage due to duplicate IP address request.

configure
context context_name
  pgw-service <pgw-service-name>
    newcall duplicate-subscriber-requested-v6-address { accept | reject }
    default newcall duplicate-subscriber-requested-v6-address { accept | reject }
end

Notes:

• **duplicate-subscriber-requested-v6-address**: Configures the support to accept or reject a duplicate address request with same IPv6 address.
• **accept**: Accepts the duplicate sessions with same IPV6 address request.
• **reject**: Rejects the duplicate sessions with same IPV6 address request.
• **default**: Disables the support to accept a duplicate address request.

**Performance Indicator Changes**

**show configuration**

The following field has been added to the output of this command under the P-GW service:

• duplicate-subscriber-requested-v6-address accept
• duplicate-subscriber-requested-v6-address reject

**show configuration verbose**

The following field has been added to the output of this command under the P-GW service:

• duplicate-subscriber-requested-v6-address accept
• duplicate-subscriber-requested-v6-address reject

**show pgw-service name <pgw-service-name>**

The following field has been added to the output of this command under the P-GW service:

• Duplicate Subscriber Addr Request IPv6: Accept
• Duplicate Subscriber Addr Request IPv6: Reject
CSCuw86628 - UBR suppression should not be applied to Modify Bearer command scenarios

Feature Changes

UBR Suppression Should Not Be Applied to Modify Bearer Command Scenarios

When Modify Bearer command (MBCmd) received in P-GW call comes with the same value of APN-AMBR and/or DEBQ, then UBR from the MB command was suppressed per UBR suppression feature. Currently, after receiving MBCmd with similar values already present in P-GW call, P-GW suppresses UBR and sends Modify Bearer Failure Indication.

UBR should not be suppressed when it is triggered due to MBCmd.

Previous Behavior: MBCmd was responded to with Modify Bearer Failure Indication if bit rates and all other parameters of default bearer were unchanged.

New Behavior: If the bit rates and all other parameters in MBCmd/CCA-U for MBCmd are the same as previous authorized values, the UBRReq triggered due to MBCmd is not suppressed. MBCmd will always respond with UBR.

P-GW Enhancements for 18.4

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

**CSCut53373, CSCuu63751, CSCuu64308 - PGW initiates UBR while no QoS change**

**Feature Changes**

**UBR Suppression Feature**

**Important**

The Update Bearer Request (UBR) Suppression feature is a license controlled feature. Please contact your Cisco sales representative for more information.

As the bit rate is expressed in bps on Gx and kbps on GTP, P-GW does a round-off to convert a Gx request into a GTP request. When P-GW receives RAR from PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in Kbps) is already set for the bearer. The UBR suppression feature enables P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

A new CLI has been added to the P-GW service configuration to enable UBR suppression. Once the CLI is configured, P-GW suppresses the UBR if the bit rate is the same after the round-off.

When UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

**Previous Behavior:** UBR was not suppressed, even if bit rates were the same.

**New Behavior:** If license is enabled and CLI is configured for UBR suppression, then UBR is suppressed if bit rates in kbps are the same after round-off and all other parameters, such as QCI, ARP, and TFT, that might trigger UBR are also unchanged.

**Command Changes**

`suppress-ubr no-bitrate-change`

A new CLI command has been introduced to control UBR suppression. This CLI is disabled by default; UBR is triggered, even if the Gx and GTP bit rates in kbps are the same after round-off.

```
configure
  context context_name
    pgw-service <pgw-service-name>
      egtp suppress-ubr no-bitrate-change
      no egtp suppress-ubr no-bitrate-change
    end
end
```
Notes:

- **suppress-ubr**: Enables or disables suppression of UBR when there is no change in PCRF authorized bit rates. By default, the UBR suppression feature is disabled.
- **no-bitrate-change**: Configures UBR suppression when there is no change in bit rates after bps to kbps round-off. By default, this keyword is disabled.
- **no**: Disables UBR suppression. UBR is triggered, even if the Gx and GTP bit rates in kbps are the same after round-off.

**Performance Indicator Changes**

`show configuration`

The following field has been added to the output of this command under the P-GW service:

- egtp suppress-ubr no-bitrate-change

`show configuration verbose`

The following field has been added to the output of this command under the P-GW service:

- no egtp suppress-ubr no-bitrate-change

`show pgw-service name <pgw-service-name>`

The following field has been added to the output of this command under the P-GW service:

- EGTP Suppress Update Bearer Request (no bitrate change): Enabled / Disabled

**P-GW Enhancements for 18.3**

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

CSCuv03271 - s2b-ho-no-context details not shown in show egtp-service all

Feature Changes

Correction to show egtp-service all Command Output

The output of the show egtpc-service all command has been modified to indicate if s2b-ho-no-context, which can be configured after the gtpc reject keyword, is enabled or disabled.

Previous Behavior: No s2b-ho-no-context configuration status information was provided when the show egtp-service all command was executed.

New Behavior: s2b-ho-no-context configuration status is shown in the show egtp-service all command output. By default, the rejection of S2b Handover calls when there is no UE context at the demux is disabled. When gtpc reject s2b-ho-no-context is not configured, the display will show that rejecting such a call is disabled. Only when this CLI is configured and enabled will the command output show that rejecting such a call is enabled.

Customer Impact: The show egtp-service all command output includes the configuration status of 2b-ho-no-context.

Performance Indicator Changes

show egtp-service all

The output of the show egtp-service all command has been modified to provide gtpc reject s2b-ho-no-context related details.

• Reject S2b HO(No UE Context) : Disabled
• Reject S2b HO(No UE Context) :Enabled
P-GW Enhancements for 18.2

This section identifies all of the P-GW enhancements included in this release:

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

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

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

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

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

CSCum59119, CSCus32111, CSCus32116 - SM support for non standard QCI

**Feature Changes**

**Related CDETS ID:** CSCum59123 - ECS support for non standard QCI

**Non-standard QCI Support**

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.
Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. A new license, however, allows non-standard QCIs (128-254) to be used on P-GW/GGSN (not standalone GGSN).

QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture". From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128-254. As per 3GPP Specification TS 29.212 "Policy and Charging Control over Gx reference point,” QCI values 0 and 10 to 255 are defined as follows:

- 0: Reserved
- 10-127: Reserved
- 128-254: Operator-specific/Non-standard QCI
- 255: Reserved

Unique operator-specific QCIs (128-254) can be used to differentiate between various services/applications carriers provide to the end users in their network.

The `operator-defined-qci` command in the QCI-QoS Mapping Configuration Mode configures the non-standard QCIs in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF. Unique DSCP parameters (uplink and downlink) and GBR or Non-GBR can also be configured. Non-standard QCIs can only be supported with S5/S8/S2a/S2b interfaces; the Gn interface is not supported. As non-standard QCIs are not supported in GGSN, `pre-rel8-qos-mapping` is used as a reference for mapping the non-standard QCI values to pre-rel8 QoS values during 3G calls or GnGp handovers.

### Command Changes

**operator-defined-qci**

| Important | This command is only visible if the license key supporting non-standard QCIs is installed. Contact your Cisco Account or Support representative for information on how to obtain a license. |

This new command configures the non-standard QCI in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF.

```plaintext
configure
    qci-qos-mapping name
        operator-defined-qci num { gbr | non-gbr } | { downlink | uplink } | encaps-header { copy-inner | copy-outer | dscp-marking dscp-marking-value } | internal-qos priority priority | | internal-qos priority priority | | user-datagram dscp-marking dscp-marking-value | encaps-header { copy-inner | copy-outer | dscp-marking dscp-marking-value } | internal-qos priority priority | | | | pre-rel8-qos-mapping num |
    no operator-defined-qci num
end
```

Notes:

- `operator-defined-qci num`: Specifies the operator-defined QCI value to be enabled. `num` must be an integer from 128 through 254.

  Standards-based QCI values 1 through 9 are configured through the `qci` command.
• **pre-rel8-qos-mapping** $num$: Maps non-standard QCI to a standard QCI that has the characteristics (TC, THP, SI, TD, SSD) similar to desired pre-rel8 standard QoS values during 3G call or GnGp handover. $num$ must be an integer from 1 through 4 for GBR and 5 through 9 for non-GBR. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

### 3G GGSN Call

If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI under P-GW which is associated with a GGSN, then the 3G call would be rejected.

### GnGp Handoff

1. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for default bearer, then the handoff would be rejected.

2. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for dedicated bearer, then only that bearer would be rejected during handoff.

3. In the following scenario:
   - default bearer with standard QCI or non-standard QCI (with **pre-rel8-qos-mapping** configured)
   - more than one dedicated bearer (some with standard QCI, some with non-standard QCI with **pre-rel8-qos-mapping** configured, and some with non-standard QCI with no mapping)

During LTE-to-GnGp handoff:

- UPC Request for all the dedicated bearers with non-standard QCI with no mapping would be rejected
- handoff will be successful for the remaining bearers

### Performance Indicator Changes

#### APN Schema

The following counters have been added in support of non-standard QCIs (GBR and Non-GBR):

- nonstdqci-nongbr-uplinkpkt-drop-mbrexcd
- nonstdqci-nongbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-nongbr-uplinkbyte-drop-mbrexcd
- nonstdqci-nongbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-nongbr-rejbearer
- nonstdqci-gbr-uplinkpkt-drop-mbrexcd
- nonstdqci-gbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-gbr-uplinkbyte-drop-mbrexcd
- nonstdqci-gbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-gbr-rejbearer
show apn statistics

The output of this command has been enhanced to show the following non-standard QCI counters (GBR and Non-GBR):

- Non-Std QCI(Non-GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)

- Non-Std QCI(GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)

show qci-qos-mapping table all

The output of this command has been enhanced to show when non-standard QCI are configured:

- Operator-defined-qci
- pre-rel8-qos-mapping

CSCum70938 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure

Feature Changes

Graceful Cleanup During Audit Failure

During an audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or ICSR event, if any critical information — internal or external — related to subscriber session inconsistency is detected, the associated session information is locally purged from the gateways. Since peer nodes are unaware of this, it is possible that the UE session is maintained at other nodes. This leads to unnecessarily clogging of the resources external to the gateway and unreachable UE for VoLTE calls.

When Audit Failure is detected at P-GW, Delete Bearer Request from P-GW to S-GW and S-GW to MME will carry the following cause code:

IMS/Custom
APNs: Reactivation Requested
Non-IMS/Custom1
APNs: CLI Configurable (No Cause IE by Default)
When Audit Failure is detected at S-GW, Delete Bearer Request from S-GW to MME would not carry the Cause IE.

Previous Behavior: During an Audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or an ICSR event, if any critical information, internally or externally related to a subscriber session seems inconsistent, ICSR will locally purge the associated session information.

Since external gateways (peer nodes) are unaware of the purging of this session, the UE session may be maintained at other nodes. This leads to unnecessary clogging of resources external to the gateway and an unreachable UE for VoLTE calls.

New Behavior: When this feature is enabled, graceful cleanup for an ICSR audit of failed calls occurs. External signaling notifies peers of session termination before purging the session. The gateway will attempt to notify external peers of the removal of the session. External nodes to the local gateway include: S-GW, P-GW, SGSN, MME, AAA, PCRF, and IMSA.

Audit failure can occur because of missing or incomplete session information. Therefore, only the peers for which the information is available will be notified.

Customer Impact: External signaling will be sent towards the peers while deleting the subscribers.

Command Changes

require graceful-cleanup-during-audit-failure

This new Global Configuration mode CLI command enables or disables the graceful cleanup feature.

configure
  require graceful-cleanup-during-audit-failure | del-cause non-ims-apn { none | system-failure } |
  default require graceful-cleanup-during-audit-failure
  no require graceful-cleanup-during-audit-failure
end

Notes:

• For P-GW, del-cause specifies the Cause Code to be sent in the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

• non-ims-apn: Specifies the Cause Code to be sent in the Delete Bearer Request from the P-GW resulting from the graceful cleanup for Audit Failure.
  * none: Omits the GTP Cause IE from the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.
  * system-failure: Sends the GTP Cause Code SYSTEM FAILURE.

• default: By default, the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

• no: The Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.
Performance Indicator Changes

show srp checkpoint statistics
The output of this command has been modified to display call drop counts due to ICSR audit failures:
• Graceful call drops during audit failure

show session disconnect-reasons
The output of this command has been modified to display call drop counts due to ICSR audit failures:
• graceful-cleanup-on-audit-fail(586)

CSCuo72738 - VoLTE-ICSR:GTPC Flow preinstallation

Feature Changes

GTP-C Flow Pre-installation with ICSR

Previous Behavior: GTP-C flows installed are deleted and created again upon chassis switchover.

New Behavior: All pre-installed GTP-C flows are not deleted upon chassis switchover. For example:
1. On active chassis, install seven source port flows for eGTP-C service.
2. On standby chassis, install two source port flows for eGTP-C service.
3. On active chassis becoming standby, delete five source port flows for eGTP-C service.
4. On standby chassis becoming active, install five source port flows for eGTP-C service.

Customer Impact: Data outage reduced.

CSCup49111,CSCuq45024,CSCup89018-PGW/GGSN/SAEGWRLF enhancements

Feature Changes

Bypass Rate Limit Function Enhancement
The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature, which is a license-enabled feature. The GTP Throttling feature helps control the rate of incoming/outgoing messages on P-GW/GGSN. It prevents the message flood from P-GW toward S-GW and MME. Currently, the following outgoing messages are throttled by P-GW and GGSN using the RLF framework:
• CBR
• DBR
Once throttling is enabled for outgoing messages, all outgoing messages are throttled except the Create Bearer Request (CBR) message, which is piggybacked with Create Session Response message. This feature has been enhanced to control the bypassing of some messages being throttled. This enhancement requires no additional license. Existing license for the GTP-Throttling feature (RLF License) and VoLTE prioritized handling feature licenses have been applied and used as follows:

- **RLF License**: The GTP-Throttling feature license has been enhanced to accommodate the message-types based RLF throttling bypass.

- **VoLTE Prioritized Handling Feature License**: This license has been enhanced to accommodate the emergency call, priority call, and apn-names-based RLF throttling bypass.

A new command option, `throttling-override-policy`, has been added to the existing CLI command `gtpc overload-protection egress rlf-template rlf-temp` which allows you to selectively bypass throttling for a configured message type or for all messages in emergency call, priority call, or call for the configured APN. A new CLI command mode, `throttling-override-policy`, has been also been introduced for generic syntax for throttling override policy.

Operator can configure Overload Protection/RLF Throttling-override (Bypass RLF) on P-GW along with Overload Control feature at the egress side. In this scenario, the Overload Control based on peer's reduction metrics will take higher precedence and messages will be throttled based on Overload Control feature first.

If the message is passed to RLF throttling after Overload Control feature processing, then the Throttling-override (Bypass RLF) will be applied after that according to the configuration. If the Overload Control feature is not configured and RLF Throttling and Bypass RLF Throttling is configured, then messages would be throttled based on RLF and Throttling-override (Bypass RLF) feature.

**Previous Behavior**: All outgoing messages except piggybacked request were throttled.

**New Behavior**: The outgoing request messages for create, update, and delete can be bypassed for RLF throttling.

**Customer Impact**: Can selectively bypass throttling for create, update, and delete outgoing request messages.

## Command Changes

**gtpc overload-protection egress**

This command has been modified to add a new CLI command option `throttling-override-policy`. The new command option allows you to selectively bypass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN.

```plaintext
configure
  context context_name
    gtpc overload-protection egress { rlf-template rlf_template_name throttling-override-policy throttling-override-policy_name }
```
throttling-override-policy

This new command mode has been added to Global Configuration Mode to create a GTP-C Throttling Override Policy and to enter GTP-C Throttling Override Policy mode.

configure

    throttling-override-policy throttling-override-policy_name

Notes:

Entering the above command sequence results in the following prompt:

[local]host_name(config-throttling-override-policy)#

egress bypass-rlf

A new command or egress bypass-rlf has been added to the throttling-override-policy command mode. This command configures message types which can bypass the rate limiting function.

configure

    throttling-override-policy throttling-override-policy_name

    [ default | no ] egress bypass-rlf { ggsn { msg-type { dpc | ipca | nrupc | emergency-call | arp { 1 | 2 | 3 }+ | apn-names <apn-name1> <apn-name2> <apn-name3> } } | pgw { msg-type { cbr | dbr | ubr | emergency-call | earp-pl-list { 1 | 2 | 3 | 4 | 5 | 15 | 15 }+ | apn-names <apn-name1> <apn-name2> <apn-name3> } } }

end

Notes:

• If an empty throttling-override-policy is created, then the default values for all the configurables are zeros/disabled.

• If no throttling-override-policy is associated, then show service configuration for P-GW and GGSN will show it as "n/a".

• Maximum number of throttling-override-policy that can be added are 1024. This limit is the same as max RLF templates.

• default: Resets the default attribute values for egress bypass configuration. If an empty throttling-override-policy is created then the default values for all the configurables are zeros/disabled.

• no: Disables the egress bypass rlf throttling configuration.

• ggsn: Configures GGSN specific message types to bypass rlf throttling.

• pgw: Configures P-GW specific message types to bypass rlf throttling.

• msg-type: Configures GGSN or P-GW message type to bypass rlf throttling.

• dpc: Bypasses RLF throttling for network initiated Delete PDP Context message type. By default, dpc is not bypassed.
- **ipca**: Bypasses RLF throttling for network initiated Delete PDP Context message type. By default, dpc is not bypassed.

- **nrupc**: Bypasses RLF throttling for Network Requested Update PDP Context message type. By default, nrupc is not bypassed.

- **emergency-call**: Bypasses rlf throttling for all request messages initiated by GGSN/P-GW emergency call. By default, emergency-call is NOT bypassed.

- **arp**: Configures Allocation-Retention-Policy (ARP) values associated with priority calls to be bypassed rlf throttling. By default, none of the ARP values are set. This option accepts the PL (Priority Level) values. The outgoing control messages of the calls with specified priority levels will bypass throttling. 

  +: More than one of the previous keywords can be entered within a single command.

- **apn-names**: Configures GGSN/P-GW APN names to bypass rlf throttling. You can configure up to three apn-names.

- **cbr**: Bypasses RLF throttling for create-bearer-request message type. By default, cbr is not bypassed.

- **dbr**: Bypasses RLF throttling for delete-bearer-request message type. By default, dbr is not bypassed.

- **ubr**: Bypasses RLF throttling for update-bearer-request message type. By default, ubr is not bypassed.

- **earp-pl-list**: Configures the list of Priority Levels(PL) associated with priority calls to be bypassed rlf throttling. By default none of the PLs are set. The outgoing control messages of the calls with specified priority levels will be bypassed throttling.

  +: More than one of the previous keywords can be entered within a single command.

### Performance Indicator Changes

**show configuration config**

This output of this command has been modified to include the following:

- throttling-override-policy policy1
- egress bypass-rlf pgw msg-type cbr
- egress bypass-rlf pgw msg-type dbr
- egress bypass-rlf pgw emergency-call
- egress bypass-rlf pgw earp-pl-list 1 2 4
- egress bypass-rlf pgw apn-names apn1.com apn2.com
- egress bypass-rlf ggsn msg-type ipca
- egress bypass-rlf ggsn msg-type dpc

**show configuration verbose**

This output of this command has been modified to include the following:

- throttling-override-policy policy1
- egress bypass-rlf pgw msg-type cbr
- no egress bypass-rlf pgw msg-type ubr
- egress bypass-rlf pgw msg-type dbr
- egress bypass-rlf pgw emergency-call
- egress bypass-rlf pgw earp-pl-list 1 2 4
- egress bypass-rlf pgw apn-names apn1.com apn2.com
- no egress bypass-rlf ggsn msg-type nrupc
- egress bypass-rlf ggsn msg-type ipca
- egress bypass-rlf ggsn msg-type dpc
- no egress bypass-rlf ggsn emergency-call
- no egress bypass-rlf ggsn arp
- no egress bypass-rlf apn-names

**show ggsn-service { all | name <name>**}

This output of this command has been modified to include the following:

- Throttling override
- Throttling override policy

**show pgw-service {all | name <name>**

This output of this command has been modified to include the following:

- Throttling override
- Throttling override policy

**show throttling-override-policy { all | name <name>**

This output of this command has been modified to include the following:

- Throttling Override Policy Name
- Bypass rlf throttling for GGSN:
  - NRUPC
  - IPCA
  - DPC
  - Emergency call
  - ARP
  - APN-Names
• Bypass rlf throttling for PGW:
  * CBR
  * UBR
  * DBR
  * Emergency call
  * EARP-PL-List
  * APN-Names

show rlf-context-statistics sessmgr gtpc-context-name ingress
  This command displays the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress
  This command displays the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress summary
  This command displays the summary of the RLF-Context statistics for GTP-C services like P-GW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress verbose
  This command displays the RLF-Context statistics verbose level for GTP-C services like PGW and GGSN configured in the VPN-Context/GTPC-Context-name "ingress" for session-manager instance "1".

show rlf-memcache-statistics sessmgr
  This command displays the cumulative RLF memory cache statistics for all session managers.

show rlf-memcache-statistics sessmgr instance 1
  This command displays the RLF memory cache statistics for session manager instance 1.

clear rlf-context-statistics sessmgr gtpc-context-name ingress
  This command clears the RLF context statistics in the VPN-Context/GTPC-Context-name "ingress".
CSCuq00838 - SM Support for P-GW/GGSN needs P-CSCF failure detection support

Feature Changes

P-CSCF Failure Detection Support Enhancement

P-CSCF failure detection support has been enhanced to ensure a failed P-CSCF address is not provided to the IMS client. Previously, P-CSCF restoration was already supported by using the Private Extn IE. Through this new enhancement, failure detection mechanism is made configurable so that it can be standards-based. The `pcscf-restoration` CLI command in P-GW Service Configuration Mode is used to enable/disable the standard based mechanism for P-CSCF failure detection. By default, this feature is disabled, in which case Private Extn mechanism will be used for P-CSCF restoration.

**Previous Behavior:** Only the Private Extn IE mechanism was supported for P-CSCF restoration.

**New Behavior:** Operators have the option of configuring the Private Extn IE or the Release 12 standards-based mechanism for P-CSCF restoration.

Command Changes

`pcscf-restoration`

This new command has been added to PGW Service Configuration mode to configure the mechanism to support P-CSCF restoration when a failure is detected.

```
config context context_name
    pgw-service pgw_service_name
        pcscf-restoration { hss-solution | custom-hss-solution }
    default pcscf-restoration
end
```

Where:

- **hss-solution** Enables the Release 12-based HSS solution for P-CSCF restoration.
- **custom-hss-solution** enables private extension-based HSS solution for P-CSCF restoration. This is the default setting.

Performance Indicator Changes

`show pgw-service name`

The output of this command has been enhanced to indicate the type of mechanism configured for P-CSCF restoration.

- P-CSCF Restoration solution: HSS-BASED (Rel12)
• P-CSCF Restoration solution: CUSTOM-HSS-BASED (PrivateExtn)

**show pgw-service all**

The output of this command has been enhanced to indicate the type of mechanism configured for P-CSCF restoration.

• P-CSCF Restoration solution: HSS-BASED (Rel12)
• P-CSCF Restoration solution: CUSTOM-HSS-BASED (PrivateExtn)

### CSCuq30097 - packets shown as dropped at sessmgr with ipv6 ecs readdressing

#### Feature Changes

**Packet Drop at Session Manager**

The behavior change listed for CSCuq30097 in 18.1 section of this document has now been modified by two fixes added by CSCus00503 and CSCut41926.

The old and new behavior is as follows:

**Previous Behavior:** In ECS Readdressing feature, drop counters in APN stats and in `show sub pgw-only full all` were not incremented when IPv4 and IPv6 fragmented packets were received in downlink. However, APN stats were incremented when IPv4 and IPv6 fragmented packets were received for uplink.

**New Behavior:** Now, for both IPv4 and IPv6 readdressing drop counter in APN statistics and in `show sub pgw-only full all` are not incremented.

**Customer Impact:** Correct packet drop counter in APN statistics and in `show sub pgw-only full all` will be seen for uplink and downlink.

### CSCur80218 - SAEGW - support for S2b standard based call flow

#### Feature Changes

**GTP-based S2b Interface Support on the SAEGW**

**Important**

GTP-based S2b Interface Support on the SAEGW is not currently supported. Full support for S2a and S2b calls is planned for a future release.
CSCur85237 - SFR: Licensing Bulkstats enhancements (Subscriber vs Sessions count)

Feature Changes

Licensing Bulkstats Enhancements

To enforce pricing based on per active sessions for 2G/3G and 4G subscribers, new counters have been added to the APN schema to count the number of active sessions per RAT type per APN. The CLI commands `show apn statistics` and `show bulkstats` have been modified to display the active sessions per APN for 2G, 3G, and 4G per RAT type per APN.

Performance Indicator Changes

APN Schema

The following new gauges on active sessions per 2G, 3G, and 4G have also been modified:

- active-eutran-sessions
- active-geran-sessions
- active-utran-sessions
- active-wlan-sessions
- active-hspa-sessions
- active-other-sessions

`show apn statistics name <apn_name> | all`

This command output has been modified to include the following new fields:

- Active Sessions per RAT Type:
  - EUTRAN
  - UTRAN
  - GERAN
  - WLAN
  - HSPA
  - OTHER
CSCu74504 - Appropriate disconnect reason should be displayed

Feature Changes

New Disconnect Reason 'Reject-ho-old_tun-path-failure' Added

In following scenarios, "unknown" is displayed as session disconnect reason; a more appropriate disconnect reason should be displayed.

Scenario 1:
WiFi-to-LTE handoff and then handback to WiFi during transition of WiFi-to-LTE before CSRes is sent by P-GW.

Observation: Session
disconnect reason: unknown-1,local-purge-1

Scenario 2:
GTP-U error indication message received during LTE-to-WiFi handoff.

Observation: Session
disconnect reason: unknown-1,local-purge-1

Previous Behavior:

[local]asr5000# show
session disconnect-reasons
Session Disconnect
Statistics
Total Disconnects: 2
Disconnect
Reason Num Disc Percentage
---------------------------
Unknown 1 50.00000
Local-purge 1 50.00000

New Behavior:

New disconnect reason "Reject-ho-old_tun-path-failure" added to indicate the correct behavior in case of path failure on old access while doing LTE<>WiFi HO.

[local]asr5000# show
session disconnect-reasons
Session Disconnect
Statistics
Total Disconnects: 2
Disconnect
Reason Num Disc Percentage
---------------------------
Local-purge 1 50.00000
Reject-ho-old-tun-path-failure 1 50.00000
CSCus96089 - GTPC stats on ICSR setup

Feature Changes

GTP-C Statistics on ICSR Setup

The statistics for setup and current need to be updated properly on standby chassis.

Previous Behavior: GTP-C statistics were incremented and displayed on the standby chassis.

New Behavior: GTP-C statistics for setup and released will not be updated on standby chassis. Only active statistics will be incremented, but they will not be displayed in the output of bulkstats or show CLI.

CSCut22844 - SegFault: libc.so.6/__strlen_sse2_bsf()

Feature Changes

Behavior Change in APN Removal

Previous Behavior: Earlier, while removing APN using the no apn <apn_name> command, "active subscriber sessions" would get deallocated automatically without any warning message.

New Behavior: Now, active subscriber sessions are not deallocated when you try to remove APN using the command no apn <apn_name>. APN removal is not allowed if some active subscriber sessions or some pending-deallocate sessions are present and an error message is displayed.

Customer Impact: APN removal is not allowed if active subscriber sessions or pending-deallocate subscriber sessions are already present for the APN.

Command Changes

no apn

Modification has been made to the command no apn. When there are active subscribers or some pending sessions that need to be deallocated, earlier this was possible with a warning message. With the new modification, the removal is not possible and the following error message is displayed:

"Error: Clear all subscribers connected to the APN <apn_name> before removing it from configuration".

configure
context context_name
no apn apn_name
end
CSCut76641 - GTPC ingress throttling should have strict rate limiting

Feature Changes

GTPC Ingress Throttling Feature Enhancement

The GTP-C ingress throttling feature implemented at Demuxmgr has been enhanced to have a strict rate limiting. New counters and bulkstats have also been added.

Previous Behavior: GTP-C ingress throttling feature did not have strict rate limiting.

New Behavior: GTP-C ingress throttling feature has been enhanced to have strict rate limit.

Customer Impact: GTP-C ingress throttling feature has been enhanced to have strict rate limit and the msg-rate configured will be the maximum message rate. If the incoming message rate is higher than the configured message rate, extra messages will get silently dropped. In addition, the actual call setup rate can be lower than the msg-rate configured, which could be due to delays in setting up the session due to many reasons like slow peer nodes or overloaded sm. Also, the drops done as part of this throttling are silent drops; hence, if path failure is configured for non-echo messages, path failure can be observed. Now, GTP-C ingress throttling can be analyzed more efficiently using the new counters and bulkstats.

Performance Indicator Changes

GTPC Schema

The following new counters have been added to the GTP-C schema:

- msgs-inc-rl-drop-rate-exceed
- msgs-inc-rl-drop-queue-full

EGTPC Schema

The following new counters have been added to the eGTP-C schema:

- msgs-inc-rl-drop-rate-exceed
- msgs-inc-rl-drop-queue-full

show demux-mgr statistics egtpinmgr instance <>

The output of this show command has been modified to include the following details:

Total Messages Dropped as Msg-rate exceeded: 0
Total Messages Dropped as Queue Full: 0

show gtpc statistics

The output of this show command has been modified to include the following details:
CSCut82166 - P-cscf restoration disconnect reason and disconnect stats

Feature Changes

P-CSCF Failure Detection Support Disconnect Reason and Disconnect Statistics

A new disconnect reason and statistics have been added to support the P-CSCF Failure Detection feature. For details on the feature, refer to the "CSCut13125, CSCuq00838 - SM Support for P-GW/GGSN needs P-CSCF failure detection support” feature description in the P-GW Enhancements for 18.1 section in this document.

Performance Indicator Changes

P-GW Schema

A new bulk statistic has been added to the P-GW schema. This bulk statistics indicates the number of default bearers released as a result of UE P-CSCF Reselection not being supported.

- sessstat-bearrel-nwdefpcscf

show pgw-service statistics all

A new disconnect reason has been added to the output of this command to indicate the number of UEs that do not support P-CSCF Re-selection (PCO-based optional extension as per Release 12, 3GPP 23.380 section 5.4.3). The new disconnect reason appears in the PDNs Released by Reason section of the command output.

- UE P-CSCF Reselect not supported

The output of this command has been enhanced to show the number of UEs released due to P-CSCF Re-selection not being supported, and to show the number of P-CSCF restoration indications received.

- UE P-CSCF Reselect not supported
- P-CSCF Restoration Indications received

show session disconnect reason verbose

A new disconnect reason has been added to the output of this command to indicate the number and percentage of UEs that do not support P-CSCF Re-selection (PCO-based optional extension as per Release 12, 3GPP 23.380 section 5.4.3). The new disconnect reason appears in the PDNs Released by Reason section of the command output.

- UE P-CSCF Reselect not supported(613) <Number> <Percentage>
show subscribers pgw-only full all

The output of this command has been enhanced to indicate if UE P-CSCF restoration support is enabled.

- UE P-CSCF Restoration Support: <Yes / No>

CSCuu56803 - [SysTest] vpnctrl over mem usage during longevity

Feature Changes

IPMS Configuration Update During VPN-ctrl Start

During unplanned MIO switchover, VPN-ctrl restarts and IPMS-config is updated to all clients in non-blocking call, causing too many memory allocations.

Previous Behavior: In the absence of the IPMS-config at SCT, configuration was broadcast to all the clients by IPMS-ctrl (part of VPN-ctrl) while VPN-ctrl kick started.

New Behavior: In the absence of the IPMS-config at SCT, configuration is not broadcast to all the clients by IPMS-ctrl (part of VPN-ctrl) while VPN-ctrl kick starts.

Customer Impact: During unplanned MIO switchover, VPN-ctrl would not go to warn state.

CSCuu58335 - Unable to retrieve bulkstats server information

Feature Changes

Bulkstat Process Retries for Connection Attempt After Transfer Interval

Previous Behavior: When a receiver was not responding, bulkstat process tried reconnecting the receiver on every server poll, which is 30 seconds.

New Behavior: Now, when a receiver is not responding, bulkstat process will not try to reconnect on every server poll. Instead, it will try to reconnect upon completion of transfer-interval, which is configurable. Default transfer interval is 15 minutes.

Customer Impact: Bulkstat data collection will happen on the configured transfer interval only, even on failures.

P-GW Enhancements for 18.1

This section identifies all of the P-GW enhancements included in this release:

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

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

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

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

CSCuh44477, CSCuq65471 - Dynamically allocate protocol_(username/password) in sessmgr_callline_t

Feature Changes

Removal of 'Protocol Username' from CLI Output

The output of the CLI command `show subscribers [pgw-only | sgw-only | saegw-only | ipsg-only | ggsn-only] full all` has been modified. The modified output does not contain the "Protocol Username" field, which was present earlier.

Previous Behavior: Earlier, the CLI command `show subscribers [pgw-only | sgw-only | saegw-only | ipsg-only | ggsn-only] full all` displayed "Protocol Username" field in its output.

New Behavior: The CLI command `show subscribers [pgw-only | sgw-only | saegw-only | ipsg-only | ggsn-only] full all` does not contain "Protocol Username" field.
Command Changes

show subscribers [pgw-only | sgw-only | saegw-only | ipsg-only | ggsn-only] full all

The output of this command has been modified. The "Protocol Username" field will no longer be displayed.

CSCul17189 - [PGW] Enhance Clear subs CLI to generate DBReq to control the pace.

Feature Changes

Enhanced Clear Subscribers Command for VoLTE

The clear subscribers non-VoLTE auto-delete command was implemented in StarOS release 17.0. This command can generate a burst of Delete Bearer Requests (DBR) and Delete Session Requests (DSR) in customer setups. To prevent the flooding of peer nodes with session removal control procedures, it is important to distribute these messages evenly in a periodic manner.

The pace-out-interval keyword has been added to the clear subscribers CLI command to allow operators to specify the time duration for removing the sessions so that control messages sent across to peer nodes are evenly distributed.

Sessions that are "paced-out" over a period of time move into a disconnecting state; however, data and control path activity continue as usual until the system sends out session deletion message(s). In the case of session recovery, "paced-out" sessions are recovered in the connected state and the clear subscriber command must be initiated again to clear the recovered sessions.

Command Changes

clear subscriber

The new keyword pace-out-interval has been added to this command so that session deletion messages are paced out on the basis of the time interval specified.

clear subscribers pace-out-interval interval_in_seconds
clear subscribers all pace-out-interval interval_in_seconds
clear subscribers non-volte-calls pace-out-interval interval_in_seconds
clear subscribers pgw-only all pace-out-interval interval_in_seconds
clear subscribers saegw-only all pace-out-interval interval_in_seconds
clear subscribers sgw-only all pace-out-interval interval_in_seconds

Notes:

• Where paceout-interval is the time, in seconds, that session deletion messages are sent out.
  interval_in_seconds must be an integer from 0 to 86400.
Feature Changes

Graceful Cleanup During Audit Failure

During an audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or ICSR event, if any critical information — internal or external — related to subscriber session inconsistency is detected, the associated session information is locally purged from the gateways. Since peer nodes are unaware of this, it is possible that the UE session is maintained at other nodes. This leads to unnecessarily clogging of the resources external to the gateway and unreachable UE for VoLTE calls.

When Audit Failure is detected at P-GW, Delete Bearer Request from P-GW to S-GW and S-GW to MME will carry the following cause code:
- IMS/Custom1
- APNs: Reactivation Requested
- Non-IMS/Custom1
- APNs: CLI Configurable (No Cause IE by Default)

When Audit Failure is detected at S-GW, Delete Bearer Request from S-GW to MME would not carry the Cause IE.

Previous Behavior: During an Audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or an ICSR event, if any critical information, internally or externally related to a subscriber session seems inconsistent, ICSR will locally purge the associated session information.

Since external gateways (peer nodes) are unaware of the purging of this session, the UE session may be maintained at other nodes. This leads to unnecessary clogging of resources external to the gateway and an unreachable UE for VoLTE calls.

New Behavior: When this feature is enabled, graceful cleanup for an ICSR audit of failed calls occurs. External signaling notifies peers of session termination before purging the session. The gateway will attempt to notify external peers of the removal of the session. External nodes to the local gateway include: S-GW, P-GW, SGSN, MME, AAA, PCRF and IMSA.

Audit failure can occur because of missing or incomplete session information. Therefore, only the peers for which the information is available will be notified.

Customer Impact: External signaling will be sent towards the peers while deleting the subscribers.

Command Changes

**require graceful-cleanup-during-audit-failure**

This new Global Configuration mode CLI command enables or disables the graceful cleanup feature.

```plaintext
configure
  require graceful-cleanup-during-audit-failure [ del-cause non-ims-apn { none | system-failure } ]
default require graceful-cleanup-during-audit-failure
no require graceful-cleanup-during-audit-failure
end
```

Notes:
For P-GW, **del-cause** specifies the Cause Code to be sent in the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

**non-ims-apn**: Specifies the Cause Code to be sent in the Delete Bearer Request from the P-GW resulting from the graceful cleanup for Audit Failure.

  * none: Omits the GTP Cause IE from the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.
  * system-failure: Sends the GTP Cause Code SYSTEM FAILURE.

**default**: By default, the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

**no**: The Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

### Performance Indicator Changes

**show srp checkpoint statistics**

The output of this command has been modified to display call drop counts due to ICSR audit failures:

- Graceful call drops during audit failure

**show session disconnect-reasons**

The output of this command has been modified to display call drop counts due to ICSR audit failures:

- graceful-cleanup-on-audit-fail(586)

### Feature Changes

**Support for RAN/NAS Cause Standard IE**

When an E-RAB or a data session is dropped, an operator may need to get detailed RAN and/or NAS release cause code information, as well as ULI information from the access network to be included in P-GW and S-GW CDRs for call performance analysis, user QoE analysis, and proper billing reconciliation. The operator may also need to retrieve the above information at the P-CSCF for IMS sessions.

"Per E-RAB Cause" was received in an E-RAB Release command and an E-RAB Release Indication messages over S1. However RAN and NAS causes were not forwarded to the P-GW and the S-GW and they were not provided by the P-GW to the PCRF.

A "RAN/NAS Release Cause" information element (IE), which indicates AS and/or NAS causes, has been added to the Session Deletion Request and Delete Bearer Command. The "RAN/NAS Release Cause" provided by the MME is transmitted transparently by the S-GW to the P-GW (if there is signaling towards the P-GW) for further propagation towards the PCRF.
Previous Behavior: Previously, RAN/NAS cause code was supported only in a specific private extension. There was no support for RAN/NAS cause code IE received in Delete Session Request and Delete Bearer Command.

New Behavior: Added support for 3GPP-defined RAN/NAS Cause code IE. The P-GW will support the existing behavior of the specific private extension to carry RAN/NAS cause code for backward compatibility. The same is supported in the P-GW CDR in dictionary custom35.

Customer Impact: Added support for RAN/NAS Cause code IE in Delete Session Request and Delete Bearer command. This change will be forwarded to the P-GW and in the S-GW-CDR and it will be provided to by the P-GW to the PCRF.

CSCuo61687 - PGW Bearer Duration KPI's

Feature Changes

Bearer Duration Statistics Expanded

Previous Behavior: Display the call duration for APN(s) in different duration bucket only for default bearer.

New Behavior: Display the call duration for APN(s) in different duration bucket only for dedicated bearers; new duration buckets have been added.

Customer Impact: Customer can see dedicated bearers duration for all the existing calls, however, this CLI is performance intensive and should be used judicially.

Command Changes

bearer-duration-stats

This new command enables/disables per QCI call duration statistics for dedicated bearers.

configure
  context  context_name
  apn  apn_name
  [ no ] bearer-duration-stats qci { all |1|2|3|4|5|6|7|8|9 } +
end

Notes:

• 1|2|3|4|5|6|7|8|9: Configure bearer duration statistics for QCI 1 to 9.
• all: Configure QCI-based duration statistics for all QCI.
• +: More than one of the previous keywords can be entered within a single command.

show session duration

This command displays session duration information. The keyword qci has been added.

show session duration apn apn_name  qci { all |1|2|3|4|5|6|7|8|9 } +

Notes:
• \([1|2|3|4|5|6|7|8|9]\): Displays call duration counters for QCI values 1 to 9.
• \(\text{all}\): Displays call duration counters for all QCI values.
• \(+\): More than one of the previous keywords can be entered within a single command.

Performance Indicator Changes

apn-qci-duration Schema

This new schema captures per-QCI duration statistics at APN level and includes the following statistics:

• apn-name
• qci-value
• qci-calldur-5sec
• qci-calldur-10sec
• qci-calldur-30sec
• qci-calldur-1min
• qci-calldur-2min
• qci-calldur-5min
• qci-calldur-15min
• qci-calldur-30min
• qci-calldur-1hour
• qci-calldur-4hour
• qci-calldur-12hour
• qci-calldur-24hour
• qci-calldur-over24hour
• qci-calldur-2day
• qci-calldur-4day
• qci-calldur-5day

show apn name \(apn\_name\)

The following field has been added to show which bearer duration statistics have been configured:

• Bearer duration stats config

show session duration apn \(apn\_name\) qci \{ all |1|2|3|4|5|6|7|8|9 \} +

The following in-progress call duration statistics have been added per specified QCI.
Feature Changes

Configurable Guard Timer on Create Session Request Processing

P-GW has an existing timer "session setup-timeout" which is hard coded to 60 seconds, which is used as a guard timer for session creation. This timer is used for all APNs and is started when a Create Session Request is received for any session creation.

Internal or external processing issues or delay at external interfaces, for example, Gx/Gy, can cause Create Session Request processing to run longer than time expected in end to end call setup. If the session processing is not complete when the timer expires, the Create Session Request processing is stopped and the P-GW performs an internal cleanup by stopping all other corresponding sessions, for example Gx/Gy. The P-GW responds with a Create Session Failure response stating that no resources are available to S-GW. In successful cases when there's no delay timer is stopped during sending out the Create Session Response.

A new CLI command has been introduced to allow a configurable value to override the previously hardcoded default session setup timeout value of 60 seconds. This will help to fine tune the call setup time at P-GW with respect to end to end call setup time.

Previous Behavior: On receiving a Create Session Request, the P-GW service started with a hardcoded setup timer value of 60 seconds.
New Behavior: The guard session setup timeout value has been made configurable from 1 to 120 seconds. If a Create Session Request is received and setup timeout is configured, the timer starts with the configured value. If the setup timeout is not configured, the timer starts with the default value of 60 seconds.

Command Changes

setup-timeout

A new command has been added to make P-GW session setup timeout configurable.

configure
context context_name
pgw-service service_name
setup-timeout timer-value
default setup-timeout
end

Notes:

• setup-timeout timer-value: Specifies the session setup timeout period, in seconds. If P-GW is able to process the Create Session Request message before the timer expires, P-GW stops the timer and sends a successful Create Session Response.

timer_value must be an integer from 1 to 120.

Default: 60 seconds

• default: Default value is 60 seconds. If no value is set, the P-GW service sets the timer to the default value.

Performance Indicator Changes

P-GW Schema

The following new counter has been added to the P-GW schema:

• setup-guard-timer-expired

SAEGW Schema

The following new counter has been added to the SAEGW schema:

• saegw- setup-guard-timer-expired

show pgw-service statistics all

The output of this command has been modified to display the Setup Guard Timer Expired value.

show saegw-service statistics all

The output of this command has been modified to display the Setup Guard Timer Expired value.
CSCuo97254, CSCuq44967, CSCuq44973 - R12 Overload Support

Feature Changes

R12 GTP-C Load and Overload Support on the P-GW

GTP-C Load Control feature is a licensed, optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control information in order to mitigate overload situations for the overloaded node through actions taken by the peer node(s). This feature is supported over S4, S11, S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.

In brief, load control and Overload Control can be described in this manner:

- Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

- Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its GTP-C peers to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signalling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.

Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Operation

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.
For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, \(((\text{number of active sessions per service} / \text{max session allowed for the service license}) \times 100)\).

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

**Command Changes**

**gtpc-load-control-profile**

This command has been added to Global Configuration Mode to create a GTP-C Load Control Profile and enter GTP-C Load Control Configuration Mode.

```
configure
c[ no ] gtpc-load-control-profile  profile_name
end
```

Notes:

- **no**: Removes specified GTP-C Load Control Profile.
- **profile_name** must be an alphanumeric string from 1 to 64 characters in length.

**inclusion-frequency**

This new command has been added to GTP-C Load Control Profile Configuration Mode to configure parameters to decide the inclusion frequency of the Load Control Information IE.

```
configure
  gtpc-load-control-profile  profile_name
  inclusion-frequency  { advertisement-interval interval_in_seconds | change-factor change_factor }
end
```

Notes:

- **inclusion frequency**: Configures parameters to decide inclusion frequency of load control information element.
- **advertisement-interval interval_in_seconds**: Configures advertisement-interval for Load Control in seconds.
  
  \( interval\_in\_seconds \) must be an integer from 0 to 3600.
  
  Default: 300
- **change-factor change_factor**: Configures change factor for load control.
  
  \( change\_factor \) must be an integer from 1 to 20.
  
  Default: 5%
weightage

This new command has been added to GTP-C Load Control Profile Configuration Mode to configure weightage for various load control parameters. Total weightage of all parameters should be 100%.

configure

gtpc-load-control-profile profile_name
  weightage system-cpu-utilization percentage system-memory-utilization percentage
  license-session-utilization percentage
default weightage
end

Notes:

• The total of all three parameter entries should be 100%.

• system-cpu-utilization percentage: Configures system CPU utilization weightage as a percentage of 100.
  percentage must be an integer from 0 to 100.
  Default: 40%

• system-memory-utilization percentage: Configures system memory utilization weightage as a percentage of 100.
  percentage must be an integer from 0 to 100.
  Default: 30%

• license-session-utilization percentage: Configures license session utilization weightage as a percentage of 100.
  percentage must be an integer from 0 to 100.
  Default: 30%


gtpc-overload-control-profile

This new command has been added to Global Configuration Mode to create a GTP-C Overload Control Profile and to enter GTP-C Overload Configuration Mode

configure

[ no ] gtpc-overload-control-profile profile_name
end

Notes:

• no: Removes specified GTP-C Overload Control Profile.

• profile_name must be an alphanumeric string from 1 to 64 characters in length.

inclusion-frequency

This new command has been added to GTP-C Overload Configuration Mode to configure parameters to decide inclusion frequency of the Overload Control Information IE.

configure

gtpc-overload-control-profile profile_name
  inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor }
default inclusion-frequency { advertisement-interval | change-factor }
end

Notes:

• **inclusion frequency**: Configures parameters to decide inclusion frequency of load control information element.

• **advertisement-interval** *interval_in_seconds*: Configures advertisement-interval for Overload Control in seconds.

  *interval_in_seconds* must be an integer from 0 to 3600.

  Default: 300

• **change-factor** *change_factor*: Configures change factor for Overload Control.

  *change_factor* must be an integer from 1 to 20.

  Default: 5%

**throttling-behavior**

This new command has been added to GTP-C Overload Configuration Mode to exclude events/messages from throttling due to a peer's overload reduction metric.

**configure**

`gtpc-overload-control-profile profile_name
  throttling-behavior { earp [ 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15 ]+ exclude } | emergency-events exclude }

  no throttling-behavior [ earp [ 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15 ]+ exclude ] | emergency-events exclude ]
end`

Notes:

• **throttling-behavior**: Configures throttling behavior based on peer's overload reduction metric.

• **earp**: Excludes the specified messages with configured earp from throttling due to the peer's overload reduction metric.

• **+**: More than one of the previous keywords can be entered within a single command.

• **emergency-events exclude**: Excludes the emergency events from throttling due to the peer's overload reduction metric.

**tolerance**

This new command has been added to GTP-C Overload Configuration Mode to configure overload tolerance limits.

**configure**

`gtpc-overload-control-profile profile_name
  tolerance { initial-reduction-metric percentage | threshold report-reduction-metric percentage self-protection-limit percentage } | default tolerance [ initial-reduction-metric | threshold ]
end`

Notes:
• **initial-reduction-metric percentage**: Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit. 
  
  `percentage` must be an integer from 1 to 100.
  
  Default: 10%

• **threshold-report-reduction-metric percentage**: Configures the minimum overload tolerance threshold for advertising the overload reduction metric to the peer.
  
  `percentage` must be an integer from 1 to 100.
  
  Default: 80%

• The **threshold-report-reduction-metric** should always be lower than the **self-protection-limit**.

• **self-protection-limit percentage**: Configures the maximum overload tolerance threshold after which node will move to self protection mode.
  
  `percentage` must be an integer from 1 to 100.
  
  Default: 95%

**validity-period**

This new command has been added to GTP-C Overload Configuration Mode to configure the time, in seconds, that specifies how long the Overload Control information is valid.

```plaintext
configure
gtpc-overload-control-profile profile_name
  validity-period seconds
  default validity-period
end
```

Notes:

• The default is 600 seconds.

• **validity-period seconds**: Configures the validity of Overload Control information.
  
  `seconds` must be an integer from 1 to 3600.

**weightage**

This new command has been added to GTP-C Overload Configuration Mode to configure weightage for various Overload Control parameters.

```plaintext
configure
gtpc-overload-control-profile profile_name
  weightage system-cpu-utilization percentage system-memory-utilization percentage license-session-utilization percentage
  default weightage
end
```

Notes:

• Total weightage for all parameters should be 100%.

• **system-cpu-utilization percentage**: Configures system cpu utilization weightage as a percentage of 100.
  
  `percentage` must be an integer from 0 to 100.
Default: 40%

- **system-memory-utilization**

  
  **system-memory-utilization percentage**: Configures system memory utilization weightage as a percentage of 100.

  *percentage* must be an integer from 0 to 100.

  Default: 30%

- **license-session utilization percentage**: Configures license session utilization weightage as a percentage of 100.

  *percentage* must be an integer from 0 to 100.

  Default: 30%

**associate**

The `gtpc-load-control-profile <profile_name>` and `gtpc-overload-control-profile <profile_name>` commands have been added to P-GW Service Configuration Mode to associate existing Load Control Profile and Overload Control Profiles to a configured P-GW service.

```
configure
c  context  context_name
c    pgw-service pgw_service_name
          associate gtpc-load-control-profile profile_name
          associate gtpc-overload-control-profile profile_name
          no associate gtpc-load-control-profile
          no associate gtpc-overload-control-profile
  end
```

**associate**

The `gtpc-load-control-profile <profile_name>` and `gtpc-overload-control-profile <profile_name>` commands have been added to S-GW Service Configuration Mode to associate an S-GW Load Control Profile to a configured S-GW service.

```
configure
c  context  context_name
    sgw-service sgw_service_name
          associate gtpc-load-control-profile profile_name
          associate gtpc-overload-control-profile profile_name
          no associate gtpc-load-control-profile
          no associate gtpc-overload-control-profile
  end
```

**associate**

The `gtpc-load-control-profile <profile_name>` and `gtpc-overload-control-profile <profile_name>` commands have been added to S-GW Service and P-GW Service Configuration Modes to enable the association of a Load and Overload Control Profile to a configured SAEGW service.

```
configure
c  context  context_name
    sgw-service sgw_service_name
```
Performance Indicator Changes

EGTPC Schema

The following bulk statistics have been added to the eGTP-C schema in support of the R12 Load and Overload Control feature:

- load-overload-own-lci
- load-overload-own-oci
- load-overload-num-msg-throttled
- load-overload-num-ovrload-cond-reached

show egtpc statistics

The output of this command has been enhanced to provide information on the S-GW's configured Load and Overload Control Profiles.

- Load Control Information
  - No. of Times Load Control Info TX
  - Current Load Factor

- Overload Control Information
  - No. of Times Overload Control Info TX
  - Current Overload Factor
  - Current Overload Reduction Metric
  - No. of times Overload Threshold Reached
  - Number of Messages Throttled

The output of this command has also been enhanced to show S-GW Load and Overload Control Profile information of the S-GW peer. For example, peer output would appear if the following command was executed on the S-GW:

show egtpc statistics mme-address 1.1.1.1
• Load Control Information
  ◦ No. of Times Load Control Info RX
  ◦ Current Load Factor

• Overload Control Information
  ◦ No. of Times Overload Control Info TX
  ◦ Current Overload Factor
  ◦ Current Overload Reduction Metric
  ◦ No. of times Overload Threshold Reached
  ◦ Number of Messages Throttled

**show gtpc-load-control-profile full all**

This new command has been added to Exec Mode to enable operators to view all configured parameters for all GTP-C Load Control Profiles on the S-GW.

• GTP-C Load Control Profile Name
• Weightage
  ◦ System CPU Utilization Weightage <percentage>
  ◦ System Memory Utilization Weightage <percentage>
  ◦ License Session Utilization Weightage <percentage>

• Inclusion Frequency
  ◦ Change Factor <factor:20>
  ◦ Advertisement Interval <seconds>

**show gtpc-overload-control-profile full all**

This new command has been added to Exec Mode to enable operators to view all configured parameters for all GTP-C Overload Control Profiles on the S-GW.

• GTP-C Overload Control Profile Name
• Weightage
  ◦ System CPU Utilization Weightage <percentage>
  ◦ System Memory Utilization Weightage <percentage>
  ◦ License Session Utilization Weightage <percentage>

• Tolerance
  ◦ Report Reduction Metric <percentage>
show pgw-service all

The output of this command has been enhanced to list the configured S-GW Load and Overload Control profiles associated with P-GW services.

• GTP-C Load Control Profile <name>
• GTP-C Overload Control Profile <name>

show sgw-service all

The output of this command has been enhanced to list the configured S-GW Load and Overload Control profiles associated with S-GW services.

• GTP-C Load Control Profile <name>
• GTP-C Overload Control Profile <name>

CSCup17404, CSCur88824 - ICSR IDLE Secs checkpointing optimization

Feature Changes

Stop Sending Idle secs Micro-checkpoint

Previous Behavior: When idle timeout is configured, idle seconds micro checkpoints were sent very frequently from active chassis to standby chassis to notify that a particular session is actively transmitting. This resulted in a large number of idle seconds messages leading to a high CPU usage.

New Behavior: By default, idle seconds micro checkpoints will not be sent from the ICSR framework. A CLI to configure periodic idle seconds micro checkpoint timer on a per-APN basis has been introduced through this feature. By default, this command is disabled and the default value of this timer is 10 seconds. The idle seconds micro checkpoint timer configured is recommended to be smaller than the session idle timeout timer...
value. Whenever timeout idle value is configured to be less than micro checkpoint periodicity value, a CLI warning message is displayed, indicating to the user that this configuration can lead to unstable state.

**Customer Impact:** When this CLI is configured, idle seconds micro checkpoints are sent at configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value.

### Command Changes

**timeout idle**

Enables configuration of periodic idle seconds micro checkpoint timer on a per-APN basis.

```cli
configure
ccontext  context_name
apn  apn_name
    timeout idle  time_in_seconds  [micro-checkpoint-periodicity  time_in_seconds]  
default timeout idle
    no timeout idle
end
```

**Notes:**

- **micro-checkpoint-periodicity:** Number of seconds.

  **Important** Micro-checkpoint-periodicity value should be less than idle timeout value.

- **default | no:** Default value is 10 seconds.

### Performance Indicator Changes

**show apn**

The `show apn apn_name` command has been modified to display "micro-checkpoint-periodicity" in the output.

For example:

```
micro-checkpoint-periodicity 10
```

**show configuration**

The `show configuration` command has been modified to display "micro-checkpoint-periodicity" in the output.

For example:

```
micro-checkpoint-periodicity 60
```

**show configuration verbose**

The `show configuration verbose` command has been modified to display "micro-checkpoint-periodicity" in the output.

For example:

```
micro-checkpoint-periodicity 10
```
CSCup29785, CSCup56949, CSCus96432 - Show command enhancements

Feature Changes

Show Command Enhancements
The current implementation of `show session historical` command does not provide a breakdown of access technology type. New keywords have been added to this command to display more precise output regarding access technology. The `show subscribers` CLI commands provides the session information instead of subscriber information. This command has been modified to give more precise output for the subscriber information.

Command Changes

`show session counters historical`
Following new keywords have been added to the command `show session counters historical` so that the session information can be displayed as per access-type.

- all
- 2g
- 3g
- 3g-ha
- 4g
- ehrpd
- wifi

`show session counters historical { all | arrived | callops | connected | disconnected | failed | handoff | rejected | renewal } { all-intervals | cumulative | graph | incremental | recent-intervals | table } { all | 2g | 3g | 3g-ha | 4g | ehrpd | wifi}

Notes:

- **all**: Displays session counters for all access-types (2g/3g/4g/ehrp/wifi)
- **2g**: Displays session counters for 2G (GERAN, GPRS) calls [GGSN, P-GW/S-GW and S4 SGSN] calls
- **3g**: Displays session counters for 3G (GERAN, GPRS) calls [GGSN, P-GW/S-GW and S4 SGSN] calls
- **3g-ha**: Displays session counters for 3G-HA calls
- **4g**: Displays session counters for 4G (EUTRAN, LTE) calls [P-GW, S-GW] calls
- **ehrp**: Displays session counters for EHRPD (evolved High Rate Packet Data) calls
- **wifi**: Displays session counters for Wireless LAN (WiFi) calls [P-GW, CGW]
Performance Indicator Changes

show session counters historical

This command has been modified to support the following new keywords for filtering output by access technologies:

- all – display counters for all access technology types
- 2g – display counters for 2G (GERAN, GRPS) access technology
- 3g – display counters for 3G (UTRAN, UMTS) access technology
- 3g-ha – display counters for 3G-HA sessions
- 4g – display counters for 4G (EUTRAN, LTE) access technology
- eHRPD – display counters only for eHRPD access technology
- wifi – display counters only for Wireless LAN access technology

When an access technology filter is specified, the output of this command separates session counters by category.

show session summary

This new command displays session types by access technology categories. The following information appears in the output of this command:

- 4G LTE (EUTRAN)
- 2G (GERAN)
- 3G (UTRAN)
- WiFi (WIRELESS LAN)
- eHRPD
- Others
- Total sessions
- Active
- Dormant
- pdsn-simple-ipv4
- pdsn-simple-ipv6
- pdsn-mobile-ip
- ha-mobile-ipv6
- hsgw-ipv6
- hsgw-ipv4
- hsgw-ipv4-ipv6
Feature Changes

Configurable Behavior on PDN Type IPv4v6

With this enhancement P-GW/GGSN will provide a new CLI configuration to enable the following four options, when MME/SGSN sets PDN type to IPv4v6 and Dual Address Flag (DAF) is set to False in Create Session Request or Create PDP Request.

1. Option 1: Assign IPv6 address using current method and respond with Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
2. Option 2: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #19 "New PDN type due to single address bearer only".
3. Option 3: Assign IPv6 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".
4. Option 4: Assign IPv4 address and respond with a Create Session Response or Create PDP Response with Success and Cause Code #18 "New PDN type due to network preference".

When the CLI is not configured, the default behavior is Option 1. The gateway supports multiple PDN connections for the same APN to accommodate for Option 1, Option 2, and the UE attempting a second PDN connection. It is possible to configure the CLI individual for each APN differently.

Previous Behavior: There was no configurable support for the type of PDN assigned and the cause code returned in a Create Session Response or Create PDP Response when a Create Session Request or CPC was received for IPv4v6 PDN with DAF False at the P-GW and GGSN.

New Behavior: Added configurable support for the type of PDN assigned and the cause code returned in Create Session Response or Create PDP Response when a Create Session Request or CPC is received for ipv4v6 PDN with DAF False added at the P-GW and GGSN.

Command Changes

daf-pdp-type

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received.
If this command is not configured P-GW/GGSN it uses the default option of assigning ipv6 pdn type with return cause of "New PDN Type due to single address bearer only".

```
configure
  context context_name
    apn apn_name
      daf-pdp-type { ipv4 | ipv6 } cause-code { network-preference | single-address-bearer-only }
  end
```

Notes:

- **daf-pdp-type**: Configures PDP type for requested IPv4v6 PDN with Dual Address Flag zero. Default PDP type is IPv6.
- **ipv4**: Configures PDP type for this APN to be IPv4.
- **ipv6**: Configures PDP type for this APN to be IPv6
- **cause-code**: Configures GTP cause code for requested IPv4v6 PDN with Dual Address Flag zero. Default GTP cause code is single-address-bearer-only.
- **network-preference**: New PDP type due to network preference
- **single-address-bearer-only**: New PDP type due to single address bearer only

### Performance Indicator Changes

#### P-GW Schema

A counter for number of Create Session Requests/Create PDP Requests received with PDN type IPv4v6 and DAF set to False on P-GW or GGSN which is not associated with SAEGW has been added to P-GW Schema:

- `sessstat-ipv4v6-pdn-daf-false-recv`

#### SAEGW Schema

A counter for number of Create Session Requests/Create PDP Requests received with PDN type IPv4v6 and DAF set to False on P-GW or GGSN which is associated with SAEGW has been added to SAEGW Schema:

- `pgw-sessstat-ipv4v6-pdn-daf-false-recv`

```
show apn { <name> | all }
```

The output of the command now includes the following text.

Zero Dual Address Flag:
PDP Type:   IPv4 | IPv6
Cause Code: New
PDN Type Due To Single Address Bearer Only | New PDN Type
Due To Network

```
show configuration apn
```

Based on the configuration, the output of this command now displays one of the following options:

- `daf-pdp-type ipv4 cause-code network-preference`
• daf-pdp-type ipv6 cause-code network-preference
• daf-pdp-type ipv4 cause-code single-address-bearer-only
• daf-pdp-type ipv6 cause-code single-address-bearer-only

show pgw-service statistics all
The output of this command now includes the following text:
IPv4v6 PDN-Type Received
with DAF False: 0

show saegw-service statistics all function pgw
The output of this command now includes the following text:
IPv4v6 PDN-Type Received
with DAF False: 0

CSCup44635 - SM support for CSCul22770, SFR - PSP algorithm modification

Feature Changes

Modification in Bandwidth Policy Selection During Call Setup

Previous Behavior: A single bandwidth policy was being sent from the session manager to ECS for validation. When an invalid bandwidth policy was received from RADIUS, the call was being terminated.

New Behavior: Primary and fallback policies are sent from SM to ECS. When an invalid bandwidth policy is received from RADIUS, bandwidth policy from APN can be applied if it is valid and the call will remain active.

Customer Impact: This will help prevent termination of calls when an incorrect bandwidth policy is sent through RADIUS.

CSCup71684, CSCup98374, CSCup71747 - PGW RTT Support for GTP procedures

Related CDETS ID: CSCup71713 - PGW RTT Support for Diameter procedures

Feature Changes

RTT Support for P-GW
The RTT feature will enable P-GW to generate event records containing a series of fields or IEs at the completion of specific GTPv2 procedures identified below:

• Create Session Request/ Response
• Create Bearer Request/ Response
• Delete Bearer Request/ Response
• Delete session Request/ Response
• Modify Session Request/ Response
• Update Bearer Request/ Response

Similarly, the RTT feature will enable P-GW to generate event records at the completion of specific Diameter procedures identified below:

• Diameter S6b - AAR/ AAA
• Diameter S6b - RAR/ RAA
• Diameter S6b – Session Termination
• Diameter S6b – Abort Session
• Diameter Gx - CCR-I/CCA-I
• Diameter Gx - CCR-U/CCA-U
• Diameter Gx - CCR-T/CCA-T
• Diameter Gy – CCR-I/CCA-I
• Diameter Gy – CCR-U/CCA-U
• Diameter Gy – CCR-T/CCA-T
• Diameter Gy – RAR/ RAA

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

Important

These records are made available to customers in CSV file format through their Real Time Tool (RTT) system. This feature allows for near real time monitoring of the LTE network.

Enabling the new `reporting-action event-record` CLI command at APN level causes event records for GTPv2/Diameter to be sent to CDR modules. This should be enabled for both Access side APN and RADIUS returned APNs (or virtual APNs). Existing CLI command `session-event-module` in Context Configuration Mode should also be initialized.

This CLI is used for enabling RTT records of both Diameter and GTPv2 procedures.

Command Changes

`reporting-action event-record`

This new command enables the reporting of APN-related events to a log.

```
configure
context context_name
  apn apn_name
    [ default | no ] reporting-action event-record
end
```
Notes:

- **default**: Disables reporting of events to a log. By default, reporting is disabled.
- **no**: Disables reporting of events to a log if reporting has been enabled.

**show event-record**

This new command displays event record statistics for a P-GW node.

`show event-record statistics pgw`

**Performance Indicator Changes**

**System Schema**

The following bulkstats have been added to the system schema:

- `sess-pgw-total-number-event-records`
- `sess-pgw-total-gtpv2-event-records`
- `sess-pgw-total-csr-event-records`
- `sess-pgw-total-cbr-event-records`
- `sess-pgw-total-dsr-event-records`
- `sess-pgw-total-dbr-event-records`
- `sess-pgw-total-mbr-event-records`
- `sess-pgw-total-ubr-event-records`
- `aaa-pgw-total-diam-event-records`
- `aaa-pgw-total-s6b-aar-event-records`
- `aaa-pgw-total-s6b-rar-event-records`
- `aaa-pgw-total-s6b-asr-event-records`
- `aaa-pgw-total-s6b-str-event-records`
- `sess-pgw-total-gx-ccri-event-records`
- `sess-pgw-total-gx-ccrt-event-records`
- `sess-pgw-total-gx-ccru-event-records`
- `sess-pgw-total-gx-rar-event-records`
- `sess-pgw-total-gy-ccri-event-records`
- `sess-pgw-total-gy-ccrt-event-records`
- `sess-pgw-total-gy-ccru-event-records`
- `sess-pgw-total-gy-rar-event-records`
show event-record statistics pgw

This is a new show CLI command that provides events statistics for the P-GW service. The following information appears in the output of this command:

- Total Number of Event Records
- GTPv2 Event Records:
  - CSR
  - CBR
  - DSR
  - DBR
  - MBR
  - UBR
- Diameter Event Records
- S6b Procedures:
  - AAR
  - RAR
  - ASR
  - STR
- Gx Procedures:
  - CCR-I
  - CCR-U
  - CCR-T
  - RAR
- Gy Procedures:
  - CCR-I
  - CCR-U
  - CCR-T
  - RAR
CSCup88929 - PGW/GGSN/SAEGW Abnormal bearer termination info in CDR

Feature Changes

Abnormal Bearer Termination Information in CDR

Currently, the dropped bearer is reported as a "abnormalrelease" in the CDR. This feature gives additional information in a P-GW CDR for a VoLTE drop. P-GW application will provide additional information (disconnect-reason) with "abnormalrelease" in "Delete-Bearer-Indication" and "Session-Release-Request" to ECS, so that ECS can add this information in P-GW CDR.

Previous Behavior:
1. For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls previously, for GTP-C/GTP-U path failure disconnect-reason of path-failure was used.
2. For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls for GTP-U error indication local-disconnect was used.

New Behavior:
1. For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls new disconnect reasons have been added containing interface information for GTP-C/GTP-U path failure
2. For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls new disconnect reasons have been added containing interface information for GTP-U error indication.

Performance Indicator Changes

show session disconnect-reasons

The output of this command will now include the following disconnect statistics:

- path-failure-s5
- path-failure-s11
- path-failure-s4
- gtpu-err-ind-s5u
- gtpu-err-ind-s12
- gtpu-err-ind-s1u
- gtpu-err-ind-s4u
- gtpu-path-failure-s5u
- gtpu-path-failure-s12
- gtpu-path-failure-s1u
- gtpu-path-failure-s4u
CSCup89677, CSCup73076, CSCup92630 - PGW/GGSN/SAEGW ULI enhancements

Feature Changes

P-GW, GGSN, SAEGW ULI Enhancements

S5/S8 eGTP-C now supports ULI/ULI Timestamp/Timezone in a "Delete Session Request" and a "Delete Bearer Command".

Timezone information received in a "Delete Bearer Request" and a "Delete Session Request" will be sent in a CCR-U and CCR-T through the Gx interface. The NPLI license and RetLoc Indication from the PCRF will control when the AVP is sent.

Important

Use of NPLI requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Previous Behavior: A ULI/ULI Timestamp/MS Timezone received in a "Delete Bearer Command" was ignored at the session manager. Also, an MS Timezone received in a "Delete Session Request" was not sent on the Gx interface.

New Behavior: Now, a ULI/ULI Timestamp/MS Timezone received in a "Delete Bearer Command" is sent to the ECS and the IMSA module. They are sent in a CDR and a CCR-U depending on the corresponding changes from the ECS and the IMSA. Also, an MS Timezone received in "Delete Session Request" is sent to the IMSA module. The IMSA module will send it to the CCR-T depending on IMSA changes.

Customer Impact: A CDR may carry ULI/ULI Timestamp/MS Timezone from the "Delete Bearer Command". CCR-T may carry MS Timezone from the "Delete Session Request".

CSCq11994, CSCup98379, CSCus94777 - PGW/GGSN/SAEGW LTE/WiFi GTP S2b Make-Before-Break HO Compliance

Feature Changes

DBR is delayed until HO completion for Inter-rat HO from S2a/S2b to LTE

When the UE moves from WiFi to LTE, the P-GW sends a Delete Bearer Request to the ePDG (WiFi access). Previously, the Delete Bearer Request was sent as soon as a Create Session Request for handoff was received at the P-GW. In some cases (for some specific handsets) this broke the IP sec tunnel between the handset and the WAP. In these instances, the handoff failed.

To avoid handoff failure, the P-GW will send a Create Session Response first and delay the Delete Bearer Request until handoff is complete for UE. Next, the UE generates a Modify Bearer Request to indicate handoff completion and the Delete Bearer Request is only generated after the P-GW receives the Modify Bearer Request. This indicates that both access types (WiFi and LTE) will remain active until the Modify Bearer
Request is received at the P-GW. When the UE moves from LTE to WiFi, handoff completion occurs at the Create Session Response.

**Previous Behavior:** When a Create Session Request came from the LTE for HO from S2a/S2b, the P-GW sent a Delete Bearer Request for S2a/S2b before sending a Create Session Response.

**New Behavior:** When a Create Session Request comes from the LTE for HO from S2a/S2b, the P-GW will send a Create Session Response. It will only send a Delete Bearer Request when HO is complete (for example: when SGW sends MBR with HO_Ind=1). When HO happens from the LTE to S2a/S2b, then Delete Bearer Request is sent after a Create Session Response is sent for HO completion.

**Customer Impact:** Previously, packets on old tunnel were being dropped. Now, packets on an old tunnel will be processed.

---

**CSCuq13125, CSCuq00838 - SM Support for P-GW/GGSN needs P-CSCF failure detection support**

**Feature Changes**

**P-CSCF Failure Detection Support**

In LTE, P-GW performs the P-CSCF discovery and provides UE with the list of P-CSCF addresses it can use for IMS Calls. P-GW supports the following mechanisms to select the P-CSCF address for a subscriber:

- P-CSCF info from S6b FQDN based DNS query
- P-CSCF info from Config FQDN based DNS query
- P-CSCF info from IMSA configured table
- P-CSCF info from APN config

P-CSCF failure detection is currently supported on P-GW using S6b FQDN/Config FQDN and APN Config. The similar support has been extended to IMSA. IMSA retrieves the P-CSCF information at ATTACH time, but did not perform a lookup when a Modify Request is received. With this enhancement, IMSA performs the lookup and provides a list of IP Address in Modify Response. P-GW does not keep track of the P-CSCF Address which the UE serves and hence the list of IP Addresses provided in Modify Response might have an Overlapping IP. The UE may or may not retry to the alternate IP Address provided.

**Previous Behavior:** Earlier only private extension based restoration was supported.

**New Behavior:** Now, both private extension and indication flags based restoration is supported.

**Customer Impact:** Customer now has support for custom and standard based restoration mechanisms.
CSCuq30097 - packets shown as dropped at sessmgr with ipv6 ecs readdressing

Feature Changes

Packet Drop at Session Manager

Previous Behavior: In ECS Readdressing feature, drop counter was updated only for IPv6. However, for IPv4, readdressing drop counter was not updated.

New Behavior: Now, for both IPv4 and IPv6 readdressing drop counter is updated.

CSCuq44987 - License for Wifi integration support in 18.0.

Feature Changes

License for WiFi Integration Support in Release 18.0.

This new feature includes the below WiFi integration.

- Support for GTP based S2a and GTP based S2b WiFi integration.
- Support for PMIP based S2a WiFi integration.
- Gz/Gx/Gy feature support for WiFi integration.
- Handover support between LTE and WiFi.

This license accepts new calls on S2a or S2b interface. By default, new Create Session Requests on GTP based S2a/S2b are rejected unless this license is enabled.

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

CSCuq51507 - License enforcement for GTP based S2a and S2b in 18.0.

Feature Changes

License Enforcement for GTP based S2a and S2b in Release 18.0

The interface-type command has been enhanced to enable and disable S2a and S2b interfaces for P-GW and SAEGW ingress.

Previous Behavior: There were no CLI keywords for S2a and S2b interface enabling/disabling.
**New Behavior:** Added new CLI keywords to enable and disable S2a and S2b interfaces for P-GW and SAEGW ingress.

---

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

---

**Command Changes**

**interface-pgw-ingress**

Two new keywords have been added to the `interface-type` command. This command configures the interface type used by this service. The new keywords **s2a** and **s2b** are now available to accept or reject Create Session Request (CSR) on GTP based S2a and S2b interfaces. These keywords are only visible if the license is enabled.

```
configure context context_name
  egtp-service egtp_service_name
  interface-type interface-pgw-ingress [ s2a ] [ s2b ]
end
```

**Notes:**
- **s2a:** P-GW supports S2a interface.
- **s2b:** P-GW supports S2b interface.
- The **S2a** and **S2b** keywords will be available only if a valid license is installed. For more information, contact your Cisco account representative.
- Disable S2a/S2b interface support for P-GW by entering the following command:
  ```
  interface-type interface-pgw-ingress
  ```

**Performance Indicator Changes**

**show egtp-service all**

The following fields are added to the output of this show command to accept or reject Create Session Request (CSR) on GTP based S2a and S2b interfaces. These fields are only visible if the license is enabled.

- **s5/s8**
- **s2a**
- **s2b**

---

**Important**
By default, **interface-pgw-ingress** is S5/S8, which cannot be changed, and S2a/S2b is not supported. If required, S2a/S2b can be enabled using the CLI commands above.
CSCuq74490 - PGW not rejecting session when HI = 1 & no Context

Feature Changes

P-GW Rejecting WLAN request if there is No Valid S2b Session for that PDN and UE indicates Handover

Related CDETS ID: CSCut28557

Standard Behavior

When the P-GW does not reject a Create Session Request HI=1 from the ePDG and there is no context, the P-GW attempts to create a new session. This causes a SIP 503 issue for a specific customer. After an LTE attach, the PCRF binds with P-GW #1, IMSI #1 and IPv6 #1. Then, the device tries to handoff and the AAA returns the wrong P-GW information MIPv6 Agent info. As expected, the ePDG picks the second P-GW and sends a Create Session Request to P-GW #2 with HI=1. This request also contains IPv6 #1 assigned the by P-GW #1. Therefore, P-GW #2 does not have the correct context. P-GW #2 treats this as a new session and it creates a new binding with the PCRF. Then, the PCRF binds with P-GW #2, IMSI #1 and IPv6 #2 and this replaces the correct one. The session is torn down on WLAN because the client did not receive a termination notice for the eUTRAN session. The connection is not broken on the eUTRAN and P-GW #1. There is an attempt to make a VoLTE call which fails because the PCRF does not have the bind for the IMSI and the first IPv6.

When an attach request comes from the s2b interface with HI=1 and there is no UE context in the demux, the attach request is accepted and a new session is formed on the s2b interface. Then, the network releases a PDN Connection on the LTE or the UE does not establish a PDN connection. The UE performs a Handover Attach on the WLAN and the ePDG utilizes the P-GW FQDN provided by the AAA for selecting the P-GW and indicates Handover in the Create Session Request. The P-GW did not have the existing LTE session. Therefore, the P-GW rejects the PDN connection request. In the standard behavior, this request is accepted and a new WLAN call is established. The ePDG rejects the UE PDN connections.

Licensed Behavior

When an attach comes from the s2b interface with HI=1 and there is no UE context in the demux, the attach request is rejected with the cause code Context Not Found. This new behavior can only be achieved by configuring s2b-ho-no-context. If this CLI is not configured, then new calls on the s2b interface will be accepted by default and a session is formed. HO is only rejected when a UE context does not exist with eGTP-C.

Important

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

`gtpc`

This command configures the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service. The new `s2b-ho-no-context` keyword is now available to reject Handoff calls on the s2b interface when eGTP-C does not have a UE Context.

```
configure
context context_name
egtp-service svc_name
   [no] gtpc reject s2b-ho-no-context
end
```

Notes:

- `s2b-ho-no-context`: Allows handoff calls on s2b interface, even when eGTP-C does not have a UE context.
- `no`: Rejects handoff calls on S2b interface when eGTP-C does not have a UE context.

CSCur51701 - Disconnect Reason Not Updated correctly For Saegw-collapsed call

Feature Changes

P-GW and SAEGW Session Disconnect Reason Not Updated Correctly for Multi Bearer Call

**Previous Behavior:** When the first dedicated bearer was released for P-GW and SAEGW calls for a multi bearer call, the disconnect reason was set for all bearers. Other bearers went down with different disconnect reasons and the new disconnect reason was not updated in the bearers. Therefore, the `show session disconnect` reason displayed the wrong output.

**New Behavior:** When the first dedicated bearer is released for P-GW and SAEGW call s for a multi bearer call, the disconnect reason is only set to specific bearers. After other bearers go down with a different disconnect reason, the new disconnect reasons is updated correctly in the bearers. Therefore, the `show session disconnect` reason will display the correct output.
CSCur65231 - Different disconnect reason is required for PCRF unreachable case

Feature Changes

Value Change for Diagnostics AVP in Rf Record

PMIP-P-GW RF now includes details of disconnect in Diagnostics.

Previous Behavior: The Diagnostics AVP used to have the value as
SNX_DISCONNECT_REASON_IMS_AUTHORIZATION_FAILED, even when PCRF was unreachable.

New Behavior: The Diagnostics field in Rf record will have separate values when PCRF initiates termination and when PCRF is unreachable.

CSCus06045 - gtpu-service echo-interval 'default' keyword should disable echo

Feature Changes

Change to 'default gtpu-service echo-interval' Command

Previous Behavior: When the default echo-interval command was entered, it would enable echo at 60 seconds interval, instead of disabling it. To disable the gtpu-service echo, the command no echo-interval was required to be entered.

New Behavior: Now, the commands default echo-interval and no echo-interval both disable gtpu-service echo.

Command Changes

default echo-interval

The command default echo-interval disables the gtpu-service echo-interval.
CSCus30437 - Std QCI(Non-GBR) wrngly incrmntd whn traffc dropd for GBR bearer in OCP

Feature Changes

Downlink Dropped Packets Shown for Proper Bearer

Previous Behavior: When subscriber session was in overcharge-protection state with overcharge-protection { drop-all | <cr> } configured, downlink dropped packets (for any bearer, dedicated or default) were incremented under default bearer.

New Behavior: When subscriber session is in overcharge-protection state with overcharge-protection { drop-all | <cr> } configured, downlink dropped packets for a bearer are properly incremented under the corresponding bearer, dedicated or default.

Customer Impact: Change in statistics for CLI commands show pgw-service statistics and show subs pgw-only full all when traffic dropped for GBR bearer in OCP.

CSCus74784 - No QOS-Change is sent to Gy on receiving now qos from Gx on 4G to 3G

Feature Changes

Bearer Control Mode Treated as Mixed Mode if CLI is Configured on APN

When Bearer Control Mode is not configured in APN, it is set as UE-ONLY. This is done when a new call or an already established Bearer Control Mode is not mixed mode even though NCQOS support from the SGSN and the UE is indicated by a NRSN flag and PCO in CPC or UPC.

Previous Behavior: If none or none-prefer-local-value was set under APN config, then the Bearer Control Mode was derived as UE-ONLY.

New Behavior: Now, none/none prefer-local-value will be treated as mixed mode when NCQOS support from SGSN and UE is indicated by a NRSN flag and PCO in CPC or UPC.

Customer Impact: Bearer Control Mode configured on APN as none or none prefer local value will be treated as mixed mode if NCQOS support from the SGSN and the UE is indicated by a NRSN flag and PCO in CPC or UPC.
CSCus82761 - Charging Id in GTPv2 S2b/S2a

Feature Changes

Charging ID sent in Create-Session-Response and Create-Bearer-Request

Introduced charging ID IE in S2b/S2a-GTPv2 as part of CDR support for 3GPP compliance for Wifi.

Previous Behavior: The P-GW did not send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.

New Behavior: The P-GW will send a charging-id in Create-Session-Response and Create-Bearer-Request over S2b/S2a.

CSCut09653 - 2 rules with different QCI/ARP are installed on single bearer: SM support

Feature Changes

Change in Call Flow Related to Update PDP Request from SGSN

Previous Behavior: An update PDP context request received from the SGSN with upgraded QoS was rejected with Bearer Control Mode MS/NW. If a PDP context was associated with a TFT containing packet filters set by the MS and GGSN, then the update PDP context request from SGSN with any change in QoS was rejected. A change or upgrade in QoS in UPC request was detected by comparing QoS based on traffic class. If there was no change in traffic class in UPC request, then it was accepted.

New Behavior: Now, the MS will not modify the QoS of a PDP context until this PDP context is associated with a TFT containing packet filters set by the MS. If the TFT also contains packet filters set by the P-GW/GGSN, then the MS is only allowed to modify the bit rate parameters in the QoS profile of that PDP Context. Therefore, an update PDP context request from the SGSN with changed QoS is rejected with Bearer Control Mode MS/NW. A change in QoS is detected by comparing QoS based on QCI. If there is a change in QCI in a UPC request, then it is rejected.
CSCut15652 - change-condition issue in Rf record when OCS/ Gy is down during CCR

Feature Changes

Different Session Disconnect Reason Due to Unreachability of Gy

**Previous Behavior:** When connection is terminated due to Gy failure, then session disconnect reason "failed-auth-with-charging-svc" was used.

**New Behavior:** Now, when connection is terminated due to Gy failure, session will disconnect with reason "disconnect-from-charging-server".

Performance Indicator Changes

show session disconnect-reasons

This command will now display the following as a reason in its output.

- Session Disconnect Statistics Total Disconnects

CSCut28557 - Assertion failure while handling MBReq

Feature Changes

New Disconnect Reason

Added a new disconnect-reason to the show session disconnect command.

**Related CDETS ID:** CSCuq74490

Performance Indicator Changes

show session disconnect-reasons

A new disconnect-reason has been added to show the number of times a call is terminated due to HI=1 not being received (Mandatory IE) during a WiFi to LTE handoff.

- disconnect-irat-fail-hi-missing(611)
Feature Changes

P-GW Statistics Added to Count Discarded DHCPv4 DISCOVER Due to AAA Conflicts

New counters have been added under DHCP Service statistics to track dropping of DISCOVER requests.

Configuration Applied to these use-cases:
Deferred IPv4 Address allocation is enabled. One of these two IPv4 allocation methods are configured under APN.

1. dhcp-proxy allocation
2. no-dynamic allocation

Use Case 1: AAA returns Framed IP Address

1. During initial attach, the UE has requested IPv6 allocation. UE has also requested IPv4 deferred allocation. P-GW allocates IPv6 and defers IPv4 allocation.
2. During this attach, the AAA (Radius) has returned Framed-IP-Address in Authentication Response.
3. UE sends DHCPv4 Discover.
4. P-GW drops DISCOVER as this use case is not supported.

New Counter Name: Deferred Address Allocation of AAA returned IP Not Supported

Use Case 2: AAA returns IP-Pool name

1. During initial attach, the UE has requested IPv6 allocation. UE has also requested IPv4 deferred allocation. P-GW allocates IPv6 and defers IPv4 allocation.
2. During this attach, the AAA (Radius) has returned IP-Pool name in Authentication Response.
3. UE sends DHCPv4 Discover.
4. P-GW proxies DISCOVER to DHCP server. DHCP server responds with an offer.
5. The offered IP is not present in the IP pool provided by AAA; therefore, P-GW drops DISCOVER.

New Counter Name: Deferred Address Allocated by DHCPv4 Server Not in AAA Provided IP Pool

Previous Behavior: When P-GW dropped UE's DISCOVER message due to compatibility issues with Radius Auth Response, it was not visible as there were no statistics.

New Behavior: When P-GW drops UE's DISCOVER message due to compatibility issues with Radius Auth Response, statistics are provided.
Performance Indicator Changes

System Schema

The following new counters have been added:

- discover-dis-def-alloc-of-aaa-provided-ip-not-supported

**show dhcp counters all**

The output of this command will now include the following statistics:

DHCP DISCOVER Discard Reasons

- Parse error
- Deferred Address Allocation of AAA returned IP Not Supported
- Deferred Address Allocated by DHCPv4 Server Not in AAA Provided IP Pool

**show dhcp statistics dhcp-service dhcp service name**

The output of this command will now include the following statistics:

DHCP DISCOVER Discard Reasons

- Parse error
- Deferred Address Allocation of AAA returned IP Not Supported
- Deferred Address Allocated by DHCPv4 Server Not in AAA Provided IP Pool

CSCut38233 - egtp modify-bearer-cmd-negotiate-qos not enforcing the authorized QoS

Feature Changes

Enforcement of Authorized QoS

**Previous Behavior:** During HO MBReq with APN AMBR, when QoS event triggers were not set or when PCRF was not reachable, APN AMBR values in MBReq were enforced.

**New Behavior:** During HO MBReq with APN AMBR, when QoS event triggers are not set or when PCRF is not reachable, APN AMBR values in MBReq are enforced only when PCRF authorized values are not present.
CSCut38800 - PGW sends CCR-U with RESOURCES_LIMITATION for VoLTE calls in 17.1 build.

Feature Changes

Handling of Collision of GnGp (LTE to GnGP GGSN) Handoff with Ongoing CBReq or UBReq Transaction

**Previous Behavior:** Initially, when P-GW initiated CBReq for bearer creation when RAR from PCRF was received and handoff to GGSN happened before CBRes came from S-GW, the call was diverted back to P-GW. In this case, if RAR was received for the same bearer creation (same Qos/ARP) then P-GW ignored RAR and did not initiate CBReq for the bearer creation.

**New Behavior:** P-GW aborts all pending transactions while performing handoff to GGSN. Further, RAR for the same Qos/ARP RAR requests are handled.

**Customer Impact:** Further, VoLTE calls would not be impacted if the GnGp handover happens when CBReq or UBReq was in process in the LTE access.

CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure

Feature Changes

Control of GTP Cause Being Sent in Create Session Response

**Previous Behavior:** If during initial call setup at P-GW (Create Session Request) PCRF rejects the call with 5xxx cause code, P-GW sends GTP cause "User Authentication Failure" in Create Session Response message. In 16.x and earlier StarOS releases, P-GW rejected the call with GTP cause "No Resources Available". The behavior above was implemented as an enhancement.

**New Behavior:** When Create Session Request message arrives at P-GW, CCR-I is sent to PCRF and PCRF rejects calls with 5xxx cause code in CCA-I. In this case, Create Session Response is sent with failure indicated by GTP cause code. A new CLI command has been introduced to control which GTP cause code is sent, "No Resources Available" or "User Authentication Failed", in Create Session Response message for this scenario. By default, "No Resources Available" is sent for this case; however, enabling the new command sends "User Authentication Failed" cause code in Create Session Response.
Command Changes

map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail

This is a new command that maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message.

configure
    context context_name
        pgw-service pgw_service_name
            [ default | no ] map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail
    end

Notes:

• default | no: Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.
CSCut47957 - New CLI requirement to map disc cause code for Gx Authentication Failure
PSF Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from PSF in StarOS 18 software releases.

- PSF Enhancements for 18.1, page 265

PSF Enhancements for 18.1

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

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

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

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

**CSCuh13901 - SFW counting license enforcement**

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

**Feature Changes**

**Stateful Firewall License Enforcement**

Licenses are used to limit the number of subscribers using a service and the resource manager/controller is the system which handles licensing issues. In previous releases, the SFW counting license is added to the ECSv2 counting license. Due to this scenario, more number of calls were allowed for a system with lesser ECSv2 counting licenses and few SFW counting licenses. For example, if a subscriber has 200 licenses of SFW and 300 licenses of ECSv2, it is considered as 500 licenses of ECSv2 by the resource manager. An SFW license can be considered as an ECSv2 + SFW license but the vice-versa is not true. This results in a case...
where the system would allow 500 SFW subscribers since the resource manager is agnostic to SFW as a service separate from ECSv2.

With this enhancement, SFW is added as an independent service in the resource manager/controller licensing framework. Given the above example, a subscriber can have a maximum of 500 ECSv2 + 0 SFW subscribers. The number of SFW subscribers can never exceed 200. CLI support is provided to disable the feature or drop the call when license limit is exceeded for a service.

**Command Changes**

**firewall license**

The *license* keyword is added to the *firewall* command in the ACS Configuration mode, to configure the Firewall license parameters.

```markdown
configure
  active-charging service *service_name*
    firewall license exceed-action { disable-feature | drop-call | ignore }
end
```

Notes:

One of the following parameters can be configured:

- **disable-feature**: Disables the service when license is exceeded.
- **drop-call**: Drops the call if call fails to get a Stateful Firewall license.
- **ignore**: Continues using the Stateful Firewall license even if license is exceeded. This is the default behavior.

**Performance Indicator Changes**

**show resources session**

The following fields will be displayed in the output of this command to show the resource information for Subscriber Firewall sessions:

- Per Subscriber Firewall information:
  - Firewall Service
  - In Use
  - Max Used
  - Limit
  - License Status

**show task info**

The following fields will be displayed in the output of this command to display the usage information for Subscriber Firewall sessions:
Per Subscriber Firewall sessions
- Total sessions
- Status

CSCuo78207 - [NAT] Stats to display MAX port usage of subscribers

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

Feature Changes

Port Utilization by Subscribers

In a NAT call, ports are allocated to a subscriber in chunks. The size of the chunk is configured at the NAT pool from which the NAT IP is allocated. In this enhancement, statistics are added to find out the number of ports utilized by a subscriber. The maximum number of ports that were required by a subscriber at any point of time is recorded.

The port utilization data of subscribers is aggregated at the NAT pool level. The number of ports are grouped into buckets of size 8. There are 9 defined port buckets — [0-8], [9-16], [17-24], [25-32], [33-40], [41-48], [49-56], [57-64] and [>=65]. The first bucket [0-8] includes not-on-demand calls, that is, subscribers who are allocated a port chunk without using any ports at all will fall into the first bucket. The last bucket [>=65] includes all subscribers using greater than 64 ports.

Previous Behavior: The `show active-charging nat statistics` CLI command does not display statistics for maximum port usage by a subscriber.

New Behavior: The following enhancements have been done in this release.

- The `show active-charging nat statistics` CLI command has been enhanced to display the distribution of maximum port usage by subscribers at NAT pool level.
- The `show active-charging firewall statistics verbose` CLI command has been enhanced to display more granular statistics for packets dropped due to non-availability of port chunks and due to maximum usage limit of port chunks.

Performance Indicator Changes

show active-charging firewall statistics verbose

The following counters are added to the output of this command:

- Packets dropped due to MAX port chunks reached
- Packets dropped due to non-availability of port chunks
show active-charging nat statistics

The following counters are added to the output of this command:

- Ports distribution:
  - Max no. of ports used
  - Total no. of Subscribers
SAEGW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from SAEGW in StarOS 18 software releases.

• SAEGW Enhancements for 18.5, page 269
• SAEGW Enhancements for 18.4, page 272
• SAEGW Enhancements for 18.3, page 272
• SAEGW Enhancements for 18.2, page 272
• SAEGW Enhancements for 18.1, page 278

SAEGW Enhancements for 18.5

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

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

Command Changes - changes to any of the CLI command syntax. For details, refer to the 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 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**

**DHCP Options 1, 3, 6, 28, 43, 60 and 61 Relayed Between UE and External DHCP Server**

Related CDETS = CSCuv78874 - DHCP opt 1,3,6,28,43,60 and 61 between UE to Ext DHCP Server

Related Products: P-GW, SAEGW

**Feature Changes**

**DHCP Deferred IPv4 Enhancements**

Previously, when the P-GW was configured to allocate IPv4 addresses via an external DHCP server, it did not relay any DHCP parameters between the UE and the external DHCP server. This resulted in the UE not being able to configure network parameters per the external DHCP server-provided options.

Now, there will be an exchange of certain DHCP options between the UE and the external DHCP server via the P-GW. This occurs when the UE allocates a deferred IPv4 address for a PDN via an external DHCP Server where the P-GW acts as a DHCP Proxy for UE. The P-GW behaves as an independent DHCP Server towards the UE and at the same time acts as a DHCP Client towards the external DHCP Server while fetching the IPv4 address for the UE. The new options provided are:

- Subnet Mask <IPv4 address>
- Broadcast Address <IPv4 address>
- Default Gateway <IPv4 address>
- Client Identifier <hexadecimal number>
- Vendor Specific Info <string>
- Vendor Class Id <string>

**Previous Behavior:** The P-GW relayed only the IP-address from the external DHCP server to the UE when configured with IP address allocation as a proxy with a deferred address.

**New Behavior:** The P-GW supports relaying certain External DHCP Server provided options (1, 3, 6, 28, and 43) to the UE along with the IPv4-Address when Deferred Address Allocation is configured with IP-Addr alloc Proxy mode. The P-GW will also relay UE-provided options (60, 61) to the external DHCP server.

**Customer Impact:** Overall memory usage will increase as DHCP options 43, 60 and 61 each occupy a maximum size of 255 bytes. The Call Recovery Memory footprint will also increase for recovery of these options. These memory requirements do not affect any non-DHCP P-GW calls.
Limitations

Please note the following limitations of this feature in StarOS release 18.5:

- Online DHCP Service removal has a known issue (CSCuw78497) and should not be tried.
- The DHCP Server priority and address configuration should be in order. Multiple DHCP servers with a different address but the same priority would lead to operational problems.
- An external DHCP server outage can cause inconsistencies for leased addresses between the P-GW DHCP client and the DHCP server.
- If the DHCP server sends a NAK when the P-GW is waiting for an ACK, it will cause a known issue (CSCux73863). Specific customers would be required to ensure the correct configuration based on Client-Id in the DHCP server so that this condition will never occur.
- Planned DPC migration (Demux DPC) has a known issue (CSCux75717) and should not be tested with this feature.
- This feature should not be tested with ICSR.
- DHCP lease, renewal, and rebind timers must be in synchronization from the client side FSM, server-side FSM, and DHCP server to avoid known issues like CSCux76810 that will further impact the continuity of the session.

Performance Indicator Changes

show dhcp full all

The output of this command has been enhanced to provide additional DHCP-specific information when the P-GW is configured to act as a DHCP server for DHCP Deferred IPv4 Enhancements:

- Subnet Mask <IPv4 address>
- Broadcast Address <IPv4 address>
- Default Gateway <IPv4 address>
- Client Identifier <hexadecimal number>
- Vendor Specific Info <string>
- Vendor Class Id <string>

Correction for Missing QoS/AMBR AVP in CCA to PCEF

Related CDETS = CSCuw26535 - AMBR missing in CSRsp to ePDG in LTE to WiFi if AMBR absent in CCA

Applicable Products: SAEGW

The fix implemented for CSCuw26535 has resulted in a behavior change.

Previous Behavior: If the If the QoS-Information AVP has been supplied previously but is omitted in a Diameter message or AVP, then Access side Requested QoS values are enforced and previously PCRF authorized QoS are overwritten with new Access side Requested QoS values.
New Behavior: If the QoS-Information AVP has been supplied previously but is omitted in a Diameter message or the AVP, the previous information remains valid. If the QoS-Information AVP has not been supplied from the PCRF to the PCEF previously and is omitted in a Diameter message or AVP, no enforcement of the authorized QoS is performed. This behavior is per 3GPP TS 29.212, section 5.3.16.

Subscriber Session Preserved in Case of P-GW Failing to Renew IP Address

Related CDETS = CSCux53291 - Session getting cleared on renew failure

Applicable Products: SAEGW

The fix implemented for CSCux53291 has resulted in a behavior change.

Previous Behavior: In the event of a deferred IP address allocation for an IPv4/IPv6 PDN, the entire call line goes down when the P-GW failed to renew the IP address after the lease expired.

New Behavior: For a deferred IP address allocation case where the IPv4 address lease renewal fails, only the IPv4 portion of the PDN will go down. The IPv6 portion of the PDN will stay up. This results in the calling staying active.

Customer Impact: The subscriber session will stay up instead of going down. Subscriber loss is avoided in the event of lease renewal failures.

SAEGW Enhancements for 18.4

There are no SAEGW enhancements for this release.

SAEGW Enhancements for 18.3

There are no SAEGW enhancements for this release.

SAEGW Enhancements for 18.2

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 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 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

**CSCup18703 - 18.2 - Collision counter support in GTP layer**

**Feature Changes**

**Collision Counter Support in the 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 tracked by statistics and handled based on a pre-defined action for each message collision type.

If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will still see the respective collision statistics if they occur.

**Performance Indicator Changes**

`show egtp 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: SGW (S4/S11), SGW (S5), or PGW (S5).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type)**: The new procedure and message type.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - **No Collision Detected**
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old**: Abort the original message handling and processes the new message.
- **Reject New**: The new message is rejected, and the original (old) message is processed.
- **Silent Drop New**: Drop the new incoming message, and the old message is processed.
- **Parallel Hndl**: Both the original (old) and new messages are handled in parallel.
- **Buffer New**: The new message is buffered and processed once the original (old) message processing is done.

- **Counter**: The number of times each collision type has occurred.

The Message Collision Statistics section of the command output only appears if any of the collision statistics have a counter total that is greater than zero.

**Sample output:**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Old Proc (Msg Type)</th>
<th>New Proc (Msg Type)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SGW(S5)</td>
<td>NW Init Bearer Create (95)</td>
<td>NW Init PDN Delete (99)</td>
<td>Abort Old 1</td>
</tr>
</tbody>
</table>

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.

The action that is carried out due to this collision at eGTP-C is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the PDN Delete procedure. The Counter total of 1 indicates that this collision happened only once.

**Feature Changes**

**GTP-based S2b Interface Support on the SAEGW in StarOS Version 18.2**

GTP-based S2b interface support now is supported fully on the SAEGW in StarOS release 18.2. The S2b interface connects the P-GW service of the SAEGW with the ePDG. The UE tries to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies. Therefore, the UE can have independent PDN connections via multiple access types. The access types supported are 4G and WiFi.

The S2b interface implementation supports the following:

- UE connecting to PDN via WiFi access
- UE multiple PDN connections
- Initial Attach
- LTE to WiFi Handoff
- WiFi to LTE Handoff
GTP-based S2b interface support for the SAEGW is a license-controlled feature. Contact your Cisco account or support representative for licensing information.

For more detailed information on this feature, refer to the SAE-GW Administration Guide, StarOS Release 18.

**Command Changes**

```markdown
interface-type interface-pgw-ingress
```

The `s2b` option has been added to the `interface-type interface-pgw-ingress` command in eGTP Service Configuration Mode to provide GTP-based S2b interface support on the SAEGW.

```markdown
config
c
context ingress_context_name
egtp-service egtp_service_name
    interface-type interface-pgw-ingress s2b
d
```

Disable S2b interface support by entering the following commands:

```markdown
config
c
context ingress_context_name
egtp-service egtp_service_name
    interface-type interface-pgw-ingress
d
```

**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-s2bgtptolteatt`
- `pgw-handoverstat-s2bgtptoltesucc`
- `pgw-handoverstat-s2bgtptolefail`
- `pgw-handoverstat-ltetos2bgtpatt`
- `pgw-handoverstat-ltetos2bgtpsucc`
- `pgw-handoverstat-ltetos2bgtpfail`

**show saegw-service statistics all function pgw**

The output of this command has been enhanced to provide statistics related to successes, failures, and attempts for various S2bGTP-to-LTE and LTE-to-S2bGTP handovers for all P-GW SAEGW services, including:

- S2bGTP-to-LTE handover
• Attempted
• Succeeded
• Failed

• LTE-to-S2bGTP handover
  • Attempted
  • Succeeded
  • Failed

show subscribers saegw-only full all

The output of this command has been enhanced to provide S2b call-related information for P-GW subscribers:

• Username
  • SAEGW Call mode
  • Subscriber Type
  • Status
  • State
  • Bearer State
  • Connect time

• S2B Interface
  • pgw c-addr
  • pgw u-addr
  • pgw c-teid
  • pgw u-teid
  • ePdg c-addr
  • ePdg u-addr
  • ePdg c-teid
  • ePdg u-teid

• input pkts
• input bytes
• input bytes dropped
• input pkts dropped
• output pkts
• output bytes
CSCuu17820 - S2B: GW is sending incorrect Event Trigger in case of Wifi to LTE HO

Feature Changes

S2b Event Trigger Corrected

The fix implemented for CSCuu17820 has resulted in a behavior change.

Previous Behavior:

1. During a WiFi (S2b) to LTE handover, the PCEF was sending the Gx event trigger "DEFAULT_EPS_BEARER_QOS_CHANGE (20)" even when there was no Default EPS bearer QoS change in the CSR for handovers.
2. Default EPS bearer QoS change detection was not supported for S2a <--> LTE during the handover.

New Behavior:

1. During WiFi (S2b) to LTE handover, the PCEF sends a Gx event trigger "DEFAULT_EPS_BEARER_QOS_CHANGE (20)" only when there is an actual Default EPS bearer QoS change during handover.
2. Default EPS bearer QoS change detection is supported for S2a <--> LTE during handover.

Customer Impact: Operators will be able to see the correct Default EPS bearer QoS change detection during a WiFi (S2a/S2b) to LTE handover.

CSCuu31324 - Idle subscribers not being cleared from SPGW

Feature Changes

Idle Subscribers Cleared Properly

Some subscribers were not being cleared if a suspend notification was received on the call and before receiving the resume notification the 4G call received an MBR or UPC (for a 4G to 3G handoff).

Previous Behavior: If a UE went to the suspended state in 4G, the idle timer was not restarted if an MBR or UPC (for a Gn/Gp handoff) was received before the resume notification. This resulted in some idle subscribers not being cleared.

New Behavior: If a UE goes to the suspended state in 4G, the idle timer is restarted if an MBR or UPC (for Gn/Gp handoff) is received before the resume notification.

Idle subscribers are now cleared properly.
CSCuu37427, CSCut14324 - Assertion failure egtpc_handle_create_sess_req_msg_at_sgw_ingress

Feature Changes

Parallel Create Session Requests Processed Correctly

The fix implemented for CSCuu37427 has resulted in a behavior change.

Previous Behavior: When two parallel CSReq with different EBI and 0 TEID were received from the S4-SGSN, the second CSReq was rejected from the S-GW with the cause "No Resource Available."

New Behavior: When two parallel CSReqs with different EBI and 0 TEID are received from the S4-SGSN, both of the CSReqs are processed and the PDNs are created successfully at the S-GW.

1 Operators will see that both the PDNs are created successfully after the fix if the two CSReqs are received from the S4-SGSN with 0 TEID and different EBI.
2 If two parallel CSReqs are received from the MME, then the old behavior of rejecting the second CSReq with the cause "No Resource Available" is applicable.
3 If one CSReq is received from the MME and the other from the S4-SGSN, or vice-versa, with the same or different EBI, then context replacement is triggered and the second CSReq results in the replacement of the existing PDN with a new PDN.

SAEGW Enhancements for 18.1

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 ASR 5x00 Command Line Interface Reference for this release.

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

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

CSCuh13685, CSCuo97254 - Overload controls (congestion prevention by signalling)

Feature Changes

**R12 Load and Overload Support**

R12 Load and Overload Support Control has been implemented on the SAEGW. For details on this feature, refer to the S-GW Enhancements chapter in this document.

CSCur61470 - S2B Support on SAE-GW

Feature Changes

**GTP-based S2b Interface Support on the SAEGW**

Important  
GTP-based S2b Interface Support on the SAEGW is not currently supported. Full support for S2a and S2b calls is planned for a future release.

CSCut07427 - [SAEGW-stats] display changes needed for saegw-service stat

Feature Changes

**Change in Display for show saegw-service statistics all function pgw verbose**

The output of `show saegw-service statistics all function pgw verbose` has been enhanced. IPv4v6 PDN Data Statistics now are now identified as IPv4 and IPv6 PDNs for Uplink and Downlink traffic.

**Previous Behavior:** Previously, IPv4v6 PDN Data Statistics were listed as Uplink/Downlink packets and bytes without identifying which came from IPv4 PDNs and which came from IPv6 PDNs.
**New Behavior:** The output of this command has been enhanced to break out Total Pkts and Total Bytes for Uplink and Downlink traffic by IPv4 and IPv6 PDNs.

**Customer Impact:** The output of this command has been changed. Operators may have to adjust automation scripts based on this new output, if any automation scripts are being used.

## Performance Indicator Changes

### show saegw-service statistics all function pgw verbose

The output of this command has been enhanced to break out Total Pkts and Total Bytes for Uplink and Downlink traffic by IPv4 and IPv6 PDNs.

**Old Output:**

```
Ipv4v6 PDN Data Statistics
Uplink:
  Total Pkts: Total Pkts:
  Total Bytes: Total Bytes:
Downlink:
  Total Pkts: Total Pkts:
  Total Bytes: Total Bytes:
```

**New Output:**

```
Ipv4v6 PDN Data Statistics
Uplink:
  Total Pkts v4: Total Pkts v4:
  Total Bytes v4: Total Bytes v4:
  Total Pkts v6: Total Pkts v6:
  Total Bytes v6: Total Bytes v6:
Downlink:
  Total Pkts v4: Total Pkts v4:
  Total Bytes v4: Total Bytes v4:
  Total Pkts v6: Total Pkts v6:
  Total Bytes v6: Total Bytes v6:
```

---

**CSCut09582 - [18.0]: gy iface is not shown in func-pgw in template for saegw NE**

## Feature Changes

### Support for Gy Interface in Session Tracing on the SAEGW

Session tracing for the Gy interface is now available.

**Previous Behavior:** There was no support for Gy interface tracing on the SAEGW.

**New Behavior:** Support for tracing the Gy interface on the SAEGW is now available.

## Command Changes

**session trace random**

The `gy` interface has been added to this command as a function of the `session trace random` command in the func-pgw interface keyword for random tracing.

```
configure
session trace random number network-element saegw { func-pgw interface {all | gx | s2a | s2b | s2c | s5
```
template-session trace

The gy interface has been added to this command as a function of the func-pgw interface keyword.

configure
  template session trace network element saegw template name template_name
    func-pgw interface gy
    no func-pgw interface gy
  end

Performance Indicator Changes

show session trace template network-element saegw all

The output of this command has been enhanced to show the gy interface, if it has been configured as part of a session trace template.

NE Type: SAEGW
Traced Interfaces
  PGW
  Gy

CSCut28557 - Assertion failure while handling MBReq

Feature Changes

New Disconnect Reason disconnect-irat-fail-hi-missing(611)

The fix for CSCut28557 has resulted in the creation of a new disconnect reason.

Previous Behavior: During a WiFi to LTE handoff, if an MBR with HI=1 is not received then the call continues.

New Behavior: During a WiFi to LTE handoff, if an MBR with HI=1 is not received, then the call is dropped with the new disconnect reason disconnect-irat-fail-hi-missing(611).

Customer Impact: The call will be dropped during handoff if the MME/SGW sends an incorrect MBR.

Performance Indicator Changes

show session disconnect-reasons

A new disconnect reason has been added to show the number of times a call is terminated due to HI=1 not being received (Mandatory id) during a WiFi to LTE handoff.

- disconnect-irat-fail-hi-missing(611)
CSCu28557 - Assertion failure while handling MBReq
CHAPTER 17

SaMOG Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from SaMOG in StarOS 18 software releases.

• SaMOG Enhancements for 18.5, page 283
• SaMOG Enhancements for 18.4, page 286
• SaMOG Enhancements for 18.2, page 298
• SaMOG Enhancements for 18.0, page 303

SaMOG Enhancements for 18.5

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

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

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

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

Important

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

• AAA Enhancements
• CF Enhancements
• ECS Enhancements
• Firewall Enhancements
• GTPP Enhancements
Feature Changes

Optimized SaMOG Web Authorization

In an earlier release, the SaMOG Web Authorization feature was introduced to enable SaMOG gateway to authenticate a subscriber’s user equipment (UE) over a web portal, based on a user ID and password combination, a one-time password, or a voucher. On successful authentication, the AAA server stores the subscriber profile (APN, IMSI, QoS) from the HLR/HSS for the subscriber’s device, and SaMOG establishes the network connection for the UE.

The web-based authorization occurs in two phases:

• **Pre-Authentication Phase:** SaMOG assigns a local IP address and redirects the UE traffic to a web portal for subscriber authentication. On successful authentication, the subscriber session is disconnected by SaMOG on receiving a RADIUS disconnect message from the AAA server.

• **Transparent Auto-logon (TAL) Phase:** The subscriber profile is cached on the AAA server for a designated duration to enable subscribers to reconnect without further portal authentication, thus enabling a seamless user experience. During this phase, SaMOG can allocate IPv4, IPv6, or IPv4v6 addresses to the UE (The allocated IP address might be different than the one assigned during the pre-authentication phase).

With this release, the SaMOG Optimized Web Authorization feature is introduced to provide a seamless experience to the subscriber by continuing the SaMOG session after the Pre-Authentication phase with no session disconnection. This is achieved using the SaMOG Local Breakout – Enhanced feature where a P-GW is collocated with SaMOG in the same chassis.

The address assigned to the subscriber’s UE is retained by maintaining the same IP address range pools within a single Gi context, and shared across the P-GW service and SaMOG service. The SaMOG service uses the VPNMgr address transfer feature to transfer the IP address or IPv6 prefix to the P-GW service.

This feature is supported on both EoGRE and PMIPv6 access types, with IPv4 and IPv6 transports to the WLC.

License

The SaMOG Optimized Web Authorization feature is currently supported on the SaMOG general license (4G).
Important Contact your Cisco account representative for detailed information on specific licensing requirements.

Command Changes

newcall

The `newcall` command under the P-GW Service Configuration mode enables P-GW to accept or reject requests for a static IP address if the address is already in use by another session. The SaMOG service transfers the IPv4 address or IPv6 prefix (if applicable) to the P-GW service in order to retain the same IP address range pool specified under the Gi context.

The `duplicate-subscriber-requested-address` is an existing keyword that can be used to enable P-GW service to accept or reject an existing IP address that is in use by another session.

With this release the `duplicate-subscriber-requested-address-v6` keyword has been introduced to enable the P-GW service to accept or reject an existing IPv6 prefix that is in use by another session.

```
config
  context context_name
    pgw-service service_name
      newcall { duplicate-subscriber-requested-address |
        duplicate-subscriber-requested-address-v6 } { accept | reject } |
      default newcall { duplicate-subscriber-requested-address |
        duplicate-subscriber-requested-address-v6 }
      end
```

Notes:

- **accept**: Specifies that the old session with the requested address will be ended to accept the new session with the same address.
- **reject**: Specifies that the new session requesting the same address will be rejected.
- **Default**: reject

Performance Indicator Changes

show samog-service statistics

The following fields have been introduced under the "Non-EAP Session Stats" section of the output of this command in support of the Optimized Web Authorization feature:

- Post-authentication Calls
  - Attempted
  - Success
  - Failure

- Locally Terminated PDNs
show subscriber samog-only full

The "Web authorization phase" field has been introduced to the output of this command in support of the Optimized Web Authorization feature:

- Web Authorization: Yes
  - Web authorization phase: { Pre-Auth | Post-Auth }

SaMOG Enhancements for 18.4

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

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

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

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

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
Feature Changes

**Important**
This enhancement is applicable to 18.4.3 and later releases.

**NAS-Identifier Support for SWw Interface**

Prior to Release 18.4, the RADIUS attribute "NAS-Identifier" towards WLC/Access-Point over the SWw Interface in RADIUS protocol was not supported by SaMOG.

With this release, SaMOG supports the RADIUS attribute "NAS-Identifier" in the RADIUS Authentication and Accounting messages, as defined by RFC 2865. The Access point/WLC can include the NAS-Identifier AVP either in the Authentication or Accounting messages (Start/Interim). SaMOG supports a 64-byte string NAS-Identifier value and validates string formats only. SaMOG includes the "NAS-Identifier" attribute in the Disconnect Message towards the WLC/Access point (if received from WLC) during UE (DHCP-release) initiated detach and network initiated disconnect procedures or admin clear.

**Performance Indicator Changes**

`show subscribers samog-only full`

The output of this command is modified to display the following field under the *MRME Subscriber Info* section:

- NAS-Identifier

**CSCuv92889 - [SaMOG] - AAA-Failure-Indication AVP support needed by SaMOG**

Refer the *AAA Enhancements for 18.4* section of this guide for more information on this feature.
Feature Changes

IPv6 Transport Support Using the S2a GTPv2 Interface

In earlier releases, SaMOG provided seamless mobility between the 3GPP EPC network and WLANs for EPS (Evolved Packet System) services via a GTPv2-based S2a interface using IPv4 addresses.

With this release, SaMOG supports IPv6 transport between SaMOG and P-GW over the EoGRE and PMIPv6 access types. SaMOG can now bind IPv6 and IPv4 addresses in the EGTP and GTPU services associated with the CGW service. SaMOG DNS can query P-GW IPv6 addresses and support static IPv6 address allocation from the AAA server. Session recovery for PDN sessions on the IPv6 transport are now supported.

Supported EGTP Bind Addresses

<table>
<thead>
<tr>
<th>Bind Address (EGTP Service)</th>
<th>Supported by SaMOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single IPv4 Address</td>
<td>Yes</td>
</tr>
<tr>
<td>Single IPv6 Address</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple IPv4 address</td>
<td>No</td>
</tr>
<tr>
<td>Multiple IPv6 address</td>
<td>No</td>
</tr>
<tr>
<td>Mix of IPv4 and IPv6 address</td>
<td>No</td>
</tr>
</tbody>
</table>

Performance Indicator Changes

SaMOG Schema

The following bulk statistics counters are introduced in support of this feature:

- cgw-s2a-gtpu-ipv4-in-ipv4-uplink-total-pkts
- cgw-s2a-gtpu-ipv4-in-ipv4-uplink-total-bytes
- cgw-s2a-gtpu-ipv4-in-ipv4-uplink-drop-pkts
- cgw-s2a-gtpu-ipv4-in-ipv4-uplink-drop-bytes
- cgw-s2a-gtpu-ipv4-in-ipv4-downlink-total-pkts
- cgw-s2a-gtpu-ipv4-in-ipv4-downlink-total-bytes
- cgw-s2a-gtpu-ipv4-in-ipv4-downlink-drop-pkts
- cgw-s2a-gtpu-ipv4-in-ipv4-downlink-drop-bytes
• cgw-s2a-gtpu-ipv6-in-ipv4-uplink-total-pkts
• cgw-s2a-gtpu-ipv6-in-ipv4-uplink-total-bytes
• cgw-s2a-gtpu-ipv6-in-ipv4-uplink-drop-pkts
• cgw-s2a-gtpu-ipv6-in-ipv4-uplink-drop-bytes
• cgw-s2a-gtpu-ipv6-in-ipv4-downlink-total-pkts
• cgw-s2a-gtpu-ipv6-in-ipv4-downlink-total-bytes
• cgw-s2a-gtpu-ipv6-in-ipv4-downlink-drop-pkts
• cgw-s2a-gtpu-ipv6-in-ipv4-downlink-drop-bytes
• cgw-s2a-gtpu-ipv4-in-ipv6-uplink-total-pkts
• cgw-s2a-gtpu-ipv4-in-ipv6-uplink-total-bytes
• cgw-s2a-gtpu-ipv4-in-ipv6-uplink-drop-pkts
• cgw-s2a-gtpu-ipv4-in-ipv6-uplink-drop-bytes
• cgw-s2a-gtpu-ipv4-in-ipv6-downlink-total-pkts
• cgw-s2a-gtpu-ipv4-in-ipv6-downlink-total-bytes
• cgw-s2a-gtpu-ipv4-in-ipv6-downlink-drop-pkts
• cgw-s2a-gtpu-ipv4-in-ipv6-downlink-drop-bytes
• cgw-s2a-gtpu-ipv6-in-ipv6-uplink-total-pkts
• cgw-s2a-gtpu-ipv6-in-ipv6-uplink-total-bytes
• cgw-s2a-gtpu-ipv6-in-ipv6-uplink-drop-pkts
• cgw-s2a-gtpu-ipv6-in-ipv6-uplink-drop-bytes
• cgw-s2a-gtpu-ipv6-in-ipv6-downlink-total-pkts
• cgw-s2a-gtpu-ipv6-in-ipv6-downlink-total-bytes
• cgw-s2a-gtpu-ipv6-in-ipv6-downlink-drop-pkts
• cgw-s2a-gtpu-ipv6-in-ipv6-downlink-drop-bytes

**show samog-service statistics**

The output of this command is modified to display the following fields under the *S2A-GTP Total Data Statistics* section:

- Uplink:
  - Total Pkts:
  - IPv4 Pkts (IPv4):
  - IPv4 Pkts (IPv6):
  - IPv6 Pkts (IPv4):
  - IPv6 Pkts (IPv6):
• Total Bytes:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):
  • Total Dropped Pkts:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):
  • Total Dropped Bytes:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):

• Downlink:
  • Total Pkts:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):
  • Total Bytes:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):
  • Total Dropped Pkts:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
  • IPv6 Pkts (IPv4):
  • IPv6 Pkts (IPv6):
  • Total Dropped Bytes:
  • IPv4 Pkts (IPv4):
  • IPv4 Pkts (IPv6):
show subscribers samog-only full

The output of this command is modified to display the following fields under the CGW Subscriber Info section:

- pgw c-addr: IPv6 Address
- pgw u-addr: IPv6 Address
- cgw s2a c-addr: IPv6 Address
- cgw s2a u-addr: IPv6 Address

CSCuv74182 - [SaMOG] - IPv6 Transport Interface support for EoGRE Access-Type

Feature Changes

IPv6 Transport Support Using EoGRE Access Type

With this release, the SaMOG Gateway supports IPv6 transport between the WLC/Access Point (AP) and the SaMOG gateway for trusted Wi-Fi subscribers using the EoGRE access type. This enables SaMOG Gateway to support a rapidly increasing number of subscribers accessing the internet via mobile devices, and technologically advanced (example, Internet of Things) internet-enabled devices (sensors, machine-readable identifiers) that demand high network address assignments.

The access side peers (WLC/AP) and SaMOG communicate over an IPv6 transport, and the data travels over the tunnel between IPv6 endpoints.

Command Changes

bind

The bind command configures IP address(es) for the LMA driver.

Use the ipv4-address and ipv6-address keywords to configure the CGW service with IPv6 bind addresses. This enables IPv6 transport between the WLC and SaMOG for the EoGRE interface.
no bind { ipv4-address | ipv6-address | ipv6-address | ipv4-address | }
end

Notes:

• *ipv4_address* must be an IPv4 address expressed in dotted-decimal notation.
• *ipv6_address* must be an IPv6 address expressed in colon (or double-colon) notation.
• IPv4 and/or IPv6 address(es) can be bound to the CGW service.
• The CGW service is started even when one of the address is bound.
• Both addresses (IPv4/IPv6) can be bound to the CGW service using either one command, or two separate commands.
• When a second address is configured, the service restarts and existing sessions are lost for the other bind address.

Performance Indicator Changes

SaM0G Schema

The following bulk statistics counters are introduced in support of this feature:

• cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv4-pkts
• cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv4-bytes
• cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv6-pkts
• cgw-sessstat-eogre-tunnel-data-receive-ipv6-inipv6-bytes
• cgw-sessstat-eogre-tunnel-data-receive-drop-errors
• cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv4-pkts
• cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv4-bytes
• cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv6-pkts
• cgw-sessstat-eogre-tunnel-data-send-ipv6-inipv6-bytes

The following bulk statistics counters are modified to support this feature:

<table>
<thead>
<tr>
<th>Counters in Earlier Releases</th>
<th>Modified Counters in Current Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-pkts</td>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv4-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv4-bytes</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv6-pkts</td>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv6-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv6-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-receive-ipv4-inipv6-bytes</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-pkts</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv4-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv4-bytes</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv6-pkts</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv6-bytes</td>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-inipv6-bytes</td>
</tr>
</tbody>
</table>
### Counters in Earlier Releases

<table>
<thead>
<tr>
<th>Modified Counters in Current Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv6-pkts</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv4-bytes</td>
</tr>
<tr>
<td>cgw-sessstat-eogre-tunnel-data-send-ipv6-bytes</td>
</tr>
</tbody>
</table>

**show cgw-service all**

The output of this command is modified to display the following fields:

- Bind IPv4 Address
- Bind IPv6 Address

**show subscribers samog-only full**

The output of this command is modified to display the following field under the *CGW Subscriber Info* section:

- care-of-addr

**show samog-service all**

The output of this command is modified to display the following field:

- Associated DHCPv6 service

**show samog-service statistics**

The output of this command is modified to display the following fields:

**EoGRE Data Statistics:**

- Tunnel Data Received:
  - Total Packets
  - IPv6 EoGRE(IPv4)
  - IPv4 EoGRE(IPv6)
  - Total Bytes
  - IPv6 EoGRE(IPv4)
  - IPv4 EoGRE(IPv6)

- Tunnel Data Sent:
  - Total Packets
  - IPv6 EoGRE(IPv4)
Feature Changes

**SaMOG Web Authorization IPv6 Support for UE (Pre-Authentication Phase)**

The SaMOG Web Authorization feature was introduced in an earlier release as an alternative to EAP-SIM/AA/AKA'-based authentication where the subscriber's user equipment (UE) is authenticated over an external web portal before establishing the network connection. This feature has two phases:

- **Pre-Authentication Phase:** SaMOG supports local IP address assignment and redirects the UE traffic to an external web portal where the subscriber authenticates with a username and password combination, a one-time password, or a voucher.

- **Transparent Auto-logon (TAL) Phase:** SaMOG caches the subscriber profile in the AAA server for a designated duration to enable subscribers to reconnect without further portal authentication, thus enabling a seamless user experience. During this phase, SaMOG can allocate IPv4, IPv6, or IPv4v6 addresses to the UE.

**Previous Behavior:** In earlier releases, SaMOG can allocate only IPv4 addresses to the UE during the Pre-Authentication Phase.

**New Behavior:** With this release, SaMOG can allocate IPv4, IPv6, or IPv4v6 addresses to the UE during the Pre-Authentication Phase.

**Diameter Changes**

The following AVPs are introduced as part of the Diameter AA-Answer message in the MRME StA Dictionary:

- **Framed-IPv6-Pool:** The AAA server uses this attribute to send the IPv6 pool-name configured in the Gi context. SaMOG uses this IPv6 pool-name to allocate the IPv6 prefix during the Pre-Authentication Phase.

- **SN1-IPv6-Primary-DNS:** The AAA server uses this attribute to send the IPv6 address of the primary DNS server in the ADDRESS format.

- **SN1-IPv6-Secondary-DNS:** The AAA server uses this attribute to send the IPv6 address of the secondary DNS server in the ADDRESS format.
Command Changes

ipv6 address

With this release, the `ipv6 address` command is introduced under the APN Profile Configuration mode to specify the IPv6 pool-name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in the Diameter AA-Answer message. SaMOG uses the configured IPv6 prefix in the Gi context with this IPv6 pool-name.

```configure
apn-profile profile_name
  [no] ipv6 address prefix-pool pool_name
end```

Performance Indicator Changes

`show apn-profile full name profile_name`

The output of the `show apn-profile full name` command is modified to display the following field:

- [SaMOG] IPv6 Prefix Pool Name

CSCuw31457 - [SAMOG] Provide DHCP lease time configuration of WebAuth pre-auth calls

Related CDETS ID = CSCuw55736

Feature Changes

SaMOG Web Authorization DHCP Lease Time Configuration

With the SaMOG Web Authorization feature, during the pre-authentication phase, SaMOG allocates an IP address to the UE and redirects the UE traffic to an external web portal for authentication. When authentication completes, SaMOG disconnects the UE from the WiFi.

The UE then automatically reconnects to WiFi, and SaMOG obtains a new IP address for the UE using a GTP tunnel towards P-GW (Transparent Auto-logon (TAL) phase). At this stage, the UE is expected to send a DHCP Request/Discover message to learn the new IP address (as WiFi was disconnected and reconnected).

Previous Behavior: Some UEs might not initiate a DHCP transaction after the WiFi reconnection. The UE might still hold the IP address allocated during the pre-authentication phase, instead of the new IP address allocated by P-GW during the TAL phase. This is due to the infinite lease period allowed by SaMOG in the DHCP Offer message sent to the UE.

New Behavior: The IP address for the UE is allocated with a short lease duration to force the UE to initiate the DHCP request after the pre-authentication phase disconnection. The short lease duration can be configured using the `dhcp lease` command under the APN Profile Configuration mode.
Command Changes

dhc lease

With this release, the `dhc lease` command is introduced under the APN Profile Configuration mode to enable SaMOG to specify a lease period for the UE's IP address during pre-authentication phase and TAL phase.

- **Important**
  - This command requires the SaMOG Web Authorization license. For more information, contact your Cisco account representative.

```
configure
  apn-profile profile_name
    dhc lease { short duration | time duration }
    default dhcp lease { short | time }
    remove dhcp lease short
end
```

Notes:
- Default for `dhc lease short`: 20 seconds
- Default for `dhc lease time`: 4294967295 seconds

Performance Indicator Changes

```
show apn-profile full name profile_name
```

The output of the `show apn-profile full name` command is modified to display the following fields:

- [SaMOG] DHCP SHORT LEASE
- [SaMOG] DHCP LEASE TIME

CSCuw54703 - [SAMOG] Trigger unsolicited RA to deprecate and/or advertise IPv6 prefix

Feature Changes

**SaMOG Unsolicited Router Advertisement Support**

With this release, SaMOG supports sending unsolicited router advertisements (RA) for the EoGRE access type.
IPv6 Prefix Advertisement
SaMOG can send unsolicited RA with a newly allocated IPv6 prefix when a session is established, and the AAA server has authorized the IPv6 or IPv4v6 PDN type for the session without waiting for an RS message from the UE.

The total number of retries and retry interval for RA to advertise an IPv6 prefix can be configured using the `ipv6 unsolicited-router-advt advertise` command under the APN Profile Configuration mode.

IPv6 Prefix Deprecation
SaMOG sends an RA with the preferred and valid lifetime as 0 to deprecate the IPv6 prefix in the following scenarios:

- When the network, SaMOG or the AAA server triggers a disconnect for an IPv6 or IPv4v6 PDN-type session.
- When a session receives an IPv6 packet with an old prefix (prefix that does not match the currently allocated prefix for the session), and the AAA server has authorized an IPv6 or IPv4v6 PDN-type for the session.

The total number of retries and retry interval for RA to deprecate an IPv6 prefix can be configured using the `ipv6 unsolicited-router-advt deprecate` command under the APN Profile Configuration mode.

Virtual MAC Validation
With this release, SaMOG can validate if the destination MAC address in the packet received over the EoGRE tunnel matches with its virtual MAC, broadcast, or multicast address. SaMOG drops those packets whose address does not match. This validation can be enabled using the `violation drop` keywords to the `virtual-mac` command under the APN Profile Configuration mode.

Command Changes

ipv6 unsolicited-router-advt
With this release, the `ipv6 unsolicited-router-advt` command is introduced under the APN Profile configuration mode to enable SaMOG to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.

```plaintext
configure
apn-profile  profile_name
ipv6 unsolicited-router-advt { advertise | deprecate } { interval duration [ num-advts num_advts ] [ num-advts num_advts ] interval duration } [ default | no ] ipv6 unsolicited-router-advt { advertise | deprecate }
end
```

Notes:
- Default for `interval duration` : 3000 ms
- `duration` must be an integer between 100 through 16000.
- Default for `num-advts num_advts` : 3
- `num_advts` must be an integer between 1 through 16.
virtual-mac

With this release, the **violation drop** keywords are introduced to the **virtual-mac** command under the APN Profile Configuration mode to enable SaMOG to drop packets whose destination MAC address does not match SaMOG's Virtual MAC, broadcast, or multicast address.

```
configure
apn-profile profile_name
    virtual-mac { mac_address | violation drop }
    no virtual-mac [ violation drop ]
end
```

**Performance Indicator Changes**

**show samog-service statistics**

The output of the **show samog-service statistics** command is modified to display the following field:

- Dest MAC Violation

**SaMOG Enhancements for 18.2**

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

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

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

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

---

**Important**

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

- **AAA Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
CSCus51250 - [SaMOG] - IPv6 Support for Subscriber Sessions

Feature Changes

IPv6/Dual-Stack Support for Subscriber User Equipment (UE)

With this release, the SaMOG Gateway supports IPv6 and dual-stack (IPv4v6) address allocation for trusted Wi-Fi subscribers on the EPC core. This enables SaMOG Gateway to support a rapidly increasing number of subscribers accessing the internet via mobile devices, and technologically advanced (example, Internet of Things) internet-enabled devices (sensors, machine-readable identifiers) that demand high network address assignment.

SaMOG can support IPv6 or dual-stack (IPv4v6) address allocation for both SIM and non-SIM (non-UICC) based subscriber's user equipment (UE) on the trusted Wi-Fi network. This is achieved using an external P-GW for SIM-based devices, and internal P-GW (Local Breakout - Heavy) for non-SIM-based devices to provide access to the EPC core. In this release, SaMOG supports IPv6/IPv4v6 address allocation over PMIPv6 and EoGRE access types along with GTPv2-based S2a interface.

Command Changes

associate

The dhcpv6-service keyword has been introduced to the associate command under the SaMOG Service Configuration Mode to associate a configured DHCPv6 service to the SaMOG service, in order to process DHCPv6 packets.

configure context context_name
    samog-service samog_service_name
        associate dhcpv6-service dhcpv6_service_name
        no associate dhcpv6-service
    end

Notes:

- The no associate dhcpv6-service command stops the SaMOG service from processing DHCPv6 packets.
- Use the bind address command in the DHCPv6 Service Configuration Mode to configure the DHCPv6 server.
The **ipv6** keyword has been introduced to the `dns` command under the APN Profile Configuration Mode to configure an IPv6 DNS server to enable Flow-based Local Breakout GTPv2 sessions.

```
configure
  apn-profile_profile_name
    dns | ipv6 | { primary | secondary } ip_address
    no dns | ipv6 | { primary | secondary }
end
```

Notes:

- `ip_address` must be expressed in IPv4 dotted-decimal or IPv6 colon-separated (when the **ipv6** keyword is configured) notation format.

### Performance Indicator Changes

**SaM0G Schema**

The following bulk statistics counters are introduced in support of this feature:

- `cgw-sessstat-ipv6-router-solicit-rcvd`  
- `cgw-sessstat-ipv6-router-advt-sent`  
- `cgw-sessstat-ipv6-router-solicit-rx-dropped`  
- `cgw-ipv4v6-pdn-ipv4-uplink-total-pkts`  
- `cgw-ipv4v6-pdn-ipv4-uplink-total-bytes`  
- `cgw-ipv4v6-pdn-ipv6-uplink-total-pkts`  
- `cgw-ipv4v6-pdn-ipv6-uplink-total-bytes`  
- `cgw-ipv4v6-pdn-ipv6-downlink-total-pkts`  
- `cgw-ipv4v6-pdn-ipv6-downlink-total-bytes`

**show samog-service all**

The following fields have been introduced to the output of this command:

- Associated DHCPv6 Service: DHCPv6

**show subscriber samog-only full**

The following fields have been introduced to the output of this command:

- ip address: <IPv4 or IPv6 address>
• Subscribed PDN-Type: IPv4v6/IPv4/IPv6
• CGW Subscriber Info:
  • Accepted PDN-Type: IPv4v6/IPv4/IPv6
  • home-addr: <IPv4 or IPv6 address>

show subscriber full

The following fields have been introduced to the output of this command:
• DNS server address(es)
  • Primary DNS IPv6 Address: <IPv6 address>
  • Secondary DNS IPv6 Address: <IPv6 address>

show samog-service statistics

The following fields have been introduced to the output of this command:
• PDNs BY PDN-Type:
  • IPv6 PDNs:
    • Active
    • Setup
    • Released
    • Rejected

• IPv6 Neighbor Discovery Statistics:
  • IPv6 RS Received
  • IPv6 RS Dropped
  • IPv6 RS Sent

• IPv6 PDNs:
  • Uplink:
    • Total Pkts
    • Total Bytes
  • Downlink:
    • Total Pkts
    • Total Bytes
• IPv4v6 PDNs:
  ◦ Uplink v4:
    * Total Pkts
    * Total Bytes
  ◦ Downlink v4:
    * Total Pkts
    * Total Bytes
  ◦ Uplink v6:
    * Total Pkts
    * Total Bytes
  ◦ Downlink v6:
    * Total Pkts
    * Total Bytes

• PMIPv6 Data Statistics:
  ◦ Tunnel Data Received:
    * Total Packets:
      * IPv4 GRE (IPv6)
      * IPv4 GRE (IPv6)
    * Total Bytes:
      * IPv4 GRE (IPv6)
  ◦ Tunnel Data Sent:
    * Total Packets:
      * IPv4 GRE (IPv6)
      * IPv4 GRE (IPv6)
    * Total Bytes:
      * IPv4 GRE (IPv6)

• EoGRE Data Statistics:
  ◦ Tunnel Data Received:
SaMOG Changes in Release 18

**CSCut22121 - [SaMOG] - Qualification of SaMOG on VPC-DI platform**

**Feature Changes**

**SaMOG vPC-DI Qualification**

With this release, the SaMOG Gateway has been fully qualified to run on Cisco's virtual Packet Core (vPC)-Distributed Instance (DI) platform. In vPC-DI, multiple virtual machines (VMs) act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management. For more information about the vPC-DI platform, refer to the `vPC-DI System Administration Guide`.

**SaMOG Enhancements for 18.0**

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

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

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

**Performance Indicator Changes** - new, modified, and deprecated bulk statistics, disconnect reasons, counters and/or fields in new or modified schema and/or show command output. For details, refer to the `ASR 5x00 Statistics and Counters Reference` for this release.
CSCuo87191 - [SAMOG]: UE and Access Point Identity Support

Feature Changes

User Equipment (UE) Identity Support

With this release, SaMOG can receive the User Equipment's (UE) MAC address as the UE's identity in the Calling-Station-ID AVP in the Radius message (Access-Request). The UE's identity can then be forwarded over the GTPv1 or GTPv2 interface in the IMEI Software Version (SV) IE to GGSN, or Mobile Equipment Identity (MEI) IE to P-GW.

As the UE identity (MAC address) is 12 Bytes long (6 Bytes in the TBCD format), and the total length of the IMEISV is 8 bytes, the additional 2 Bytes can be padded with an user configurable filler value.

Access Point (AP) Location Support

SaMOG can now share the location information of the AP in the User Location Information (ULI) IE during the PDP context setup, and update the locations as Update Context Requests on the GTPv1 interface. When SaMOG detects a change in the AP's location during handovers, an Update PDP Context message is triggered.

With this release, SaMOG supports a new format to facilitate AP location in the Called-Station-ID AVP forwarded in the Radius messages. APs are assigned AP-Names which contain the location details and its identity MAC address. The AP location consists of the Location Area Code (LAC) and the Cell Identity (CI), and they are separated by an underscore in the format (LAC_CI). SaMOG can support both 'LAC_CI-APMAC:SSID' and 'LAC_CI:SSID' formats in the Called-Station-ID AVP.
Command Changes

samog-gtpv1

The `samog-gtpv1` command has been introduced in the Call Control Profile Configuration Mode to enable SaMOG to forward the User Equipment's (UE) Identity and/or the Access Point's (AP) Location information over the GTPv1 interface.

```
configure
  call-control-profile profile_name
    samog-gtpv1 send { imeisv value ue-mac [ filler filler_value ] | uli value cgi }
    no samog-gtpv1 send { imeisv | uli }
  end
```

Notes:
- This configuration is disabled by default.
- Default filler value is 0xFFFF.

samog-s2a-gtpv2

The `samog-gtpv1` command has been introduced in the Call Control Profile Configuration Mode to enable SaMOG to forward the User Equipment's (UE) Identity over the GTPv2 interface.

```
configure
  call-control-profile profile_name
    samog-s2a-gtpv2 send imeisv value ue-mac [ filler filler_value ]
    no samog-s2a-gtpv2 send imeisv
  end
```

Notes:
- This command is enabled when the SaMOG general license is configured.
- This configuration is disabled by default.
- Default filler value is 0xFFFF.

Performance Indicator Changes

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

The output of this command has been modified to display the following IMEIsV and ULI fields:
- Samog-GTPv1:
  - Sending IMEISV IE
  - IMEISV IE Value Type
  - IMEISV IE Filler Value
  - Sending User Location Information (ULI) IE
  - User Location Information (ULI) IE Type
• Samog-S2a-GTv2:
  ◦ Sending IMEISV IE
  ◦ IMEISV IE Value Type
  ◦ IMEISV IE Filler Value

show subscriber samog-only <full>

The output of this command has been modified to display the current state of the CGW service:

• MRME Subscriber Info:
  ◦ State
  ◦ Progress State

CSCup63891 - [SaMOG] - Delay sending Access-Accept till to complete s2a/Gn Procedures

Feature Changes

TWAP Triggered PDN

The Trusted WLAN AAA Proxy (TWAP) sends the Layer 2 attach trigger to the Trusted WLAN Access Gateway (TWAG) after a successful EAP authentication. With this release, SaMOG waits until a tunnel is established for S2a/Gn procedures before forwarding the EAP Success message to the UE.

Previous Behavior: In earlier releases, SaMOG waits on the UE triggered Request PMIPv6 PBU or DHCP-Request to initiate S2a or Gn procedures towards P-GW or GGSN.

New Behavior: From Release 18.0 onwards, SaMOG will hold the Access-Accept for the UE till it finishes S2a/Gn Procedures with P-GW/GGSN.

Customer Impact: Authentication procedure completion for user takes more duration as SaMOG holds the Access-Accept message.

Performance Indicator Changes

show subscriber samog-only <full>

The output of this command has been modified to display the current state of the CGW service:

• MRME Subscriber Info:
  ◦ State
  ◦ Progress State
Feature Changes

SaMOG Wireless Access Gateway (WAG)

With this release, SaMOG extends support for additional deployment models and access side connectivity by integrating various Wireless Access Gateway (WAG) functionalities. This enables SaMOG:

• To be deployed in environments where WLC/RGs do not use bridge mode to forward packets between the User Equipment (UE) and SaMOG gateway.
• To receive IP packets in 'plain L3' or within GRE, MPLS or VLL tunnels.
• To route packets based on the IP address and the Layer 2 tunnel on the access side to the GTP tunnel for the uplink, and vice versa for the downlink.
• To allow IP address allocation by either WLAN or SaMOG.

Layer 3 IP (L3IP)
SaMOG now supports out of band DHCP Layer 3 packet processing, and call setup with the L3IP access-type.

IP address assigned by the WLC (IP@W)

The User Equipment's (UE) IP address is assigned by WLC, and DHCP is not required in the call flow. WLC forwards the assigned IP address in the Accounting-Start message inside the Framed IPAddress field. SaMOG NATs the IP@W with the IP address assigned by P-GW (IP@G).

For Static NAT, configure the access list and the rulebase under the ACS Configuration Mode, and use the following commands under the APN Profile Configuration Mode to associate the ACS configuration:

• `ip access-group access_group_name in`
• `ip access-group access_group_name out`
• `active-charging rulebase acs_rulebase_name`

IP over GRE (IPoGRE)
SaMOG supports GRE encapsulation on the L3IP access-type to ensure a scalable deployment model.

IP over VLAN (IPoVLAN)
SaMOG supports VLAN encapsulation on the L3IP access-type to ensure a scalable deployment model.

License Requirements

With this release,

• The NAT license has been included with the SaMOG 3G license, and SaMOG general license (supporting both 3G and 4G).
• The SaMOG general license (supporting both 3G and 4G) has been enhanced to support configuration of all SaMOG WAG features.
• The IP over GRE feature requires an additional GRE Interface Tunneling license to create IP-GRE tunnels.

Command Changes

associate

The level keyword has been introduced to the associate dhcp-service command under the SaMOG Service Configuration Mode to determine if the DHCP server should run on the proxy mode.

```plaintext
class context context_name
  samog-service samog_name
    associate dhcp-service dhcp_service [ level { system | user } ]
end
```

Notes:

• Default level: user
• user: DHCP server messages are handled at user level. No Demux is required.
• system: DHCP server messages are handled at system level (and user level). Demux is required.

ue-address

The ue-address command has been introduced in the TWAN Profile Configuration Mode to detect whether a DHCP request is expected or if the configuration setup is an IP@WLAN (no DHCP required) model.

```plaintext
class context context_name
  twan-profile profile_name
    ue-address [ dhcp | twan ]
    no ue-address
end
```

Notes:

• If the access-type is PMIP or EoGRE, the UE address configuration is ignored.
• If the configured access-type is IP, and no ue address is configured, the call setup will fail. A configuration error will be displayed in the output of the show configuration errors command.

access-type

The ip keyword has been introduced to the access-type command under the TWAN Profile Configuration Mode to enable configuration of data VRF.

```plaintext
class context context_name
  twan-profile profile_name
    access-type client IPv4/IPv6_address/mask ip
    access-type ip [ vrf vrf_name ]
```
radius

The `ip` keyword has been introduced to the `radius` command under the TWAN Profile Configuration Mode to enable configuration of Virtual Routing and Forwarding (VRF) Context instance for RADIUS communication.

```
configure
  context context_name
  twan-profile profile_name
  | no | radius ip vrf vrf_name
end
```

Performance Indicator Changes

SaMOG Schema

The following bulk statistics is added in support of the WAG integration feature:

- total-l3ip-dhcp-discard-msgs

```
show mrme-service statistics
```

The following fields have been introduced to the output of this command:

- DHCP Messages Discarded
- Max Size Exceeded
- Non-Existing Session
- GiAddr Mismatch
- Unsupported HW Type or Length

```
show samog-service statistics
```

The following fields have been introduced to the output of this command:

- DHCP Messages Discarded
- Max Size Exceeded
- Non-Existing Session
- GiAddr Mismatch
- Unsupported HW Type or Length
show samog-service { all | name <name>}

The following field has been introduced to the output of this command:

- Associated DHCP service: <service_name> (system | user)

show subscriber samog-only full

The following fields have been introduced to the output of this command:

- Rad VRF Ctxt Id
- Data VRF Ctxt Id
- Twan Assigned UE IP: <ip_address> | n/a
- Access Type: samog-ip
- MRME Subscriber Info:
  - Twan Assigned UE IP: <ip_address> | n/a
  - Twan VRF

show subscriber full

The following fields have been introduced to the output of this command:

- Access Type: samog-ip

show twan-profile all

The following fields have been introduced to the output of this command:

- UE-address Type: TWAN
- Radius Vrf Name
- DataPath Vrf Name

CSCup60958 - Local Breakout Basic

Feature Changes

Local Breakout Basic

In earlier releases, the SaMOG Local Breakout (LBO) enhanced model was introduced to enable SaMOG to connect subscribers to the Internet without connecting to the EPC or 3G core. This LBO model was implemented by configuring a local P-GW or a local GGSN, and subscribers belonging to an APN were locally broken out.
With this release, the LBO basic model is introduced enabling SaMOG to connect the subscriber's User Equipment (UE) directly to the Internet without employing a local or external PGW or GGSN service. The UE's IP address is allocated using an IP pool configured locally (or provided by the AAA server). The LBO basic model can be used with or without a Network Address Translation (NAT) service. If dynamic NAT is enabled for a subscriber, SaMOG allocates a global IP address from a pool, and replaces the source IP address of the data packet with this address.

The LBO basic model is best suited when subscribers connect from a network where no web content filtering is required.

License Requirements

In support of the LBO Basic feature, a separate SaMOG LBO Basic license (bundled with a NAT license) has been introduced. This license is mutually exclusive with the SaMOG LBO Enhanced license, and works with both SaMOG 3G and SaMOG General (supporting both 3G and 4G) licenses.

Important

For more information on SaMOG feature licenses, contact your Cisco account representative.

Performance Indicator Changes

SaMOG Schema

The following bulk statistics are added in support of the Local Breakout Basic feature:

- cgw-locally-terminated-uplink-total-pkts
- cgw-locally-terminated-uplink-total-bytes
- cgw-locally-terminated-uplink-drop-pkts
- cgw-locally-terminated-uplink-drop-bytes
- cgw-locally-terminated-downlink-total-pkts
- cgw-locally-terminated-downlink-total-bytes
- cgw-locally-terminated-downlink-drop-pkts
- cgw-locally-terminated-downlink-drop-bytes

show subscriber samog-only full

The output of this command has been modified to display the following LBO Basic-related information:

- Network Type: Local-Offload
- Network Access Mode: Local Offload (Basic)
- Local Offload Details:
  - Rulebase Name: (<rulebase_name> | n/a)
  - IP Pool Name
show apn-profile full { all | name <apn_profile_name> }

The output of this command has been modified to display the following LBO Basic-related counters and information:

• Local Offload: ( Enabled | Disabled )
• Type: PDN
• Local Offloaded Total Data Statistics:
  • Uplink:
    • Total Pkts
    • Total Bytes
    • Dropped Pkts
    • Dropped Bytes
  • Downlink:
    • Total Pkts
    • Total Bytes
    • Dropped Pkts
    • Dropped Bytes

show samog-service statistics

The output of this command has been modified to display the following LBO Basic-related counters:

• Local Offloaded Total Data Statistics:
  • Uplink:
    • Total Pkts
    • Total Bytes
    • Dropped Pkts
    • Dropped Bytes
  • Downlink:
    • Total Pkts
CSCup60968, CSCup60984 - Flow-based Local Breakout

Feature Changes

Flow-based Local Breakout

The Flow-based Local Breakout (LBO) model has been introduced with this release to enable SaMOG to selectively offload certain user data directly to the Internet without employing an external or internal P-GW or GGSN service, and forward the remaining traffic to an external P-GW or GGSN (via the S2a tunnel) depending on configured Layer 4 rules. The User Equipment's (UE) IP address is allocated by the external P-GW or GGSN service. SaMOG applies NAT addressing to all traffic that are offloaded directly to the Internet to differentiate between packets intended for local offload and packets intended to be forwarded to P-GW or GGSN.

SaMOG applies Layer 4 rules to the data traffic using Access Control Lists (ACLs) to determine the part of traffic to be offloaded directly or sent to the P-GW or GGSN service. This decision can be based off an ACL whitelist or an ACL blacklist. While the ACL whitelist identifies the data to be forwarded to the P-GW or GGSN service, the ACL blacklist identifies the data to be locally offloaded.

**Flow-based LBO using a Whitelist:** A flow-based LBO using a whitelist is ideal in situations when a subscriber signs up for some premium content, and this content must be charged differently. SaMOG uses the ACL to route all traffic intended for the premium content server to be forwarded to P-GW or GGSN where special charging is applied using the Gx/Gy interface. SaMOG offloads the rest of the traffic that does not match the ACL directly to the Internet.

**Flow-based LBO using a Blacklist:** A flow-based LBO using blacklist is ideal in situations when SaMOG is deployed in a vicinity where a large number of subscribers access the same content (for example, a streaming video of an event in a stadium where the server is locally hosted). SaMOG offloads this content directly from the local server, and all other data traffic is routed to the P-GW or GGSN service.

License Requirements

In support of the Flow-based LBO feature, a separate SaMOG Flow-based LBO license (bundled with a NAT license) has been introduced. This license is mutually exclusive with the SaMOG LBO Enhanced license, but can be configured with the SaMOG LBO Basic license. The license works with both SaMOG 3G and SaMOG General (supporting both 3G and 4G) licenses.

**Important** For more information on SaMOG feature licenses, contact your Cisco account representative.
Command Changes

local-offload

To enable flow-based LBO, the flow keyword is introduced to the local-offload command in the APN Profile Configuration Mode.

configure
    apn-profile profile_name
        local-offload flow
    end

Performance Indicator Changes

SaMOG Schema

The following bulk statistics are added in support of the Local Breakout feature:

- mrme-local-offload-flow-num-gtpv1
- mrme-local-offload-flow-num-gtpv2
- mrme-local-offload-flow-num-pmip

show subscriber samog-only full

The output of this command has been modified to display the following Flow-based LBO-related information:

- Network Access Mode: (EPC(GTPv1) | EPC(GTPv2))
- Local Offload Flow: (Enabled | Disabled)
- Local Offload Details:
    - Rulebase Name: ( <rulebase_name> | n/a )
    - IP Context Name

show apn-profile full { all | name <apn_profile_name> }

The output of this command has been modified to display the following Flow-based LBO-related information:

- Local Offload: (Enabled | Disabled)
- Type: Flow

show samog-service statistics

In addition to the counters listed for LBO Basic, the output of this command has been modified to display the following Flow-based LBO-related counters:
Local Offload Flow Stats:
- GTPv1
- GTPv2

show cgw-service statistics
The output of this command has been modified to display the following Flow-based LBO-related counters:

- Locally Terminated Total Data Statistics:
  - Uplink:
    - Total Pkts
    - Total Bytes
    - Dropped Pkts
    - Dropped Bytes
  - Downlink:
    - Total Pkts
    - Total Bytes
    - Dropped Pkts
    - Dropped Bytes

CSCup60995, CSCup64175 - S2a PMIPv6 Support

Feature Changes

SaMOG S2a Interface using PMIPv6
In earlier releases, SaMOG could connect to the P-GW service over the S2a interface based on the GTPv2 protocol, and the GGSN service over the Gn interface based on the GTPv1 protocol.

With this release, SaMOG can connect to the P-GW service over the S2a interface based on the PMIPv6 protocol as specified by 3GPP TS 29.275, Release 11 standards. SaMOG performs a SNAPTR-based DNS query towards the DNS server to get the P-GW IP address, and initiates a PMIPv6-based registration procedure by sending a Proxy Binding Update message to the P-GW. The IP address of the User Equipment (UE) allocated by P-GW is then received in the Proxy Binding Acknowledge message.
The SaMOG Local Breakout Enhanced model, and the Web Authorization feature are currently not supported on a PMIPv6 based S2a interface.

**License Requirements**

The SaMOG general license (supporting both 3G and 4G) has been enhanced to support configuration of PMIPv6-based S2a interface. As SaMOG with a PMIPv6-based S2a interface cannot be used with a GGSN service, the SaMOG 3G license is not supported.

For more information on the SaMOG General license, contact your Cisco account representative.

**Command Changes**

**MAG Service Configuration Mode**

The following existing commands under the MAG Service Configuration Mode can be used to create and manage a Mobility Access Gateway service and communicate with the Local Mobility Anchor (LMA) on a P-GW:

- bind
- encapsulation
- heartbeat
- information-element-set
- max-retransmissions
- mobility-option-type-value
- reg-lifetime
- renew-percent-time
- retransmission-policy
- retransmission-timeout

In the current release:

- SaMOG supports an IPv4 bind address only.
- SaMOG supports GRE encapsulation only.
- The information element set for SaMOG must be set to **standard**.
associate

The **mag-service** keyword has been introduced in the CGW Service Configuration Mode to associate a MAG service to the CGW service.

```plaintext
configure
c   context context_name
c   cgw-service cgw_service_name
   associate mag-service mag_service [ context context_name ]
   no associate mag-service variable
end

mobility-protocol

The **pmip** keyword has been introduced to configure the mobility protocol type in the APN Profile Configuration Mode.

```plaintext
configure
c   apn-profile profile_name
   mobility-protocol pmip
end
```

mobility-protocol

The **pmip** keyword has been introduced to configure the mobility protocol type in the Call Control Profile Configuration Mode.

```plaintext
configure
c   call-control-profile profile_name
   mobility-protocol pmip
end
```

**Performance Indicator Changes**

**SaMOG Schema**

The following bulk statistics are added in support of the S2a PMIPv6 support feature::

- cgw-sessstat-pdns-pmip-active
- cgw-sessstat-pdns-pmip-setup
- cgw-sessstat-pdns-pmip-released
- cgw-sessstat-pdns-pmip-rejected
- cgw-s2a-gtpu-uplink-total-pkts
- cgw-s2a-gtpu-uplink-total-bytes
- cgw-s2a-gtpu-uplink-drop-pkts
- cgw-s2a-gtpu-uplink-drop-bytes
- cgw-s2a-gtpu-downlink-total-pkts
• cgw-s2a-gtpu-downlink-total-bytes
• cgw-s2a-gtpu-downlink-drop-pkts
• cgw-s2a-gtpu-downlink-drop-bytes
• cgw-s2a-pmip-uplink-total-pkts
• cgw-s2a-pmip-uplink-total-bytes
• cgw-s2a-pmip-uplink-drop-pkts
• cgw-s2a-pmip-uplink-drop-bytes
• cgw-s2a-pmip-downlink-total-pkts
• cgw-s2a-pmip-downlink-total-bytes
• cgw-s2a-pmip-downlink-drop-pkts
• cgw-s2a-pmip-downlink-drop-bytes
• mrme-access-mode-pmip-selected

The following bulk statistics have been deprecated:
• cgw-s2au-uplink-total-pkts
• cgw-s2au-uplink-total-bytes
• cgw-s2au-uplink-drop-pkts
• cgw-s2au-uplink-drop-bytes
• cgw-s2au-downlink-drop-bytes
• cgw-s2au-downlink-total-pkts
• cgw-s2au-downlink-total-bytes
• cgw-s2au-downlink-drop-pkts

**show subscriber samog-only full**

The output of this command has been modified to display the following PMIPv6-based S2a-related fields:
• Network Type: PMIPv6 (IPv4)
• Configured Mobility Protocol: PMIP
• Network Access Mode: PMIP
• CGW Subscriber Info:
  • Home-addr
  • mag-addr
  • lma-addr
  • lifetime
  • remaining life
The output of this command has been modified to display the following PMIPv6-based S2a-related field:

- Network Type: PMIPv6

The output of this command has been modified to display the following PMIPv6-based S2a-related fields:

- PMIP
- PMIP PDNs:
  - Active
  - Setup
  - Released
  - Rejected
- S2A-GTP Total Data Statistics:
  - Uplink:
    - Total Pkts
    - Total Bytes
    - Dropped Pkts
    - Dropped Bytes
  - Downlink:
    - Total Pkts
    - Total Bytes
    - Dropped Pkts
    - Dropped Bytes
- Gn Total Data Statistics:
  - Uplink:
    - Total Pkts
    - Total Bytes
    - Dropped Pkts
• Dropped Bytes

• Downlink:
  • Total Pkts
  • Total Bytes
  • Dropped Pkts
  • Dropped Bytes

show cgw-service all
The output of this command has been modified to display the following PMIPv6-based S2a-related fields:
  • MAG Service
  • MAG Service context

show call-control-profile full { all | name <profile_name> }
The output of this command has been modified to display the following PMIPv6-based S2a-related field:
  • MRME Mobility Protocol: PMIP

show apn-profile full { all | name <profile_name> }
The output of this command has been modified to display the following PMIPv6-based S2a-related field:
  • MRME Mobility Protocol: PMIP

CSCup61006, CSCur35158 - EAP authentication method agnostic SAMOG service

Feature Changes

EAP Agnostic Authentication
In earlier releases, SaMOG supported EAP-SIM, EAP-AKA, and EAP-AKA' authentication, and non-EAP (MAC-based) authentication for web authorization. SaMOG could not connect non-UICC devices to the EPC core using SIM-based authentication.

With this release, SaMOG supports EAP-based authentication where the inner layer of EAP protocols is agnostic. This enables SaMOG to support authentication mechanisms such as EAP-TLS and EAP-TTLS/MSCHAPv2, to connect non-UICC devices to the EPC core.

EAP-TLS: This authentication mechanism enables SaMOG to provide a certificate-based mutual authentication mechanism between the UE and the EAP Server for non-UICC devices.
EAP-TTLS/MSCHAPv2: SaMOG performs this authentication mechanism in two phases. During the first phase, SaMOG authenticates the server using a certificate that is used to create a secure tunnel. In the second phase, the subscriber is authenticated using MSCHAPv2 authentication mechanism within the secure tunnel.

Here, SaMOG considers the EAP-response/identity messages between the WLC and the AAA server as an uncategorized EAP authentication mechanism. SaMOG allows messages to be exchanged until received a success/failure message from the AAA server, or the session setup timer expires.

As with SIM-based authentications, in compliance to 3GPP 23.003 standard, SaMOG expects the NAI forwarded by the UE to be in the same format for P-GW selection, with the flexibility to support non-IMSI-based user-name in the AVP. If the prefix for the user-name is uncategorized (not between 0 and 9), SaMOG considers the username portion of the NAI as non-IMSI based.

**Command Changes**

```plaintext
aaa

In order for SaMOG to support EAP-TLS and EAP-TTLS/MSCHAPv2-based authentication, the `aaa` command has been introduced in the MRME Service Configuration Mode. This command allows you to control the range of EAP-payload size, or restrict the Framed-MTU AVP from being forwarded in the Auth-Request to the AAA server.

```configure
context context_name
  mrme-service mrme_service_name
    aaa send framed-mtu eap_payload_size
    no aaa send framed-mtu
end
```

Notes:

- Use the `no` keyword to disable SaMOG from forwarding Framed-MTU AVP in the Auth-Request message to the AAA server.

**Performance Indicator Changes**

**SaMOG Schema**

The following bulk statistics has been added in support of the EAP agnostic authentication feature:

- mrme-eap-rxmobile-eap-other

The following bulk statistics has been deprecated:

- mrme-eap-rxmobile-eap-unsupported

**show mrme-service all**

The following field has been introduced to the output of the `show mrme-service all` command to display the configured framed MTU size:

- AAA Send Framed-MTU Size
show samog-service statistics

The following field has been introduced to the output of the show samog-service statistics command to display the total number of EAP TLS, TTLS/MSCHAPv2 messages received:

- EAP Other

show subscribers samog-only full

The following field has been introduced to the output of the show subscribers samog-only full command to display the configured framed MTU size:

- Framed-MTU
SGSN Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from the SGSN in StarOS 18 software releases.

- SGSN Enhancements for 18.5, page 323
- SGSN Enhancements for 18.3, page 327
- SGSN Enhancements for 18.1, page 328

SGSN Enhancements for 18.5

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

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

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

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

Important

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

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

CSCur57085 - Inter-SRNS SGSN to send ULI to GGSN

This is a behavior change with modified CLI.

Feature Changes

ULI Containing Valid SAI 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.

CSCux33388, CSCur41900 - CLI Control for Target Access Restriction

CSCux33388 - InterSGSN 3G to 2G HO fails
CSCur41900 - Rollback Behavior in EPC during TAU/RAU Needs to be Corrected

Feature Changes

Target Access Restriction

Target Access Restriction feature was added to the SGSN and MME in release 17.4. The purpose of this feature is to avoid rollback behavior that exists in RAU and TAU s by checking target RAT Type IE present in the Context Request at the source node, and then rejecting the TAU/RAU based on the subscriber's ARD profile earlier in the cycle if the target RAT is restricted for the subscriber. Rollback behavior caused late TAU/RAU rejection, resulting in PDP/bearer deletion for the MME, PGW, and the SGSN, requiring the UE to reattach and reactivate lost PDP/bearer.

Previous Behavior: As a part of this functionality, the target access restriction feature instructs the source-SGSN or the source-MME to reject outbound RAU when the target access was restricted for the subscriber. Rejection was performed without checking "access-restriction-data no-check" in the call control profile configuration.

New Behavior: With release 17.6.1, a new command keyword target-access-restriction has been introduced to the call control profile configuration to control (enable/disable) target access restriction functionality. Target
access restriction is now disabled by default on both the SGSN and the MME. Refer to the Command Changes section below for the command information to enable/disable this functionality.

The default behaviors for the SGSN and the MME now differ:

• **New Behavior for the MME only:** "target-access-restriction" keyword configuration will control the target access restriction feature for the MME without other consideration:
  
  ◦ **No Rejection:** if "target-access-restriction" is *not enabled*, then the source-MME will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
  
  ◦ **Rejection:** if "target-access-restriction" is *enabled*, then the source-MME will *reject* the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

• **New Behavior for the SGSN only:** The SGSN also considers "access-restriction-data no-check" in the call control profile configuration prior to rejecting outbound RAU when target access restriction functionality is enabled. The SGSN's target access restriction behavior is dependent upon the SGSN's "access-restriction-data no-check" configuration:
  
  ◦ **No Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN will *not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
  
  ◦ **Rejection:** if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will ignore the "target-access-restriction enabled" configuration and the source-SGSN will *reject* the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

---

**Command Changes for the MME**

**access-restriction-data**

With release 17.6.1, the MME has access to this command in the call-control-profile configuration mode. The new keyword **target-access-restriction** enables or disables rejection of the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

```plaintext
configure
call-control-profile ccprof_name
  access-restriction-data target-access-restriction
  remove access-restriction-data [ target-access-restriction ]
end
```

Notes:

• Including the **target-access-restriction** keyword with the command enables the target access restriction feature.
• Including the `remove` command filter disables the target access restriction feature. Inclusion of the `target-access-restriction` keyword in the `remove` command is currently optional.

## Command Changes for the SGSN

### access-restriction-data

With release 17.6.1, the new keyword `target-access-restriction` enables or disables the Target Access Restriction feature.

```plaintext
configure
call-control-profile  ccprof_name
    access-restriction-data [eutran-not-allowed | failure-code | no-check | target-access-restriction]
]
    access-restriction-data no-check
    remove access-restriction-data [target-access-restriction]
end
```

**Notes:**

• Including the `target-access-restriction` keyword with the command enables the target access restriction feature.

• With the target access restriction feature enabled, including the `no-check` keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

• Including the `remove` command filter with the `target-access-restriction` keyword disables the target access restriction feature.

• With the target access restriction feature enabled, including the `remove` command filter with the `no-check` keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

## Performance Indicator Changes

### show call-control-profile

The Target Access Restriction field will display in the output with Enabled or Disabled and it will appear similar to the following:

```plaintext
[local]test# show call-control-profile full name ccprof1
...
Authentication Detach           : Not configured
Regional Subscription Restriction Failure Code Value : 13
ARD-Checking                            : Enabled
ARD Failure Code                      : Disabled
Access Restriction Data               : EUTRAN Allowed
Target Access Restriction             : Enabled
Zone-Code Check                       : Enabled
...
...
```
show configuration verbose

The access-restriction-data target-access-restriction field displays in the output without the "remove" prefix to indicate it is Enabled or with the "remove" prefix to indicate the feature is Disabled. The output will appear similar to the following when the feature is enabled:

[local]test# show configuration verbose
...  
call-control-profile ccprou
  remove rau-inter ctxt-xfer-failure
  no subscriber-control-inactivity
  ...
  access-restriction-data target-access-restriction
  ...
  ...

SGSN Enhancements for 18.3

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

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

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

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

---

**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 *product*.

- AAA Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements
CSCuu74352 - No rab release during upc/dpc collision

Feature Changes

Send Activate PDP Reject Instead of De-activate PDP Request

Scenario:

1. 3G Attach procedure begins.
2. The SGSN receives a PDP Context Activation Request from the UE.
3. The SGSN processes the activation until the RAB establishment procedure; as it is a direct tunnel-capable call, the SGSN initiates a UPC Request to the GGSN and waits for the UPC Response.
4. The GGSN initiates Delete PDP Context Request on the same context (Note: DPCR can occur for any reason, such as the GGSN clearing the PDP session).

Previous Behavior: The GGSN initiates a deletion before activation is completed at the SGSN. The SGSN sends a Deactivate PDP Request. Due to DPC/UPC collision, the SGSN does not release the old RAB at the RNC.

New Behavior: The SGSN now sends an Activate PDP Reject when the GGSN initiates a Delete PDP Context Request before activation is completed at the SGSN and then the SGSN releases the RAB at the RNC.

Customer Impact: DPC/UPC collision and presence of older RAB at the RNC do not affect further activations from the UE.

SGSN Enhancements for 18.1

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 ASR 5x00 Command Line Interface Reference for this release.

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

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

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

CSCtq92045 - Need Linkmgr CPU added to bulkstats for SGSN cpcty monitoring

Feature Changes

Additional Card-level Bulk Statistics Added

Previous Behavior: Some card-level bulk statistics were not supported.

New Behavior: Support for collection and display of card-level bulk statistics for LinkMgr, MMgr, GbMgr, and IMSIMgr have been added for the following:

• number of task instances
• average memory utilization
• average CPU utilization
• maximum CPU utilization
• maximum memory utilization

Performance Indicator Changes

Card Schema

The following statistical variables have been added to collect and display information for LinkMgr, MMgr, GbMgr, and IMSIMgr at the card level:

• task-linkmgr-num
• task-linkmgr-avgcpu
• task-linkmgr-avgmem
• task-linkmgr-maxcpu
• task-linkmgr-maxmem
• task-gbmgr-num
• task-gbmgr-avgcpu
• task-gbmgr-avgmem
Feature Changes

Operator Control for GPRS/EPS Subscription Data Requests in UGL/ULR Messages to the HLR/HSS.

Previous Behavior: The operator has no provision to control GPRS/EPS Subscription data requests in UGL/ULR messages to the HLR/HSS.

New Behavior: New CLI options are introduced which allow operator control over GPRS/EPS Subscription data requests in UGL/ULR messages to the HLR/HSS.

A new keyword `gprs-subscription-not-needed` is added in the `map` command. Configuration of this keyword determines whether the SGSN (or MME/IWF) requests GPRS Subscription Data in addition to EPS Subscription Data from the HLR. If this keyword is configured, the parameter `gprsSubscriptionDataNotNeeded` is set in the UGL message. The SGSN (or MME/IWF) will not request GPRS Subscription Data in addition to EPS Subscription Data from the HLR. By default, GPRS Subscription Data is always requested from the HLR.

A new keyword `eps-subscription-not-needed` is added in the `map` command. Configuration of this keyword determines whether the SGSN requests EPS Subscription Data in addition to GPRS Subscription Data from the HLR. If this keyword is configured, the parameter `epsSubscriptionDataNotNeeded` is set in the UGL message. The SGSN will not request EPS Subscription Data in addition to GPRS Subscription Data from the HLR. By default, EPS Subscription Data is always requested from the HLR.

A new command `hss message update-location-request gprs-subscription-indicator [ never | non-epc-ue ]` is introduced under the Call Control Profile configuration mode. This command provides operator control over GPRS subscription data requests in ULR messages to the HSS. If this command is configured, the parameter GPRS-Subscription-Data-Indicator is set in the ULR message. The HSS includes the GPRS subscription data in the ULA command. If the GPRS subscription data is available in the HSS and
GPRS-Subscription-Data-Indicator bit is set in the ULR message, the HSS includes the GPRS Subscription data in the ULA command. By default, GPRS Subscription Data is always requested from the HSS.

**Command Changes**

**map**

New keywords `eps-subscription-not-needed` and `gprs-subscription-not-needed` are added to the `map` command to provide operator control over GPRS/EPSSubscription Data requests in UGL messages to the HLR.

```
configure
  call-control-profile profile_name
    [ remove ] map message { mo-fwd-sm imsi | update-gprs-location { eps-subscription-not-needed | always | non-epc-ue | gprs-subscription-not-needed | always | epc-ue | imeisv | private-extension access-type } }
    remove map message update-gprs-location gprs-subscription-not-needed
    remove map message update-gprs-location eps-subscription-not-needed
end
```

**Notes:**

- By default, EPS and GPRS Subscription Data is always requested in UGL messages from the HLR.
- The keyword `always` is used to specify that EPS/GPRS Subscription Data should never be requested from the HLR.
- The keyword `non-epc-ue` is used to specify that EPS Subscription Data should never be requested from the HLR when the UE is not a EPC capable device.
- The keyword `epc-ue` is used to specify that GRPS Subscription Data should never be requested from the HLR when the UE is a EPC capable device.

For detailed information on the new keywords introduced in this command, see *Command Line Interface Reference, StarOS Release 18 guide*.

**hss**

This new command is introduced under the Call Control Profile configuration mode to provide operator control over GPRS Subscription Data requests in ULR messages to the HSS.

```
configure
  call-control-profile profile_name
    hss message update-location-request gprs-subscription-indicator { never | non-epc-ue }
    remove hss message update-location-request gprs-subscription-indicator
end
```

**Notes:**

- By default, GPRS Subscription Data is always requested from the HSS.
- The `never` keyword is used to specify that GPRS Subscription Data should never be requested from the HSS.
- The `non-epc-ue` keyword is used to specify that GPRS Subscription Data should be requested from the HSS when the UE is not a EPC capable device.
For detailed information on this new command, see Command Line Interface Reference, StarOS Release 18 guide.

**CSCty22738 - lmgr stats classification for connection-less ranap msg**

### Feature Changes

**Link Manager Parser Statistics Updated with New Statistics**

**Previous Behavior:** The Link Manager Parser statistics display the statistics only for Reset or Overload connection-less RANAP messages and all other messages are marked as "Unsupported connection-less messages".

**New Behavior:** New statistics are added to the show output "show linkmgr all parser statistics all", Reset Resource and Error Indication statistics are added to the Link Manager Parser Statistics. Addition of these statistics helps in better classification of messages.

### Performance Indicator Changes

`show linkmgr all parser statistics all`

The following new statistics have been added to the `show linkmgr all parser statistics all` output to display Reset Resource and Error Indication Statistics:

- Reset Resource
- Error Indication (Connectionless)

**CSCui82344, CSCum50067, CSCur94662, CSCur94708, CSCur40028, CSCur33100 - SGSN to select the co-located MME in case of PS-HO from SGSN to MME**

### Feature Changes

**SGSN & MME Combo Optimization**

The SGSN and MME can be enabled simultaneously in the same chassis and, though co-located, they each behave as independent nodes. This Combo Optimization feature enables the co-located SGSN and MME to co-operate with each other in order to achieve lower memory utilization and CPU utilization and to reduce signaling towards other nodes in the network. When functioning as mutually-aware co-located nodes, the SGSN and MME can share UE subscription data between each other.
This feature is supported by both the S4-SGSN and the Gn-SGSN. For the feature to apply to a Gn-SGSN, the Gn-SGSN must be configured to connect to an HSS.

The combo optimization feature in SGSN-MME node is a licensed Cisco feature. A separate feature license is required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter in the System Administration Guide.

For a detailed feature description, see SGSN Administration Guide, StarOS Release 18.

Command Changes

sgsn-mme

A new command `sgsn-mme subscriber-data-optimization` is introduced under the LTE Policy Configuration mode to enable configuration of this feature.

```
config
  lte-policy
    | no | sgsn-mme subscriber-data-optimization
  exit
```

Notes:

- By default the SGSN & MME Combo Optimization feature is disabled. Enter the command to enable the feature.
- `no` included as a prefix of the command disables the feature when it has been enabled with this command.

hss

A new command `hss message update-location-request` is introduced under the Call Control Profile Configuration mode to control requests of GPRS subscription information from the HSS.

```
config
  call-control-profile<profile_name>
    hss message update-location-request gprs-subscription-indicator | never | non-epc-ue |
  exit
```

- `never` instructs the SGSN or MME never to request a location update from the HSS.
- `non-epc-ue` instructs the SGSN or MME to request location updates from the HSS for non-EPC (4G capable) UEs.
- `remove` included as a prefix of the command deletes the "hss message" definition from the Call-Control Profile configuration.
- Configuration can be seen with the new field HSS ULR Message. GPRS Subscription Data Indicator using the `show call-control-profile full { all | name }` command
Performance Indicator Changes

show lte-policy sgsn-mme summary
The following parameter indicates if optimization on SGSN-MME combo node is "Enabled" or "Disabled":
- subscriber-data-optimization

show demux-mgr statistics imsimgr all sgsn
The following new fields are added in the show output to display the number of RAU, Attach, PTIMSI attach and Forward relocation requests arriving from a subscriber attached with co-located MME:
- IMSI attach with context in co-located MME
- P-TMSI attach with mapped P-TMSI of co-located MME
- RAU with mapped P-TMSI of co-located MME
- Fwd reloc request from co-located MME

show subscribers sgsn-only summary
The following new field is added in the show output to display the number of subscribers currently sharing subscription information with MME:
- Total HSS subscribers sharing subscription-info

show subscribers gprs-only summary
The following new field is added in the show output to display the number of subscribers currently sharing subscription information with MME:
- Total HSS subscribers sharing subscription-info

show subscribers sgsn-only full all
The STN-SR, ICS-indicator, Trace-Data and CSG subscription information is now displayed under the show subscribers sgsn-only full all output. These AVPs are currently used by MME only. Values are displayed as received from HSS without any format changes.
- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
show subscribers gprs-only full all

The STN-SR, ICS-indicator, Trace-Data and CSG subscription information is now displayed under the `show subscribers gprs-only full all` output. These AVPs are currently used by MME only. Values are displayed as received from HSS without any format changes.

- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
- OMC Id
- Trace Collection Entity
- STN-SR
- ICS-Indicator
- CSG Subscription
- CSG ID
- Expiration Date

show session subsystem facility aaamgr instance <instance>

The following new fields are added in the show output to display the total number of CSG subscription records and Trace data records:

- SGSN: Total Trace data records
- SGSN: Total CSG data records

show hss-peer-service statistics all

The following new fields are added to the show output to display the subscription data statistics:
The Skip Subscription Data statistic is incremented when the ULR is sent with the skip-subscription-data flag set. The Subscription-Data Not Received statistic is incremented if the HSS does not send the subscription data in the ULA when skip-subscription-data flag is set in ULR. The difference between the Skip Subscription Data and Subscription-Data Not Received gives us the number of times HSS does not honour the skip-subscription-data flag.

**show mme-service statistics handover**

The following new statistics are added to the show output to display the information about Inter-RAT Optimized Handoffs between the co-located SGSN and MME:

- Inter-RAT Optimized Handoffs Between Co-located MME and SGSN
- Outbound MME to SGSN RAU procedure
  - Attempted
  - Success
  - Failures
- Inbound SGSN to MME TAU procedure
  - Attempted
  - Success
  - Failures
- Outbound MME to SGSN Connected Mode Handover
  - Attempted
  - Success
  - Failures
- Inbound SGSN to MME Connected Mode Handover
  - Attempted
  - Success
  - Failures
CSCum50020, CSCur73892, CSCur30903 - Scale IMSIMGR

Feature Changes

SGSN Support for IMSI Manager Scaling

The number of IMSI Managers supported is scaled up on ASR 5500 and a VPC-DI platforms. The IMSI Manager is a de-multiplex process that selects the Session Manager instance based on the de-multiplex algorithm logic to host a new session. The IMSI Manager process also maintains the mapping of IMSI/F-PTMSI (UE identifier) to the Session Manager instance. Currently only a single instance of the IMSI Manager task is present on the SGSN or SGSN and MME combo nodes. This feature is developed to increase the number of IMSI Manager Instances. The maximum number of IMSI Managers supported on ASR5000 and SSI remains at "1". This feature is only supported on ASR5500 and VPC-DI platforms.

The IMSI Manager task is a bottleneck during single event performance testing, the Attach/RAU rates are restricted to a lower value than desired on the ASR5000 /ASR5500 platforms. The IMSI Manager receives new session requests from the Link Manager (3G) and Gb Manager (2G) processes in the SGSN. It also receives messages from the MME Manager (12 instances) processes in the MME. The IMSI Manager task communicates with a maximum of "288" Session Manager instances in a fully loaded chassis on ASR5000. On DPC2 the numbers of Session Manager Instances are much more than on ASR5000, therefore one instance of IMSI Manager will not be sufficient to support the number of Session Manager Instances on ASR5500 and VPC-DI platforms. Scaling up the number of IMSI Manager Instances improves the single event performance numbers of SGSN and MME. It also helps in utilizing the full capability of the ASR 5500 and VPC-DI platforms.

Command Changes

task facility imsimgr

The following configuration command is used to configure the number of IMSIMGR tasks that are required in the system:

```
configure
  task facility imsimgr { avoid-sessmgr-broadcast | max <integer_value> | required-sessmgr no_sess_mgrs
  sessmgr-sessions-threshold high-watermark <high_value> low-watermark <low_value> }
end
```

Notes:

- The keyword max denotes the number of IMSI managers spawned in the system. This keyword is supported only on ASR5500 and VPC-DI platforms. A maximum of "4" IMSI Manager can be configured.
- The default number of IMSI Managers supported is "4" on ASR5500 and VPC-DI platforms only.
- This is a boot-time configuration and should be added in the configuration file before any SGSN/MME related configuration is created or any IMSI Manager is started. Run-time configuration of this CLI is not valid. Any such attempt will result in the following error message being displayed:
  New config requires system restart to be effective. Please save config and restart
- This configuration should be added in the configuration file and the system should be re-loaded to apply this new configuration.
**sgsn imsimg**

The `sgsn imsimg` command in the Exec mode initiates audit for managing the SGSN's IMSI manager's (IMSIMgr) IMSI table. The command is updated with a new keyword `instance` to extend support for multiple IMSI Managers. The audit is initiated from only one specified instance of IMSI Manager at a time.

```
sgsn imsimg { instance instance_id }{ add-record imsi sessmgr instance sessmgr# | audit-with sessmgr { all | instance sessmgr# } } remove-record imsi
```

**Performance Indicator Changes**

**show linkmgr all**

The following new parameters are added to this show command to display the statistics for this feature:

- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

**show linkmgr instance parser statistics all**

The following new parameters are added to this show command to display the statistics for this feature:

- Messenger Counters
- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

**show gbmgr instance parser statistics all**

The following new parameters are added to this show command to display the statistics for this feature:

- Messenger Counters
- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4
show demuxmgr statistics imsimgr verbose

The following new parameter is added to this show command to display the statistics for this feature:

- IMSIMGR instance number

show demux-mgr statistics sgtpcmgr instance < id >

The following new parameters are added to this show command to display the statistics for this feature:

- Interactions with IMSI Manager
- Num requests sent to IMSIMgr
- Num requests not sent to IMSIMgr
- Num requests bounced from IMSIMgr
- Num responses received from IMSIMgr
- Num responses with unknown IMSI
- Num Forwarded Relocation Request forwarded
- Num Relocation Cancel Requests With IMSI forwarded
- Num Forward Relocation Requests rejected by IMSIMGR
- Num Relocation Cancel Requests rejected by IMSIMGR

show session subsystem facility mmemgr instance < id >

New counters are added in the MME manager to count the number of requests sent towards the IMSI managers:

- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

show subscribers mme-only full all/ show mme-service session full all

The IMSI Manager instance holding the mapping entry for a subscriber session is displayed as part of the subscriber session information:

- Imsimgr Instance

show mme-service db record call-id <id>

The following new parameters are added to this show command to display the statistics for this feature:

- Sessmgr Instance
CSCup86883, CSCuq24364, CSCuq55842 - VPC-DI Serving GPRS Support Node

Feature Changes

VPC-DI platform Support for SGSN

The traditional proprietary hardware platforms like ASR5K and ASR5500 provide carrier class hardware redundancy and have limited scalability. The VPC-SI model separates the StarOS from the proprietary hardware. It consists of the StarOS software running within a single VM. This provides the end user with low entry cost (software licenses and commodity hardware), simplified setup, and well-defined interfaces. The VPC-SI is ideally suited for small carriers, remote locations, lab testing, trials, demos, and other models where full functionality is needed. The Cisco VPC-Distributed Instance (VPC-DI) platform allows multiple VMs to act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management. The VPC-DI offers enhanced hardware capabilities, the SGSN is enhanced to support the VPC-DI platform.

Note

For more information on the VPC-DI platform, see VPC-DI System Administration Guide.

CSCuq06573 - Removal of TPO Code

Feature Changes

Support for TPO Feature Withdrawn

Previous Behavior: The statistics related to TPO feature are displayed on execution of `show sgtpc statistics`, `show sgtpc statistics sgtp-service <service_name>` and `show sgtpu statistics sgtp-service <service_name>` commands. The TPO feature is no longer supported and related statistics have to be removed.

New Behavior: The statistics related to the TPO feature are removed from the show commands `show sgtpc statistics`, `show sgtpc statistics sgtp-service <service_name>` and `show sgtpu statistics sgtp-service <service_name>`.
Performance Indicator Changes

show sgtpc statistics

The following statistics are deprecated as the TPO feature is no longer supported by SGSN:

- Data Path Discontinuity Indication
- Total Registration Ind
- Total Deregistration Ind

show sgtpc statistics sgtp-service <service_name>

The following statistics are deprecated as the TPO feature is no longer supported by SGSN:

- Data Path Discontinuity Indication
- Total Registration Ind
- Total Deregistration Ind

show sgtpu statistics sgtp-service <service_name>

The following statistics are deprecated as the TPO feature is no longer supported by SGSN:

- CISCO Non Standard Sent
- Data-Path-Discon-Ind

CSCur33100 - [18.0] SGSN/MME Combo - F PTMSI Attach support is required

Feature Changes

Support to Copy Subscription Information From MME during FPTMSI Attach Procedure

**Previous Behavior:** Support to copy subscription information from MME during FPTMSI attach procedure was absent.

**New Behavior:** Support is added to copy subscription information from co-located MME during FPTMSI attach procedure. Subscription information is copied from co-located MME if a subscriber does a FPTMSI attach with SGSN and the previous node was MME. The Skip-subscriber-data bit in ULR flags is set if subscription data is copied from the MME.

**Customer Impact:** Subscription information can be copied from co-located MME during FPTMSI attach request, this avoids requesting subscription-data in ULR.
Feature Changes

Support to Share Subscription Information during Attach and SRNS scenarios in co-located SGSN/MME.

**Previous Behavior:** Subscription information was not shared in a co-located SGSN/MME scenario. The SGSN and MME fetched subscription information separately when a subscriber moved from MME to SGSN during Attach and SRNS scenarios.

**New Behavior:** Support is added to share subscription information between SGSN and MME during Attach and SRNS scenarios in co-located SGSN/MME. The Skip-subscriber-data bit in ULR flags is set if the subscription information is copied from a co-located MME.

**Customer Impact:** Subscription information can be copied from co-located MME during Attach and SRNS scenarios.

Performance Indicator Changes

**show demux-mgr statistics imsimgr all sgsn**

The following new fields are added in the show output to display the number of RAU, Attach, PTIMSI attach and Forward relocation requests arriving from a subscriber attached with co-located MME:

- IMSI attach with context in co-located MME
- P-TMSI attach with mapped P-TMSI of co-located MME
- RAU with mapped P-TMSI of co-located MME
- Fwd reloc request from co-located MME

**show subscribers sgsn-only summary**

The following new field is added in the show output to display the number of subscribers currently sharing subscription information with MME:

- Total HSS subscribers sharing subscription-info

**show subscribers gprs-only summary**

The following new field is added in the show output to display the number of subscribers currently sharing subscription information with MME:

- Total HSS subscribers sharing subscription-info
show subscribers sgsn-only full all

The STN-SR, ICS-indicator, Trace-Data and CSG subscription information is now displayed under the show subscribers sgsn-only full all output. These AVPs are currently used by MME only. Values are displayed as received from HSS without any format changes.

- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
- OMC Id
- Trace Collection Entity
- STN-SR
- ICS-Indicator
- CSG Subscription
- CSG ID
- Expiration Date

show subscribers gprs-only full all

The STN-SR, ICS-indicator, Trace-Data and CSG subscription information is now displayed under the show subscribers gprs-only full all output. These AVPs are currently used by MME only. Values are displayed as received from HSS without any format changes.

- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
- OMC Id
- Trace Collection Entity
- STN-SR
- ICS-Indicator
- CSG Subscription
- CSG ID
Expiration Date

show session subsystem facility aaamgr instance <instance>

The following new fields are added in the show output to display the total number of CSG subscription records and Trace data records:

- SGSN: Total Trace data records
- SGSN: Total CSG data records

CSCus30042 - [18.0] "show conf" need not to display default configs

Feature Changes

Network Interface Selection Related Show Outputs Corrected

Previous Behavior: Consider the following scenarios:

Scenario 1:
The configuration contains a SGSN license and a Call-Control-Profile is created. The CLI "sgsn-core-nw-interface" under the Call Control Profile Configuration mode enables the operator to select either Gn or S4 interface for EPC capable UEs and Non-EPC capable UEs on the S4-SGSN. This CLI is specific to S4-SGSN and not available for Gn SGSN. When the command "show call-control-profile full name < profile_name >" is executed, the output incorrectly displays the section "SGSN Core Network Interface Selection".

Scenario 2:
The configuration contains a S4 SGSN license and a Call-Control-Profile is created. The CLI "sgsn-core-nw-interface" under the Call Control Profile Configuration mode enables the operator to select either Gn or S4 interface for EPC capable UEs and Non-EPC capable UEs on the S4-SGSN. When this CLI is not configured and the command "show call-control-profile full name <profile_name>" is executed, the output incorrectly displays the section "SGSN Core Network Interface Selection".

When the configuration contains a S4 SGSN license and a Call-Control-Profile is created. The CLI "sgsn-core-nw-interface" under the Call Control Profile Configuration mode is configured. Subsequently the command "remove sgsn-core-nw-interface" is executed and the configuration is removed. The following show outputs do not reflect the configuration changes correctly:

- The "show config" command incorrectly displays the cli "sgsn-core-nw-interface < interface_type >"
- The "show config verbose" command incorrectly displays the cli "sgsn-core-nw-interface < interface_type >"
- The "show config call-control-profile full name < profile_name >" command incorrectly displays the section "SGSN Core Network Interface Selection" section.

New Behavior: All of the above mentioned issues have been fixed:
• When the configuration contains only SGSN license, the CLI "sgsn-core-nw-interface < interface-type >" and the section "SGSN Core Network Interface Selection" are not displayed on execution of any show command.

• When the configuration contains S4 SGSN license and the CLI "sgsn-core-nw-interface" is not configured, "remove sgsn-core-nw-interface" is printed in the verbose configuration. When the CLI "sgsn-core-nw-interface" is configured, the CLI "sgsn-core-nw-interface < interface-type >" and the section "SGSN Core Network Interface Selection" are displayed in all show outputs. If the configuration is explicitly removed using the remove option of the command, the show outputs reflect this change and the CLI "sgsn-core-nw-interface < interface-type >" and "SGSN Core Network Interface Selection" sections are not displayed. When the configuration is removed, "remove sgsn-core-nw-interface" is printed in the verbose configuration.
CSCus30042 - [18.0] "show conf" need not to display default configs
S-GW Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from S-GW in StarOS 18 software releases.

- S-GW Enhancements for 18.5, page 347
- S-GW Enhancements for 18.4, page 348
- S-GW Enhancements for 18.3, page 348
- S-GW Enhancements for 18.2, page 348
- S-GW Enhancements for 18.1, page 351

S-GW Enhancements for 18.5

This section identifies all of the S-GW enhancements included in this release:

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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 S-GW.

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

Private Extension IE in DDN Message Sent Only if S-GW Paging Feature is Enabled

CDETS = CSCuu10425 - Private Extension IE in DDN message is always present

**Applicable Products:** S-GW

The fix implemented for CSCuu10425 has resulted in a behavior change.

**Previous Behavior:** A data triggered DDN always sent out the Separate Paging Information Element (IE) under Private Extension even if the S-GW Paging feature was not enabled.

**New Behavior:** A data triggered DDN sends out the Separate Paging IE only if the S-GW Paging feature is enabled.

S-GW Enhancements for 18.4

There are no S-GW enhancements for this release.

S-GW Enhancements for 18.3

There are no S-GW enhancements for this release.

S-GW Enhancements for 18.2

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 *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 S-GW.
CSCuq37460 - Min ARP calculation at SessMgr does not consider individual parameters

Feature Changes

ARP Value Calculation Change

The fix for CSCuq37460 has introduced a behavior change. The minimum ARP value sent in the DDN is now calculated considering only the ARP priority level field. The ARP contains Spare (1 bit) + PCI (1 bit) + PL (4 bits) + Spare (1 bit) + PVI (1 bit). The PL has values from 1 to 15, with 1 having the highest priority.

Previous Behavior: Previously, the whole ARP value (PCI + PL + PVI) was used for calculating the minimum ARP in the DDN.

New Behavior: Only the ARP priority level field is used for calculating the minimum ARP in the DDN.

CSCut49838 - Statistics error displayed for sgw or pgw stats associated in saegw

Feature Changes

Error Message Changed

If S-GW or P-GW service(s) were configured as part of an SAEGW service, the system would return an incorrect error message when the show sgw-service statistics name or show pgw-service statistics name commands were executed. Even though the S-GW and P-GW services were part of the SAEGW service and were configured and active, the error message indicated that the services were not configured or active.
Previous Behavior: When the `show pgw-service statistics name` command was executed for a P-GW service that was part of the SAEGW service, the error message would read:

- **PGW <name> Does not exist or is not active**

When the `show sgw-service statistics name` command was issued for an S-GW service that was part of the SAEGW service, the error message would read:

- **Warning: SGW Service <name> not yet configured**

New Behavior: The corrected behavior is as follows:

1. If the requested P-GW service is part of an SAEGW service, then issuing the `show pgw-service statistics name` command results in the following message:
   - **PGW <name> is part of SAEGW service. Use 'show saegw-service statistics' CLI.**

2. If all requested P-GW services are part of an SAEGW service, then issuing the `show pgw-service statistics all` command results in the following message:
   - **PGW is part of SAEGW service. Use 'show saegw-service statistics' CLI.**

3. If the requested SGW service is part of SAEGW service, then issuing the `show sgw-service statistics name` command results in the following error message:
   - **Warning: SGW Service <name> is part of SAEGW service. Use 'show saegw-service statistics' CLI.**

4. If all SGW services are part of the SAEGW service, then issuing the `show sgw-service statistics all` command results in the following error message:
   - **Warning: SGW Service is part of SAEGW service. Use show saegw-service statistics CLI.**

CSCuu37427, CSCut14324 - Assertion failure egtpc_handle_create_sess_req_msg_at_sgw_ingress

Feature Changes

Parallel Create Session Requests Processed Correctly

The fix implemented for CSCuu37427 has resulted in a behavior change.

Previous Behavior: When two parallel CSReq's with different EBI and 0 TEID were received from the S4-SGSN, the second CSReq was rejected from the S-GW with the cause "No Resource Available."

New Behavior: When two parallel CSReq's with different EBI and 0 TEID are received from the S4-SGSN, both of the CSReq's are processed and the PDNs are created successfully at the S-GW.

1. Operators will see that both the PDNs are created successfully after the fix if the two CSReq's are received from the S4-SGSN with 0 TEID and different EBI.
2. If two parallel CSReq's are received from the MME, then the old behavior of rejecting the second CSReq with the cause "No Resource Available" is applicable.
3. If one CSReq is received from the MME and the other from the S4-SGSN, or vice-versa, with the same or different EBI, then context replacement is triggered and the second CSReq results in the replacement of the existing PDN with a new PDN.
CSCuu50651 - SGW: MBR from S4SGSN with HI not fwded to PGW for WiFi to UTRAN/GERAN HO

Feature Changes

S-GW Support for Non-3GPP (WiFi) to UTRAN/GERAN Handover

The fix implemented for CSCuu50651 has resulted in a behavior change. The S-GW now will support the non-3GPP (WiFi) to UTRAN/GERAN handover, as per the 3GPP spec 23.402 Rel 12.7 section 8.2.1.3; General Procedure for GTP-based S5/S8 for UTRAN/GERAN.

Previous Behavior: The S-GW was not supporting the non-3GPP to UTRAN/GERAN handover.

New Behavior: The S-GW will support non-3GPP to UTRAN/GERAN handover.

CSCuu52039 - SGW is rejecting UBR in case of wifi to LTE HO

Feature Changes

Change in Action Taken During MBReq-UBReq Collision at S-GW Egress Interface

The fix implemented for CSCuu52039 has resulted in a behavior change.

Important

This behavior change affects only the action taken during MBReq-UBReq Collision at the S-GW egress interface for WiFi-to-LTE handovers.

Previous Behavior: If a handover MBResp was not yet received for a WiFi to LTE handover scenario, and a UBReq was received at the S-GW egress interface, then the UBReq was being rejected with the cause "No Resource Available."

New Behavior: If a handover MBResp is not yet received for a WiFi to LTE handover scenario, and a UBReq is received at the S-GW egress interface, then the UBReq will be dropped. Discard statistics will be incremented.

Customer Impact: Fewer update failures during inter-access handovers.

S-GW Enhancements for 18.1

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

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

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

CSCul17192 - [SGW] Enhance Clear subs CLI to generate DBReq to control the pace

Feature Changes

Enhanced Clear Subscribers Command for VoLTE

The clear subscribers non-VoLTE auto-delete command was implemented in StarOS release 17.0. This command can generate a burst of Delete Bearer Requests (DBR) and Delete Session Requests (DSR) in customer setups. To prevent the flooding of peer nodes with session removal control procedures, it is important to distribute these messages evenly in a periodic manner.

The pace-out-interval keyword has been added to the clear subscribers CLI command to allow operators to specify the time duration for removing the sessions so that control messages sent across to peer nodes are evenly distributed.

Sessions that are "paced-out" over a period of time move into a disconnecting state; however, data and control path activity continue as usual until the system sends out session deletion message(s). In the case of session recovery, "paced-out" sessions are recovered in the connected state and the clear subscriber command must be initiated again to clear the recovered sessions.
Command Changes

clear subscriber

The new keyword `pace-out-interval` has been added to this command so that session deletion messages are paced out on the basis of the time interval specified.

```
clear subscribers pace-out-interval interval_in_seconds
clear subscribers all pace-out-interval interval_in_seconds
clear subscribers non-volte-calls pace-out-interval interval_in_seconds
clear subscribers pgw-only all pace-out-interval interval_in_seconds
clear subscribers saegw-only all pace-out-interval interval_in_seconds
clear subscribers sgw-only all pace-out-interval interval_in_seconds
```

Notes:

• Where `paceout-interval` is the time, in seconds, that session deletion messages are sent out.

`interval_in_seconds` must be an integer from 0 to 86400.

CSCup56736 - SGW Bearer Duration KPIs

Feature Changes

Bearer Duration KPIs

The `show session duration` command has been enhanced to allow operators to specify one, some, or all Quality of Class Identifiers (QCI) for a session to provide detailed session duration information. These enhancements provide the length of time a dedicated bearer has been established on the network. QCI-specific bulkstats have also been added. This command is also valid for the P-GW, SAEGW, and GGSN.

Performance Indicator Changes

System Schema

The following bulk statistics have been added to the System schema in support of the Bearer Duration KPIs feature.

In-Progress Call Duration Statistics

• QCI 1:
  • sess-bearerdur-5sec-qci1
  • sess-bearerdur-10sec-qci1
  • sess-bearerdur-30sec-qci1
  • sess-bearerdur-1min-qci1
  • sess-bearerdur-2min-qci1
• sess-bearer-dur-5min-qci1
• sess-bearer-dur-15min-qci1
• sess-bearer-dur-30min-qci1
• sess-bearer-dur-1hr-qci1
• sess-bearer-dur-4hr-qci1
• sess-bearer-dur-12hr-qci1
• sess-bearer-dur-24hr-qci1
• sess-bearer-dur-over-24hr-qci1
• sess-bearer-dur-4day-qci1
• sess-bearer-dur-5day-qci1

• QCI 2:
  • sess-bearer-dur-5sec-qci2
  • sess-bearer-dur-10sec-qci2
  • sess-bearer-dur-30sec-qci2
  • sess-bearer-dur-1min-qci2
  • sess-bearer-dur-2min-qci2
  • sess-bearer-dur-5min-qci2
  • sess-bearer-dur-15min-qci2
  • sess-bearer-dur-30min-qci2
  • sess-bearer-dur-1hr-qci2
  • sess-bearer-dur-4hr-qci2
  • sess-bearer-dur-12hr-qci2
  • sess-bearer-dur-24hr-qci2
  • sess-bearer-dur-over-24hr-qci2
  • sess-bearer-dur-4day-qci2
  • sess-bearer-dur-5day-qci2

• QCI 3:
  • sess-bearer-dur-5sec-qci3
  • sess-bearer-dur-10sec-qci3
  • sess-bearer-dur-30sec-qci3
  • sess-bearer-dur-1min-qci3
  • sess-bearer-dur-2min-qci3
  • sess-bearer-dur-5min-qci3
• sess-bearer-dur-15min-qci3
• sess-bearer-dur-30min-qci3
• sess-bearer-dur-1hr-qci3
• sess-bearer-dur-4hr-qci3
• sess-bearer-dur-12hr-qci3
• sess-bearer-dur-24hr-qci3
• sess-bearer-dur-over24hr-qci3
• sess-bearer-dur-4day-qci3
• sess-bearer-dur-5day-qci3

• QCI 4:
• sess-bearer-dur-5sec-qci4
• sess-bearer-dur-10sec-qci4
• sess-bearer-dur-30sec-qci4
• sess-bearer-dur-1min-qci4
• sess-bearer-dur-2min-qci4
• sess-bearer-dur-5min-qci4
• sess-bearer-dur-15min-qci4
• sess-bearer-dur-30min-qci4
• sess-bearer-dur-1hr-qci4
• sess-bearer-dur-4hr-qci4
• sess-bearer-dur-12hr-qci4
• sess-bearer-dur-24hr-qci4
• sess-bearer-dur-over24hr-qci4
• sess-bearer-dur-4day-qci4
• sess-bearer-dur-5day-qci4

• QCI 5:
• sess-bearer-dur-5sec-qci5
• sess-bearer-dur-10sec-qci5
• sess-bearer-dur-30sec-qci5
• sess-bearer-dur-1min-qci5
• sess-bearer-dur-2min-qci5
• sess-bearer-dur-5min-qci5
• sess-bearer-dur-15min-qci5
• sess-bearerdur-30min-qci5
• sess-bearerdur-1hr-qci5
• sess-bearerdur-4hr-qci5
• sess-bearerdur-12hr-qci5
• sess-bearerdur-24hr-qci5
• sess-bearerdur-over24hr-qci5
• sess-bearerdur-4day-qci5
• sess-bearerdur-5day-qci5

• QCI 6:
  • sess-bearerdur-5sec-qci6
  • sess-bearerdur-10sec-qci6
  • sess-bearerdur-30sec-qci6
  • sess-bearerdur-1min-qci6
  • sess-bearerdur-2min-qci6
  • sess-bearerdur-5min-qci6
  • sess-bearerdur-15min-qci6
  • sess-bearerdur-30min-qci6
  • sess-bearerdur-1hr-qci6
  • sess-bearerdur-4hr-qci6
  • sess-bearerdur-12hr-qci6
  • sess-bearerdur-24hr-qci6
  • sess-bearerdur-over24hr-qci6
  • sess-bearerdur-4day-qci6
  • sess-bearerdur-5day-qci6

• QCI 7:
  • sess-bearerdur-5sec-qci7
  • sess-bearerdur-10sec-qci7
  • sess-bearerdur-30sec-qci7
  • sess-bearerdur-1min-qci7
  • sess-bearerdur-2min-qci7
  • sess-bearerdur-5min-qci7
  • sess-bearerdur-15min-qci7
  • sess-bearerdur-30min-qci7
• sess-bearerdur-1hr-qci7
• sess-bearerdur-4hr-qci7
• sess-bearerdur-12hr-qci7
• sess-bearerdur-24hr-qci7
• sess-bearerdur-over24hr-qci7
• sess-bearerdur-4day-qci7
• sess-bearerdur-5day-qci7

• QCI 8:
• sess-bearerdur-5sec-qci8
• sess-bearerdur-10sec-qci8
• sess-bearerdur-30sec-qci8
• sess-bearerdur-1min-qci8
• sess-bearerdur-2min-qci8
• sess-bearerdur-5min-qci8
• sess-bearerdur-15min-qci8
• sess-bearerdur-30min-qci8
• sess-bearerdur-1hr-qci8
• sess-bearerdur-4hr-qci8
• sess-bearerdur-12hr-qci8
• sess-bearerdur-24hr-qci8
• sess-bearerdur-over24hr-qci8
• sess-bearerdur-4day-qci8
• sess-bearerdur-5day-qci8

• QCI 9:
• sess-bearerdur-5sec-qci9
• sess-bearerdur-10sec-qci9
• sess-bearerdur-30sec-qci9
• sess-bearerdur-1min-qci9
• sess-bearerdur-2min-qci9
• sess-bearerdur-5min-qci9
• sess-bearerdur-15min-qci9
• sess-bearerdur-30min-qci9
• sess-bearerdur-1hr-qci9
show session duration qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | non-std } +

The qci keyword has been added to this command to allow operators to view the length of time a dedicated bearer is established on the network for a given QCI. More than one QCI value can be specified.

Note: < = less than, > = greater than.

In-Progress Call Duration Statistics

- QCI <QCI value>
  - <5 seconds
  - <10 seconds
  - <30 seconds
  - <1 min
CSCup82065 - Abnormal bearer termination info in CDR

Feature Changes

Abnormal Bearer Termination Cause in CDR

This feature provides additional information in a S-GW CDR for a VoLTE call drop. A dropped bearer was previously reported as a 'abnormalrelease' in the CDR. This feature has the S-GW CDRs indicate the proper bearer release for all failure cases identified in the VoLTE Retainability formula. This will provide the customer with the ability to perform gateway/network wide analysis for failures in the network.

**Previous Behavior:** 1) For SGW/SAEGW(Pure S)/SAEGW(Co-located) calls previously, for GTP-C/GTP-U path failure disconnect-reason of path-failure was used. 2) For SGW/SAEGW(Pure S)/SAEGW(Co-located) calls for GTPU error indication local-disconnect was used.

**New Behavior:** 1) For SGW/SAEGW(Pure S)/SAEGW(Co-located) calls, new disconnect reasons have been added containing interface information for GTP-C/GTP-U path failure. 2) For SGW/SAEGW(Pure S)/SAEGW(Co-located) calls, new disconnect reasons have been added containing interface information for GTPU error indication

**Customer Impact:** New disconnect reasons will be available for call disconnect. New field abnormalTerminationCause enum 83 is added in the S-GW CDR for a specific customer dictionary. New abnormal termination CDR enum values have also been added in an SGW CDR as part of the network specific diagnostic field in the appropriate dictionary. A new field has also been added in SGW CDR for CDR closure cause abnormal release.
Performance Indicator Changes

System Schema

The following bulk statistics have been added to the System schema in support of this feature.

- disc-reason-590
- disc-reason-591
- disc-reason-592
- disc-reason-593
- disc-reason-594
- disc-reason-595
- disc-reason-596
- disc-reason-597
- disc-reason-598
- disc-reason-599
- disc-reason-600

show session disconnect-reasons

The output of this command has been enhanced to show the new counters added in support of the Abnormal Bearer Termination Cause in CDR feature.

- path-failure-s5
- path-failure-s11
- path-failure-s4
- gtpu-err-ind-s5u
- gtpu-err-ind-s1u
- gtpu-err-ind-s4u
- gtpu-path-failure-s12
- gtpu-path-failure-s5u
- gtpu-err-ind-s12
- gtpu-path-failure-s1u
- gtpu-path-failure-s4u
CSCup82477 - [SGW]: ICSR IDLE Secs checkpointing optimization

Feature Changes

ICSR Micro Checkpoint Optimization for Idle Seconds

ICSR micro checkpoint periodicity for idlesecs is now configurable. This option can be used instead of using the default periodicity of 10 seconds. This way the operators can configure this setting to a large value to suit their need to reduce the number of micro checkpoints on the srp link.

Customer Impact: When this CLI command is configured, idlesecs micro checkpoints are sent at configured regular intervals to the standby chassis. If not configured, micro checkpoints are sent at intervals of 10 seconds which is the default value.

Command Changes

timeout-idle

A new keyword micro-checkpoint-periodicity has been added to the timeout-idle command in S-GW Service Configuration Mode to make the idlesecs micro checkpoint configurable. If this keyword is not configured, the default periodicity of 10 seconds is used.

configure
context context_name
  sgw-service sgw_service_name
    timeout idle seconds [micro-checkpoint-periodicity seconds]
  end
end

Notes:

• Where micro-checkpoint-periodicity specifies the time interval, in seconds, used for the sending of micro checkpoints. Valid entries are from 0 to 10000 seconds.

Performance Indicator Changes

show sgw-service name

The output of this command has been enhanced to show the configured setting for micro-checkpoint-periodicity.

• Idle timeout micro checkpoint periodicity: <seconds>.
CSCup82660 - ULI enhancements

Feature Changes

ULI Enhancements

VoLTE carriers need the last cell/sector updates within the IMS CDRs to assist in troubleshooting customer complaints due to dropped calls as well as LTE network analysis, performance, fraud detection, and operational maintenance. The ultimate objective is to get the last cell sector data in the IMS CDR records in addition to the ULI reporting for session establishment.

To address this issue, the S-GW now supports the following:

- RAN/NAS Cause IE within bearer context of Delete Bearer Command message.
- The S-GW ignores the ULI received as call is going down so there is no point in updating the CDR.

Support for ULI and ULI Timestamp in Delete Bearer Command message had already been added in release 17.0.

Previous Behavior: ULI received in Delete Bearer Command was ignored
New Behavior: When a new ULI is received in the Delete Bearer Command message, a S-GW CDR is initiated.

CSCup86002, CSCup33431, CSCuq44967, CSCuq44973 - R12 GTP-C load and overload control Support on SGW

Feature Changes

R12 GTP-C Load and Overload Support on the S-GW

GTP-C Load Control feature is a licensed, optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control information in order to mitigate overload situations for the overloaded node through actions taken by the peer node(s). This feature is supported over S4, S11, S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control Information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.
In brief, load control and overload control can be described in this manner:

- **Load control** enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

- **Overload control** enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its GTP-C peers to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signalling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.

---

**Important**
Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

---

**Operation**

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization, and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, \(((\text{number of active sessions per service}) / \text{max session allowed for the service license}) \times 100\).

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

**Command Changes**

**gtpc-load-control-profile**

This command has been added to Global Configuration Mode to create a GTP-C Load Control Profile and enter GTP-C Load Control Configuration Mode.

```
configure
  [ no ] gtpc-load-control-profile  profile_name
end
```

Notes:

- **no**: Removes specified GTP-C Load Control Profile.
- **profile_name** must be an alphanumeric string from 1 to 64 characters in length.
inclusion-frequency

This new command has been added to GTP-C Load Control Profile Configuration Mode to configure parameters to decide the inclusion frequency of the Load Control Information IE.

configure
gtpc-load-control-profile profile_name
  inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor } 
  default inclusion-frequency { advertisement-interval | change-factor } 
end

Notes:

• inclusion frequency: Configures parameters to decide inclusion frequency of load control information element.

• advertisement-interval interval_in_seconds: Configures advertisement-interval for load control in seconds.
  
  interval_in_seconds must be an integer from 0 to 3600.
  Default: 300

• change-factor change_factor: Configures change factor for load control.
  
  change_factor must be an integer from 1 to 20.
  Default: 5%

weightage

This new command has been added to GTP-C Load Control Profile Configuration Mode to configure weightage for various load control parameters. Total weightage of all parameters should be 100%.

configure
gtpc-load-control-profile profile_name
  weightage system-cpu-utilization percentage system-memory-utilization percentage
  license-session-utilization percentage
  default weightage
end

Notes:

• system-cpu-utilization percentage: Configures system CPU utilization weightage as a percentage of 100.
  
  percentage must be an integer from 0 to 100.
  Default: 40%

• system-memory-utilization percentage: Configures system memory utilization weightage as a percentage of 100.
  
  percentage must be an integer from 0 to 100.
  Default: 30%

• license-session-utilization percentage: Configures license session utilization weightage as a percentage of 100.
  
  percentage must be an integer from 0 to 100.
  Default: 30%
• The total of all three parameter entries should be 100%.

gtpc-overload-control-profile

This new command has been added to Global Configuration Mode to create a GTP-C Overload Configuration profile and to enter GTP-C Overload Configuration Mode.

configure
 [ no ] gtpc-overload-control-profile profile_name
end

Notes:
• no: Removes specified GTP-C Overload Control Profile.
• profile_name must be an alphanumeric string from 1 to 64 characters in length.

inclusion-frequency

This new command has been added to GTP-C Overload Configuration Mode to configure parameters to decide inclusion frequency of the Overload Control Information IE.

configure
 gtpc-overload-control-profile profile_name
 inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor }
 default inclusion-frequency { advertisement-interval | change-factor }
end

Notes:
• inclusion_frequency: Configures parameters to decide inclusion frequency of load control information element.
• advertisement-interval interval_in_seconds: Configures advertisement-interval for Overload Control in seconds.
  interval_in_seconds must be an integer from 0 to 3600.
  Default: 300
• change-factor change_factor: Configures change factor for overload control.
  change_factor must be an integer from 1 to 20.
  Default: 5%

throttling-behavior

This new command has been added to GTP-C Overload Configuration Mode to exclude events/messages from throttling due to a peer’s overload reduction metric.

configure
 gtpc-overload-control-profile profile_name
  throttling-behavior { earp [1|2|3|4|5|6|7|8|9|10|11|12|13|14|15 ]+ exclude } | emergency-events exclude
 }
 no throttling-behavior [ earp [1|2|3|4|5|6|7|8|9|10|11|12|13|14|15 ]+ exclude | emergency-events exclude
 end

Notes:
• **throttling-behavior**: Configures throttling behavior based on peer's overload reduction-metric.

• **earp**: Excludes the specified messages with configured earp from throttling due to the peer's overload reduction metric.

• **+**: More than one of the previous keywords can be entered within a single command.

• **emergency-events exclude**: Excludes the emergency events from throttling due to the peer's overload reduction metric.

### tolerance

This new command has been added to GTP-C Overload Configuration Mode to configure overload tolerance limits.

```plaintext
configure
gtpc-overload-control-profile profile_name
tolerance { initial-reduction-metric percentage | threshold report-reduction-metric percentage
self-protection-limit percentage }
default tolerance [ initial-reduction-metric | threshold ]
end
```

**Notes:**

• **initial-reduction-metric percentage**: Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit.
  
  *percentage* must be an integer from 1 to 100.
  
  Default: 10%

• **threshold report-reduction-metric percentage**: Configures the minimum overload tolerance threshold for advertising the overload reduction metric to the peer.
  
  *percentage* must be an integer from 1 to 100.
  
  Default: 80%

• The **threshold report-reduction-metric** should always be lower than the **self-protection-limit**.

• **self-protection-limit percentage**: Configures the maximum overload tolerance threshold after which node will move to self protection mode.
  
  *percentage* must be an integer from 1 to 100.
  
  Default: 95%

### validity-period

This new command has been added to GTP-C Overload Configuration Mode to configure the time, in seconds, that specifies how long the overload control information is valid.

```plaintext
configure

gtpc-overload-control-profile profile_name
validity-period seconds
default validity-period
end
```

**Notes:**

• The default is 600 seconds.
• **validity-period** seconds: Configures the validity of overload control information. 
  
  *seconds* must be an integer from 1 to 3600.

### weightage

This new command has been added to GTP-C Overload Configuration Mode to configure weightage for various overload control parameters.

```configure
gtpc-overload-control-profile profile_name
  weightage system-cpu-utilization percentage
  system-memory-utilization percentage
license-session-utilization percentage
  default weightage
end
```

**Notes:**

- Total weightage for all parameters should be 100%.
- **system-cpu-utilization** percentage: Configures system cpu utilization weightage as a percentage of 100.
  
  *percentage* must be an integer from 0 to 100.
  
  Default: 40%

- **system-memory-utilization**

```system-memory-utilization percentage
```

*percentage* must be an integer from 0 to 100.

Default: 30%

- **license-session-utilization** percentage: Configures license session utilization weightage as a percentage of 100.

```license-session-utilization percentage
```

*percentage* must be an integer from 0 to 100.

Default: 30%

### associate

The `gtpc-load-control-profile profile_name` and `gtpc-overload-control-profile profile_name` commands have been added to P-GW Service Configuration Mode to associate existing Load Control Profile and Overload Control Profiles to a configured P-GW service.

```configure
context context_name
  pgw-service pgw_service_name
    associate gtpc-load-control-profile profile_name
    associate gtpc-overload-control-profile profile_name
    no associate gtpc-load-control-profile
    no associate gtpc-overload-control-profile
end
```
associate

The `gtpc-load-control-profile profile_name` and `gtpc-overload-control-profile profile_name` commands have been added to S-GW Service Configuration Mode to associate an S-GW Load Control Profile to a configured S-GW service.

```plaintext
configure
  context context_name
    sgw-service sgw_service_name
      associate gtpc-load-control-profile profile_name
      associate gtpc-overload-control-profile profile_name
    exit
  pgw-service pgw_service_name
    associate gtpc-load-control-profile profile_name
    associate gtpc-overload-control-profile profile_name
  exit
  saegw-service saegw_service_name
    associate sgw-service sgw_service_name
    associate pgw-service pgw_service_name
  exit
end
```

associate

The `gtpc-load-control-profile <profile_name>` and `gtpc-overload-control-profile <profile_name>` commands have been added to S-GW Service and P-GW Service Configuration Modes to enable the association of a Load and Overload Control Profile to a configured SAEGW service.

```plaintext
configure
  context context_name
    sgw-service sgw_service_name
      associate gtpc-load-control-profile profile_name
      associate gtpc-overload-control-profile profile_name
    exit
  pgw-service pgw_service_name
    associate gtpc-load-control-profile profile_name
    associate gtpc-overload-control-profile profile_name
  exit
  saegw-service saegw_service_name
    associate sgw-service sgw_service_name
    associate pgw-service pgw_service_name
  exit
end
```

Performance Indicator Changes

EGTPC Schema

The following bulk statistics have been added to the eGTP-C schema in support of the R12 Load and Overload Control feature:

- load-overload-own-lci
- load-overload-own-oci
- load-overload-num-msg-throttled
- load-overload-num-ovrload-cond-reached
show egtpc statistics

The output of this command has been enhanced to provide information on the S-GW's configured Load and Overload Control Profiles.

- Load Control Information
  - No. of Times Load Control Info TX
  - Current Load Factor

- Overload Control Information
  - No. of Times Overload Control Info TX
  - Current Overload Factor
  - Current Overload Reduction Metric
  - No. of times Overload Threshold Reached
  - Number of Messages Throttled

The output of this command has also been enhanced to show S-GW Load and Overload Control Profile information of the S-GW peer. For example, peer output would appear if the following command was executed on the S-GW:

show egtpc statistics mme-address 1.1.1.1

- Load Control Information
  - No. of Times Load Control Info RX
  - Current Load Factor

- Overload Control Information
  - No. of Times Overload Control Info TX
  - Current Overload Factor
  - Current Overload Reduction Metric
  - No. of times Overload Threshold Reached
  - Number of Messages Throttled

show gtpc-load-control-profile full all

This new command has been added to Exec Mode to enable operators to view all configured parameters for all GTP-C Load Control Profiles on the S-GW.

- GTP-C Load Control Profile Name
- Weightage
  - System CPU Utilization Weightage <percentage>
Inclusion Frequency
  - Change Factor <factor:1:20>
  - Advertisement Interval <seconds>

**show gtpc-overload-control-profile full all**

This new command has been added to Exec Mode to enable operators to view all configured parameters for all GTP-C Overload Control Profiles on the S-GW.

- GTP-C Overload Control Profile Name
- Weightage
  - System CPU Utilization Weightage <percentage>
  - System Memory Utilization Weightage <percentage>
  - License Session Utilization Weightage <percentage>
- Tolerance
  - Report Reduction Metric <percentage>
  - Self Protection Limit <percentage>
  - Initial-Reduction-Metric <percentage>
- Inclusion Frequency
  - Change Factor <factor:1:20>
  - Advertisement Interval <seconds>
- Validity Period <seconds>
- Throttling Profile
  - Exclude Emergency Events <Enabled/Disabled>
  - Exclude EARP <Enabled/Disabled>

**show pgw-service all**

The output of this command has been enhanced to list the configured S-GW Load and Overload Control profiles associated with P-GW services.

- GTP-C Load Control Profile <name>
- GTP-C Overload Control Profile <name>
show sgw-service all

The output of this command has been enhanced to list the configured S-GW Load and Overload Control profiles associated with S-GW services.

- GTP-C Load Control Profile <name>
- GTP-C Overload Control Profile <name>

**CSCup86011 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure**

**Feature Changes**

**VoLTE-ICSR-SR: Resolving IMS Sessions Hung after SR Failure**

Audit failures at time of session recovery or ICSR switchover could lead to IMS sessions being hung on peer nodes (MME/S4-SGSN and P-GW) because previously, the S-GW service didn't signal them for session removal. Any signaling messages initiated by the network towards the UE, for example, SIP message or IMS data will not be delivered, as the S-GW did not have valid session information for the UE.

The S-GW has been enhanced to attempt to notify all the peers of the removal of the session. Session recovery and ICSR switchover audit failures are handled in such a way that UE will be informed about the call failure so that it triggers the re-registration procedure. The S-GW will send Delete Bearer Request and Delete Session Request to the MME/S4-SGSN and P-GW respectively for audit-failed sessions.

**Previous Behavior:** When this feature is not enabled, local purge for ICSR audit failed calllines is being done. No external signaling is done to signal peer of session termination.

**New Behavior:** When this feature is enabled, graceful cleanup for ICSR audit failed calllines will happen, that is, signaling to external peers of session termination will occur in this case.

**Important**

The Inter-Chassis Session Recovery (ICSR) license is required to use this feature. Please contact your Cisco representative for licensing requirement information.

**Command Changes**

**require graceful-cleanup-during-audit-failure**

This new command has been added to Global Configuration Mode to enable graceful cleanup for ICSR audit failures.

```
configure
  require graceful-cleanup-during-audit-failure
  no require graceful-cleanup-during-audit-failure cmd
end
```

Notes:
Performance Indicator Changes

**show session disconnect-reasons**

The output of this Exec Mode command has been enhanced to show the number of sessions purged based on gracefully cleaned up audit failed calllines.

- Disconnect Reason
  - graceful-cleanup-on-audit-fail <total>

**show srp checkpoint statistics**

The output of this Exec Mode command has been enhanced to provide a count maintained on the number of audit failed calllines that are gracefully cleaned up. That is, for the calllines where the gateway made an attempt to notify the peers of session termination gracefully.

- Graceful call drops during audit failure <total>

CSCup86021, CSCum49101 - Rel12 New Cause-code IE

Feature Changes

**3GPP Release 12 Cause-Code IE Support**

When an ERAB or a data session is dropped, an operator may need to get, in addition to the ULI information, detailed RAN and/or NAS release cause codes information from the access network to be included in the S-GW and P-GW CDRs for call performance analysis, and user QoE analysis and proper billing reconciliation. Also, for IMS sessions, the operator may need to get the above information available at P-CSCF.

'Per E-RAB Cause' is received in ERAB Release Command and ERAB Release Indication messages over S1. However RAN and NAS causes are not forwarded to the SGW and PGW, nor provided by the P-GW to PCRF.

To resolve this issue a "RAN/NAS Release Cause" information element (IE), which indicates AS and/or NAS causes, has been added to the Session Deletion Request and Delete Bearer Command. The "RAN/NAS Release Cause" provided by the MME is transmitted transparently by the S-GW to the P-GW (if there exists signalling towards P-GW) for further propagation towards the PCRF.

For backward compatibility, the S-GW can still receive the cause code from the CC IE in the S4/S11 messages and/or receive the cause code from some customers' private extension.

**Previous Behavior:** Previously RAN/NAS Cause code was supported only in a specific private extension. New RAN/NAS cause code IE was not coming in earlier releases.
**New Behavior:** 3GPP defined RAN/NAS Cause code IE support is added. The S-GW will still support the existing behavior of the specific private extension to carry RAN/NAS cause code for backward compatibility. The same is supported in S-GW CDR in dictionary **custom34**.

**Customer Impact:** Support has been added for RAN/NAS Cause code IE in DSR & DBCmd and also forwarded the same to the P-GW and in the S-GW-CDR.

**CSCuq03551 - [SGW] Show command enhancements**

**Feature Changes**

*show session Counter Enhancements*

Several show session commands have been enhanced to provide detailed information on the access type (3G, 4G, eHRPD or WiFi) being used for the session, as well as for call states.

**Performance Indicator Changes**

*show session counters historical all 3g*

The output of this command has been enhanced to provide various call states by session and 3G access type:

- Arrived
- Rejected
- Connected
- Disconn (Disconnected)
- Failed
- Handoffs
- Renewals
- CallOps (Call Operations)

*show session counters historical all 4g*

The output of this command has been enhanced to provide various call states by session and 4G access type:

- Arrived
- Rejected
- Connected
- Disconn (Disconnected)
- Failed
- Handoffs
show session summary

The new keyword summary has been added to this command to provide the same output as `show subscriber summary` along with additional session information for each access-type.

- 4G LTE (EURTRAN)
- 2G (GERAN)
- 3G (UTRAN)
- WiFi (Wireless LAN)
- eHRPD
- Others
- Total Subscribers:
  - Active
  - Dormant
  - LAPI Devices
  - pdsn-simple-ipv4
  - pdsn-simple-ipv6
  - pdsn-mobile-ipv
  - ha-mobile-ipv6

show session counters historical all 3g

The output of this command has been enhanced to provide historical information on various call states by session for 3G sessions.

- Arrived
- Rejected
- Connected
- Disconn (Disconnected)
- Failed
- Handoffs
- Renewals
- CallOps (Call Operations)
show session counters historical all 4g

The output of this command has been enhanced to provide historical information on various call states by session for 4G sessions.

- Arrived
- Rejected
- Connected
- Disconn (Disconnected)
- Failed
- Handoffs
- Renewals
- CallOps (Call Operations)

**CSCuq11129 - SGW SM Support for P-GW/GGSN needs P-CSCF failure detection support**

**Feature Changes**

**P-CSCF Failure Detection Support**

In the HSS-based P-CSCF restoration procedure, the MME/SGSN receives a specific indication from the HSS when a P-CSCF restoration procedure must be triggered. The MME/SGSN then must propagate this indication to the PGW.

The HSS-based P-CSCF restoration procedure is added as a new procedure triggering a Modify Bearer Request procedure. A new P-CSCF Restoration Indication flag is introduced in the Modify Bearer Request message.

**Previous Behavior:** PCRI flag was not supported.

**New Behavior:** PCRI flag is supported in Indication IE and when it is received in MBR, the S-GW forwards the MBR to the P-GW including the PCRI flag.

**CSCur47721 - [SGW]: Integration test support for abnormal bearer info feature**

**Feature Changes**

**Behavior Change Resulting from Fix for CSCur47721**

The fix implemented for CSCur47721 has resulted in a behavior change for the show session disconnect-reasons display for S12 interface disconnect reasons.
Previous Behavior: S12 Disconnect reason display was gtpu-path-failure-s12u and gtpu-err-ind-s12u.
New Behavior: S12 disconnect reason display changed to gtpu-path-failure-s12 and gtpu-err-ind-s12.
Customer Impact: Disconnect reason display string is changed for s12 disconnect reasons.

Performance Indicator Changes

show session disconnect-reasons

The disconnect reason output for S12 disconnect reasons have been changed.

• gtpu-err-ind-s12
• gtpu-path-failure-s12

CSCur98632 - show egtpc peer need to display immediate and remote peer separately

Feature Changes

Immediate and Remote Peer Listed Separately in show egtpc peer Command

The show egtpc peer command has been enhanced to show the immediate and remote peer separately for the R12 Load and Overload Support feature.

Previous Behavior: show egtpc peer CLI command was listing the immediate and remote peer together for the R12 Load and Overload Support

New Behavior: show egtpc peer CLI command lists the immediate and remote peer separately for the R12 Load and Overload Support.

Performance Indicator Changes

show egtpc peer

The output of this command has been enhanced to show the remote peer separately from the immediate peer.

• Total Remote Peers
This chapter identifies SNMP MIB objects and alarms added to, modified for, or deprecated from StarOS 18 software releases.

- SNMP MIB Object Changes for 18.5, page 378
- SNMP MIB Alarm Changes as of 18.5, page 378
- SNMP MIB Conformance Changes for 18.5, page 379
- SNMP MIB Object Changes for 18.4, page 380
- SNMP MIB Alarm Changes as of 18.4, page 380
- SNMP MIB Conformance Changes for 18.4, page 381
- SNMP MIB Object Changes for 18.3, page 382
- SNMP MIB Alarm Changes as of 18.3, page 382
- SNMP MIB Conformance Changes for 18.3, page 383
- SNMP MIB Object Changes for 18.2, page 384
- SNMP MIB Alarm Changes as of 18.2, page 384
- SNMP MIB Conformance Changes for 18.2, page 385
- SNMP MIB Object Changes for 18.1, page 386
- SNMP MIB Alarm Changes as of 18.1, page 386
- SNMP MIB Conformance Changes for 18.1, page 387
- SNMP MIB Object Changes for 18.0, page 388
- SNMP MIB Alarm Changes as of 18.0, page 388
- SNMP MIB Conformance Changes for 18.0, page 389
- SNMP Command Changes for 18.0, page 390
SNMP MIB Object Changes for 18.5

This section provides information on SNMP MIB object changes in release 18.5.

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 18.5.
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 18.5.
The following objects 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 18.5.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Alarm Changes as of 18.5

This section provides information on SNMP MIB alarm changes in release 18.5.

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 18.5.
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 18.5.
The following alarms have been modified in this release:
- starDhcpServiceStarted
- starDhcpServiceStopped

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 18.5.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 18.5

This section provides information on SNMP MIB conformance changes in release 18.5.

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 18.5.
The following units of conformance are new in this release:
None in this release.

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 18.5.
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 18.5.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 18.4

This section provides information on SNMP MIB object changes in release 18.4.

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 18.4.
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 18.4.
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 18.4.
The following objects have been deprecated in this release:
None in this release.

SNMP MIB Alarm Changes as of 18.4

This section provides information on SNMP MIB alarm changes in release 18.4.

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 18.4.
The following alarms are new in this release:
• starSAEGWSERVICESTART
• starSAEGWSERVICESTOP

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 18.4.
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 18.4.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 18.4

This section provides information on SNMP MIB conformance changes in release 18.4.

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 18.4.
The following units of conformance are new in this release:
None in this release.

Modified SNMP MIB Conformance

This section identifies modified SNMP MIB conformance available in release 18.4.
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 18.4.
The following units of conformance have been deprecated in this release:
None in this release.
**SNMP MIB Object Changes for 18.3**

This section provides information on SNMP MIB object changes in release 18.3.

---

**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 18.3.

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 18.3.

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 18.3.

The following objects have been deprecated in this release:

None in this release.

---

**SNMP MIB Alarm Changes as of 18.3**

This section provides information on SNMP MIB alarm changes in release 18.3.

---

**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 18.3.

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 18.3.
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 18.3.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 18.3

This section provides information on SNMP MIB conformance changes in release 18.3.

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 18.3.
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 18.3.
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 18.3.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 18.2

This section provides information on SNMP MIB object changes in release 18.2.

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 18.2.
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 18.2.
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 18.2.
The following objects have been deprecated in this release:
None in this release.

SNMP MIB Alarm Changes as of 18.2

This section provides information on SNMP MIB alarm changes in release 18.2.

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

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 18.2.
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 18.2.
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 18.2.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 18.2

This section provides information on SNMP MIB conformance changes in release 18.2.

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 18.2.
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 18.2.
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 18.2.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 18.1

This section provides information on SNMP MIB object changes in release 18.1.

**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 18.1.

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 18.1.

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 18.1.

The following objects have been deprecated in this release:

None in this release.

SNMP MIB Alarm Changes as of 18.1

This section provides information on SNMP MIB alarm changes in release 18.1.

**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 18.1.

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 18.1.
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 18.1.
The following alarms have been deprecated in this release:
None in this release.

SNMP MIB Conformance Changes for 18.1

This section provides information on SNMP MIB conformance changes in release 18.1.

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 18.1.
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 18.1.
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 18.1.
The following units of conformance have been deprecated in this release:
None in this release.
SNMP MIB Object Changes for 18.0

This section provides information on SNMP MIB object changes in release 18.0.

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 18.0.

The following objects are new in this release:

- starImsimgrInstId
- starMMEEMBMSPeerId
- starMMEEMBMSPeerIpAddr
- starMMEEMBMSPeerPortNum

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 18.0.

The following objects have been modified in this release:

- StarentCardType
- starPhyPortId
- starBGPPeerIpv6Address
- starMMEEMBMSServiceVpnName
- starMMEEMBMSServiceServName

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 18.0.

The following objects have been deprecated in this release:

None in this release.

SNMP MIB Alarm Changes as of 18.0

This section provides information on SNMP MIB alarm changes in release 18.0.
New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 18.0.
The following alarms are new in this release:

- starS102ServiceStart
- starS102ServiceStop

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 18.0.
The following alarms have been modified in this release:

- starMMENewConnectionsDisallowed
- starMMENewConnectionsAllowed
- starMCEAssocDown
- starMCEAssocUp

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 18.0.
The following alarms have been deprecated in this release:

None in this release.

SNMP MIB Conformance Changes for 18.0

This section provides information on SNMP MIB conformance changes in release 18.0.

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 18.0.
The following units of conformance are new in this release:

- starGTPCRLFSessMgrInst
- starGTPCRLFVPNName
- starGTPCRLFVPNId
- starGTPCRLFContextName
- starGTPCRLFCurrAppTPS
- starGTPCRLFCurrAppDelayTol
- starGTPCRLFOverThreshold
- starGTPCRLFOverLimit
- starGTPCRLFOverThresholdClear
- starGTPCRLFOverLimitClear

**Modified SNMP MIB Conformance**

This section identifies modified SNMP MIB conformance available in release 18.0.
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 18.0.
The following units of conformance have been deprecated in this release:
None in this release.

**SNMP Command Changes for 18.0**

**CSCur13393 - Cisco ASR5000 SAE-GW High CPU Utilisation Vulnerability**

**Command Changes**

**snmp runtime-debug**

This command enables or disables runtime SNMP debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.
This command also supports optional DEBUGMSG MIB tokens that represent textual MIB files that are to be found and parsed. The list of supported tokens is limited to those that appear in the CLI.

**configure**

```configure
snmp runtime-debug [ debug-tokens token_id token_id ...token_id ]
no snmp runtime-debug
```

Notes:

- **no**: Disables SNMP runtime debugging.
- **[ debug-tokens token_id token_id ...token_id ]**: Enables DEBUGMSG tokens from the list of supported tokens appearing below. Multiple token IDs can be specified.
  - **agentx** – agentx(12) token
  - **disman** – disman(11) token
  - **dump** – dumph(13) token
  - **dumpv** – dumpv token
  - **init_mib** – init_mib(14) token
  - **mib_init** – mib_init(1) token
  - **parse-file** – parse-file(2) token
  - **parse-mibs** – parse-mibs(3) token
  - **read_config** – read_config(4) token
  - **snmp** – snmp(5) token
  - **snmpd** – snmpd(6) token
  - **snmptrapd** – snmptrapd(7) token
  - **transport** – transport(9) token
  - **trap** – trap(8) token
  - **usm** – usm(10) token

The numbers appearing in parentheses above will appear in the output of the `show snmp server` command for "Runtime Debug Token."
CHAPTER 21

System Changes in Release 18

This chapter identifies ASR 5x00 and virtual platform system-level features and functionality added to, modified for, or deprecated from StarOS 18 software releases.

- System and Platform Enhancements for Release 18.5, page 393
- System and Platform Enhancements for Release 18.4, page 394
- System and Platform Enhancements for Release 18.3, page 395
- System and Platform Enhancements for Release 18.2, page 396
- System and Platform Enhancements for Release 18.1, page 401
- System and Platform Enhancements for Release 18.0, page 402

System and Platform Enhancements for Release 18.5

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.

**CSCuv45511 - When an invalid license is applied, CLI should throw error**

*Applicable Products: All*
Feature Changes

Invalid License Automatically Rejected

Previous Behavior: When an invalid license was applied via the Global Configuration mode license key command, the license key was accepted with a one-month grace period.

New Behavior: An invalid license will not be accepted. A Failure error will appear in the output of the license key command when you attempt to configure an invalid license key.

If you use the -force option to install an expiring license key, the license will be placed into a 30-day grace period. StarOS will generate daily syslog error messages and SNMP traps during the grace period.

The output of the show license information command will indicate "License State" as "Not Valid".

CSCuw44496 - Explicit route limit enhancement

Applicable Products: ASR 5000 and ASR 5500, P-GW

Feature Changes

Previous Behavior: When enabled on a P-GW IP address pool, explicit-route advertise causes StarOS to suppress the announcement of a summary route for the address pool. Instead, a host-specific route (/32 for IPv4) is announced each time an address is allocated to a session from the address pool. When the session terminates, the host-specific route for that session will be withdrawn. The limit for explicit host routes was 5,000 per context (5,000 per chassis) towards an upstream router using either iBGP or eBGP as the routing protocol.

New Behavior: The limit for explicit host routes has been increased to 24,000 per context (24,000 per chassis)

System and Platform Enhancements for Release 18.4

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.

CSCut24782 - RAID support for new FSC with single 400GB SSD

Applicable Products: ASR 5500
Feature Changes

New Version of FSC with Single 400GB SSD

**Previous Behavior:** Fabric Storage Cards (FSCs) were equipped with two 200GB solid state drives (SSDs). The two drives were in a RAID 0 configuration supported under the RAID 5 configuration across all FSCs in the ASR 5500 chassis.

**New Behavior:** The 200GB SSDs are no longer available. A new version of the FSC is quipped with a single 400GB SSD in a non-RAID 0 configuration. This new drive configuration required changes to the underlying Linux configuration. Those changes are supported in this release. FCS-400GB cards can be mixed with FSC-200GB cards in an ASR 5500 chassis running this StarOS release.

Performance Indicator Changes

**show card table**

The output of this command now displays the new FCS-400GB as "Fabric & 1x400GB Storage Card".

**show hd raid verbose**

The output of this command now displays only one drive as part of its FSC card details for the FCS-400GB.

System and Platform Enhancements for Release 18.3

This section identifies all of the system and platform enhancements included in this release:

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

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

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

**CSCuv23480** - RAID: CLI options for FSC cards must show only drives that are present

**Applicable Products:** ASR 5500
Feature Changes

Only FSC Slots with Available HD Arrays Can Be Selected

Previous Behavior: The HD RAID Configuration mode select command allowed you to select an HD array for an FSC slot where the array was not available resulting in a system crash.

New Behavior: The list of \texttt{hd<slot>} disk arrays will only include FSC slots for which an array is available.

Command Changes

\texttt{hd-raid select}

In the HD RAID Configuration mode, only those \texttt{hd<slot>} arrays having an FSC slot number with an available disk array can be selected.

\begin{verbatim}
   configure
   \hspace{1em} hd-raid
   \hspace{1em} select \hspace{0.5em} disk
   \hspace{1em} end
\end{verbatim}

Notes:

\begin{itemize}
  \item \texttt{disk} identifies an hd array in the format \texttt{hd<slot>}, where \texttt{<slot>} is an integer from 13 through 18.
\end{itemize}

System and Platform Enhancements for Release 18.2

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.

CSCuo77496 - Upgrade version of OpenSSH used in StarOS

Applicable Products: All products

Feature Changes

Upgrade Remote SSH Service

The StarOS remote SSH service has been upgraded from OpenSSH 3.9 to OpenSSH 6.7.
CSCup47534 - DPC2: GTPU manager, memory + session reconciliation optimization

Applicable Products: ASR 5500 S-GW GTPU

Feature Changes

Potential Impact on Unplanned Card Migration

This DPC2 optimization introduces a probability that during unplanned card migration, if too many requests are pending for the GTPUMgr to add, delete or update a session, some call loss can occur due to an out-of-sync condition between the Sessmgr and GTPUMgr during the audit.

This potential for call loss is very much specific to an unplanned card migration scenario. The optimization increased the number sessions sent towards the GTPUMgr. Depending on the number of pending requests during unplanned card migration, an audit failure may occur and lead to some lost calls.

There is no work around for this problem, as this is happening as part of unplanned migration.

CSCuq86655 - TACACS+ commands not being logged or some commands missing

Applicable Products: All products

Associated CDETS ID: CSCuu72188

Feature Changes

StarOS Authorizations for TACACS+ Users

Previous Behavior: StarOS administrative privilege levels for individual TACACS+ privilege levels were hard-coded.

New Behavior: StarOS administration levels, as well as specific access permissions and restrictions, can be configured for TACACS+ privilege levels and individual user IDs.

Command Changes

priv-lvl

This new TACACS+ Configuration mode command configures authorized StarOS privileges for a specified TACACS+ privilege level.

configure
tacas mode
  priv-lvl lvl_number authorization-level { administrator | inspector | operator | security-admin }
cli | ecs | ftp | li-administration | nocli | noecs | noftp | nocli-administration | end

Notes:

• *lvl_number* specifies the TACACS+ priv-level as an integer from 1 through 15.

• *authorization-level* specifies the StarOS administrative authorization level for this privilege level.
  * administrator – Allows user to execute Administrator level configuration commands.
  * inspector – Allows user to execute Inspector commands.
  * operator – Allows user to execute Operator commands.
  * security-admin – Allows user to execute Security Administrator commands.

• Optional permission and restrictions can also be associated with this TACACS+ priv-level.
  * cli – Permits access to the StarOS command line interface.
  * ecs – Permits access to Enhanced Charging Services (ECS) commands.
  * ftp – Permits of File Transfer Protocol (FTP).
  * li-administration – Permits access to Lawful Intercept (LI) administrative commands.
  * nocli – Denies access to the StarOS CLI.
  * noecs – Denies access to ECS commands
  * noftp – Denies use of FTP.
  * nocli-administration – Denies access to StarOS Administrator and Security Administrator commands.

For detailed information about StarOS administration levels, refer to the System Settings chapter of the System Administration Guide.

user-id

This new TACACS+ Configuration mode command configures additional profile attributes for a specific TACACS+ user identifier.

configure
tacacs mode
   user-id *tacacs_userid* | li-admin | noli-admin |
end

Notes:

• *tacacs_userid* identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

• li-admin grants access to Lawful Intercept (LI) administrative commands.

• noli-admin denies access to LI administrative commands.
Performance Indicator Changes

show tacacs priv-lvl

The show tacacs command has been modified to include a new priv-lvl keyword. This keyword displays TACACS+ priv-level authorization attributes.

CSCus11708 - L2TP support with Demux on MIO

Applicable Products: All products that support L2TP on an ASR 5500 MIO

Feature Changes

L2TP Support with Demux on MIO (ASR 5500)

Previous Behavior: The StarOS CLI did not allow L2TP Access Concentrator (LAC) service to be configured if Demux MIO was enabled. It returned an error.

New Behavior: If Demux MIO is configured, LAC service can be successfully configured via the StarOS CLI.

CSCut57399 - Output pkts stats post recovery/switchover

Applicable Products: SAE-GW in an ICSR configuration

Feature Changes

Adjusted Packet Counts for Collapsed Calls

Previous Behavior: For collapsed calls, the post recovery/switchover packet count was equal to the total input packets.

New Behavior: For collapsed calls, the post recovery/switchover packet count is now stored as the total packets received minus packets dropped. The resulting packet count is aligned with that of the pre-recovery/switchover (active-standby) count.

CSCuu14795 - [MARS] uDPC2 license not being enforced

Applicable Products: ASR 5500, UDPC2
Feature Changes

Add Support for UDPC2 on ASR 5500 Chassis

The ASR 5500 and StarOS 18.2+ now support the Universal DPCv2 (UDPC2).

A chassis software license that enables universal card support is required when UDPC2s are installed. This license also specifies the maximum number of UDPC2s that can run on the chassis at the same time. Both active and standby UDPC2s are counted against the maximum UDPC/UDPC2 limit.

Important Contact your Cisco account representative for detailed information regarding ASR 5500 license requirements.

For additional information on the UDPC2, refer to the Chassis, UMIO, UDPC and UDPC2 License Requirements appendix in the ASR 5500 Installation Guide.

CSCuu20436 - Increase the number of configurable tacacs server priorities to 4

Applicable Products: All products

Feature Changes

Increase Number of TACACS+ Server Priorities

The number of configurable TACACS+ server priorities has been increased from 3 to 4.

Command Changes

server priority

The TACACS Configuration mode server priority command has been modified to accept up to four priority levels.

configure
tacacs mode
server priority priority_number
end

Notes:

- priority_number can be an integer from 1 (highest priority) to 4 (lowest priority). It corresponds to a configured TACACS+ server.
CSCuu58335 - Unable to retrieve bulkstats server information

Applicable Products: All

Feature Changes

Retry Bulkstat Connection at Configured Transfer Interval

Previous Behavior: When a bulkstat receiver failed to respond, the bulkstat process tried reconnecting with the receiver during every server poll (30-second interval).

New Behavior: The bulkstat process no longer tries to reconnect on every server poll. Instead it will try to reconnect on expiry of the configurable bulkstat transfer-interval. The default transfer interval is 15 minutes. Bulkstat data collection continues during the configured transfer interval on receiver failures.

System and Platform Enhancements for Release 18.1

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.

CSCum24783 - Live Migrate Support

Applicable Products: All

Feature Changes

Traffic Handling During Planned Card Migration

Previous Behavior: During a planned card migration, subscriber handling is suspended during the virtual memory copy of tasks being migrated. Depending on the size of the processes being migrated, traffic handling is impacted for anywhere between a few seconds up to about 25 seconds.

New Behavior: This new live migration feature reduces the traffic outage time during planned card migration. All migrating tasks are allowed to handle incoming packets while their virtual memory is being copied onto the destination card. Once the entire task memory is copied to the destination card, memory pages modified during the memory copy process are iteratively copied until the number of modified pages are small enough to copy in a single memory copy operation.
Live migration limits the outage time to the amount of time taken to copy only the remaining small number of modified memory pages. After the remaining modified pages of memory are copied to the destination card, the destination card starts to serve the incoming traffic.

CSCuo82292 - [ICSR Perf] srp chkpnt stats need to include counters for all chkpnts

**Applicable Products:** All products that support ICSR

### Feature Changes

**SRP Checkpoint Counters**

Statistics for full checkpoints and micro-checkpoints appear in the output of the Exec mode `show srp checkpoint statistics verbose` command. For detailed information, see the *ICSR Schema Statistics* chapter in the *Statistics and Counters Reference*.

A new *ICSR Checkpoints* appendix appears in the *System Administration Guide*. This appendix lists and describes the macro-checkpoints and categories of micro-checkpoints supported by ICSR.

### System and Platform Enhancements for Release 18.0

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.

CSCuj74022 - Support ICSR upgrade/downgrade across N-2 builds

**Applicable Products:** All products that support ICSR

**Related CDETS ID:** CSCup33465 - Support ICSR upgrade/downgrade across N-2 builds

**Important**

Downgrade support is limited to the minimum version of StarOS required to support the type of hardware installed in the chassis. For example, the ASR 5500 DPC2 requires release 18.0+. If you downgrade to any previous version of StarOS, the DPC2s will not boot.
Feature Changes

ICSR Support for Upgrade and Downgrade Across Two StarOS Releases

ICSR been qualified to support upgrade and downgrade across the current release (N) and up to two prior releases (N-2). The table below lists the CDETS IDs associated with identifying and fixing any application issues.

Table 1: CSCuj74022 Associated Issues

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup32368</td>
<td>Diameter</td>
</tr>
<tr>
<td>CSCup33427</td>
<td>AAA (Authentication, Authorization and Accounting)</td>
</tr>
<tr>
<td>CSCup33471</td>
<td>S-GW (Serving Gateway)</td>
</tr>
<tr>
<td>CSCup33478</td>
<td>ePDG (evolved Packet Data Gateway)</td>
</tr>
<tr>
<td>CSCup33492</td>
<td>eHRPD (evolved High Rate Packet Data Gateway)</td>
</tr>
<tr>
<td>CSCup36033</td>
<td>ECSv2 (Enhanced Charging Services version 2)</td>
</tr>
</tbody>
</table>

CSCum70938 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure

Applicable Products: ICSR for P-GW
Related CDETS ID: CSCum70938 - VoLTE-ICSR-SR:IMS Sessions hung after SR failure

Feature Changes

Graceful Cleanup of ICSR After Audit of Failed Calls

Previous Behavior: During an Audit on the gateways (P-GW/S-GW/GGSN/SAE-GW) after Session Recovery or an ICSR event, if any critical information, internally or externally related to a subscriber session seems inconsistent, ICSR will locally purge the associated session information.

Since external gateways (peer nodes) are unaware of the purging of this session, the UE session may be maintained at other nodes. This leads to unnecessary hogging of resources external to the gateway and an unreachable UE for VoLTE calls.

New Behavior: When this feature is enabled, graceful cleanup for an ICSR audit of failed calls occurs. External signaling notifies peers of session termination before purging the session. The gateway will attempt to notify external peers of the removal of the session. External nodes to the local gateway include: S-GW, P-GW, SGSN, MME, AAA, PCRF and IMSA.

Audit failure can occur because of missing or incomplete session information. Therefore, only the peers for which the information is available will be notified.

Customer Impact: External signaling will be sent towards the peers while deleting the subscribers.
Command Changes

require graceful-cleanup-during-audit-failure

This new Global Configuration mode CLI command enables or disables the graceful cleanup feature.

configure
    require graceful-cleanup-during-audit-failure | del-cause non-ims-apn \ { system-failure | none } \]

Notes:

• For P-GW del-cause specifies the Cause Code to be sent in the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

• non-ims-apn specifies the Cause Code to be sent in the Delete Bearer Request from the P-GW resulting from the graceful cleanup for Audit Failure. By default the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

  ° The none option omits the GTP Cause IE from the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

  ° The system-failure option sends the GTP Cause Code SYSTEM FAILURE.

Performance Indicator Changes

System Schema

The following new session statistic has been added to the system schema:

• disc-reason-586

show srp checkpoint statistics

The output of this command has been modified to display call drop counts due to ICSR audit failures:

• Graceful call drops during audit failure

show session disconnect-reasons

The output of this command has been modified to display call drop counts due to ICSR audit failures:

• graceful-cleanup-on-audit-fail(586)

CSCum84097 - Enhance messenger vector call internal APIs

Applicable Products: All
Feature Changes

Replace Existing Message Vector API

Replace the implementation of the vector message API with one that is more streamlined. The new algorithm performs as follows:

1. Ask the name service to build a list of destinations to which to send the message based on the target facility ID.
2. Create a canonical message handle that is the basis for sending each message.
3. Send a message to each CPU and wait for a response.
4. When a response is received, process it and then send another message to that same CPU.

CSCum92365 - ICSR:SRP link DSCP marking

**Applicable Products:** All products that support ICSR

**Related CDETS IDs:** CSCup43759 - DSCP Marking for SRP messages, CSCup72708 - Configuration Option for DSCP Marking for DNS Application, and CSCuh88268 - [PGW] SRP link DSCP marking

Feature Changes

DSCP Marking of SRP Messages

A new CLI command now supports separate DSCP marking of SRP control and checkpoint messages

Command Changes

dscp-marking

This new Context Configuration mode command sets DSCP marking values for SRP control and checkpoint (session maintenance) messages.

configure
  context context_name
    service-redundancy-protocol
      dscp-marking { control | session } dscp_value
  end

Notes:

- *dscp_value* can be:
  - *af11* – Assured Forwarding Class 1 low drop PHB (Per Hop Behavior)
  - *af12* – Assured Forwarding Class 1 medium drop PHB
  - *af13* – Assured Forwarding Class 1 high drop PHB
  - *af21* – Assured Forwarding Class 2 low drop PHB
* af22 – Assured Forwarding Class 2 medium drop PHB
* af23 – Assured Forwarding Class 2 high drop PHB
* af31 – Assured Forwarding Class 3 low drop PHB
* af32 – Assured Forwarding Class 3 medium drop PHB
* af33 – Assured Forwarding Class 3 high drop PHB
* af41 – Assured Forwarding Class 4 low drop PHB
* af42 – Assured Forwarding Class 4 medium drop PHB
* af43 – Assured Forwarding Class 4 high drop PHB
* be – Best effort Per-Hop-Behaviour (default)
* cs1 – Class selector 1 PHB
* cs2 – Class selector 2 PHB
* cs3 – Class selector 3 PHB
* cs4 – Class selector 4 PHB
* cs5 – Class selector 5 PHB
* cs6 – Class selector 6 PHB
* cs7 – Class selector 7 PHB
* ef – Expedited Forwarding PHB, for low latency traffic

---

**Important**

If *dscp_value* is set incorrectly, packet drops may occur in intermediate devices.

---

**Performance Indicator Changes**

**show srp info**

The following fields have been added to the output of the *show srp info* command:

- DSCP Markings:
  - Control *dscp_value*
  - Session *dscp_value*

---

CSCun88539 - [ePDG] Memory optimization for ePDG sessmgr component

**Applicable Products:** ePDG
Feature Changes

Memory Optimization for ePDG Sessmgr

Code changes have been made to internal memory structure (alignment of fields to avoid padding) for the ePDG (evolved Packet Data Gateway). These changes have reduced the amount of permanent and transient memory used per call.

CSCuo72680 - ICSR IDLE Stats checkpointing issue

Applicable Products: All products supporting ICSR
Related CDETs IDs: CSCup17404 - ICSR IDLE Secs checkpointing optimization, and CSCup82477 - [SGW]: ICSR IDLE Secs checkpointing optimization

Feature Changes

Stop Sending Idlesecs Micro-checkpoint

Previous Behavior: The idlesecs micro-checkpoint was sent from the active ICSR chassis every 30 seconds for active calls, and at 30-second and 60-second intervals for an idle call.

New Behavior: By default idlesecs micro-checkpoints will not be sent from the ICSR framework.
The idleseconds micro-checkpoint periodicity can be controlled via CLI commands from individual gateways. Refer to CSCup17404 (P-GW) and CSCup82477 (S-GW) in appropriate chapters of this document.

CSCuo72783 - VoLTE-ICSR: Starting the audit in pending active state

Applicable Products: All products supporting ICSR

Important: This feature requires an updated ICSR license to support this enhancement. Contact your Cisco account representative for additional information.

Feature Changes

Optimization of Switchover Control Outage Time

Changes have been made to the ICSR framework to reduce control outage time associated with flushing of critical full checkpoint statistics, network convenience and internal auditing.
The amount of time consumed by the following activities affects control outage time during switchover:

• Critical Flush – During the Active to Pending-Standby transition, all sessmgers flush any pending critical FCs (Full Checkpoints). During this time, the active chassis drops all control packets. If control signaling
is allowed during this stage, a call may get disconnected based on the control message type and accounting information will be lost.

- **Network Convergence** – This encompasses the amount of time taken to update routes and send control/data to the newly active chassis. Control messages are dropped during the transition.

- **Accounting Flush** – During this flush stage data counts are synchronized between chassis. If control signaling is allowed during this flush, the call may get disconnected based on the control message type and accounting information will be lost for calls that existed before switchover.

- **Audit** – During audit new calls are not allowed because synchronization of call resources may result in clearing of the calls.

A new CLI command allows new calls during the Accounting Flush, as soon as the Audit is completed.

### Command Changes

```
switchover control-outage-optimization
```

This new SRP Configuration mode command enables the quicker restoration of control traffic (call-setup, modification, deletion) following an ICSR switchover.

```
configure
    context context_name
    service-redundancy-protocol
    switchover control-outage-optimization
end
```

### CSCuo91183 - Finish config versioning support for services

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

### Feature Changes

**Service Reconciliation Optimization for S-GW and P-GW Services**

Complete internal code changes for optimizing session controller performance for both services.

### CSCup29785 - Show command enhancements

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

**Related CDETS ID:** CSCup56949 - Show command enhancements and CSCup03551 - [SGw] Show command enhancements
Feature Changes

Enhancements to show session Commands and Bulkstats

The output of show session commands now categorizes call events by access technologies:

- 2G (GERAN, GPRS) calls [GGSN, P-GW/S-GW and S4 SGSN]
- 3G (UTRAN, UMTS) calls [GGSN, P-GW/S-GW and S4 SGSN]
- 4G (EUTRAN, LTE) calls [P-GW, S-GW]
- eHRPD (evolved High Rate Packet Data) calls
- Wireless LAN (WiFi) calls [P-GW, CGW]

System bulkstats now include session data tracked by access technology for the above call types.

Performance Indicator Changes

System Schema

The following new session statistics have been added to the system schema:

- sess-num-calls-rejected-umts
- sess-num-calls-failed-umts
- sess-num-handoffs-umts
- sess-num-renewals-umts
- sess-num-callops-umts
- sess-num-calls-rejected-gprs
- sess-num-calls-failed-gprs
- sess-num-handoffs-gprs
- sess-num-renewals-gprs
- sess-num-callops-gprs
- sess-num-calls-rejected-ehrpd
- sess-num-calls-failed-ehrpd
- sess-num-handoffs-ehrpd
- sess-num-renewals-ehrpd
- sess-num-callops-ehrpd
- sess-num-calls-failed-lte
- sess-num-calls-rejected-lte
- sess-num-handoffs-lte
show session counters historical

This command has been modified to support the following new keywords for filtering output by access technologies:

- **all** – display counters for all access technology types
- **2g** – display counters for 2G (GERAN, GRPS) access technology
- **3g** – display counters for 3G (UTRAN, UMTS) access technology
- **4g** – display counters for 4G (EUTRAN, LTE) access technology
- **eHRPD** – display counters only for eHRPD access technology
- **wifi** – display counters only for Wireless LAN access technology

When an access technology filter is specified, the output of this command separates session counters by category.

show session summary

This new command displays session types by access technology categories. The following information appears in the output of this command:

- 4G LTE (EUTRAN)
- 2G (GERAN)
- 3G (UTRAN)
- WiFi (WIRELESS LAN)
• eHRPD
• Others
• Total sessions
• Active
• Dormant
• psdn-simple-ipv4
• psdn-simple-ipv6
• psdn-mobile-ip
• ha-mobile-ipv6
• hsgw-ipv6
• hsgw-ipv4
• hsgw-ipv4-ipv6
• pgw-pmip-ipv6
• pgw-pmip-ipv4
• pgw-pmip-ipv4-ipv6
• pgw-gtp-ipv6
• pgw-gtp-ipv4
• pgw-gtp-ipv4-ipv6
• sgw-gtp-ipv6
• sgw-gtp-ipv4
• sgw-gtp-ipv4-ipv6
• sgw-pmip-ipv6
• sgw-pmip-ipv4
• sgw-pmip-ipv4-ipv6
• pgw-gtps2b-ipv4
• pgw-gtps2b-ipv6
• pgw-gtps2b-ipv4-ipv6
• mme
• ipsg-rad-snoop
• ipsg-rad-server
• ha-mobile-ip
• ggsn-pdp-type-ppp
• ggsn-pdp-type-ipv4
• Ins-l2tp

**CSCup30816 - ICSR Non VoLTE Outage Improvement**

**Applicable Products:** ICSR on P-GW

**Related CDETS ID:** CSCuo72783 - VoLTE-ICSR: Starting the audit in pending active state

---

**Important**

This feature requires an updated ICSR license to support this enhancement. Contact your Cisco account representative for additional information.

---

**Feature Changes**

**Allow Non-VoLTE Traffic During ICSR Switchover**

**Previous Behavior:** The ICSR framework reduces switchover disruption for VoLTE traffic by enabling VoLTE traffic on the newly active chassis prior to reconciling the billing information and enabling communication with the newly active chassis when accounting is not deemed critical.

**New Behavior:** This functionality has been extended to all other traffic, including data sessions and default bearer traffic for IMS/e911, The following ICSR functionality is provided for all non-VoLTE data traffic:

- When a switchover occurs, the newly active chassis forwards all traffic the moment the chassis becomes active.
- External communication with billing servers is deferred. See Traffic Flow diagram below.
- When the newly active chassis receives all billing-related checkpointing information from the previously active chassis, it reconciles the billing data before communicating with external billing servers (OCS/OFCS).

**Table 2: CSCup30816 Associated CDETS IDs**

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup26449</td>
<td>S-GW (Serving Gateway)</td>
</tr>
<tr>
<td>CSCup26465</td>
<td>ePDG (evolved Packet Data Gateway)</td>
</tr>
<tr>
<td>CSCup33560</td>
<td>ECSv2 (Enhanced Charging Services version 2)</td>
</tr>
<tr>
<td>CSCup33775</td>
<td>NAT (Network Address Translation)</td>
</tr>
</tbody>
</table>
Command Changes

switchover allow-all-data-traffic

This new SRP Configuration mode CLI command allows all data traffic (VoLTE and non-VoLTE) during switchover transition. This command overwrites the `switchover allow-volte-data-traffic` command if enabled on a P-GW.

```configure
context context_name
service-redundancy-protocol
switchover allow-all-data-traffic
end
```

Important: This CLI command must be run on both the active and standby chassis to enable this feature.

switchover allow-volte-data-traffic

This new SRP Configuration mode CLI command allows VoLTE data traffic during ICSR switchover transition.

```configure
context context_name
service-redundancy-protocol
switchover allow-volte-data-traffic [maintain-accounting]
end
```

Notes:
- When `maintain-accounting` is enabled, accounting accuracy is maintained for VoLTE calls. VoLTE data is allowed on the active chassis after VoLTE accounting statistics are flushed.

CSCup47085 - Time slice lport utilization stats collection

**Applicable Products:** ASR 5500

**Related CDETS IDs:** CSCty77635 - CLI for vlan & npu based utilization table, and CSCul75347 - show logical-port utilization table CLI does not work on ASR5500

Feature Changes

**Improved Collection of Logical Port Statistics on ASR 5500**

**Previous Behavior:** Logical port utilization stats were introduced in StarOS Release 16.1. At 60-second intervals, the MNPUMGRs collect stats from each logical port. This collection period can block the npumgr for extended periods of time.

**New Behavior:** This functionality has been reworked as follows:
- By default stats collection on logical port is disabled.
The collection of logical port statistics must be enabled via the Ethernet Interface Configuration mode `logical-port-statistics` CLI command.

- There is a limit of 32 logical ports on which the system can collect the statistics at any given time.
- When enabled statistics are collected on a per minute basis with samples maintained for the last 5 minutes and 15-minute intervals.

**CSCup47715 - Pilot Packet Format and Trigger Update**

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

**Feature Changes**

**Support for Pilot Packet Format and Trigger**

Pilot Packet is a feature which provides key pieces of information about subscriber session to an external element. As part of this enhancement, the current pilot packet format is modified to include additional attributes — Serving network identifier, Foreign agent IP address, NAI, and RAT Type. The Pilot Packet trigger is also enhanced to send a pilot packet when RAT type changes. The new pilot packet attributes and RAT type trigger are configurable.

---

**Important**

The Pilot Packet feature is customer-specific. Contact your Cisco account representative for more information.

---

**Command Changes**

**pilot-packet**

In this release, the `attribute` and `trigger` keywords are added to this command in the Context Configuration mode. The `attribute` keyword configures the optional attributes to be sent in pilot packet. The `trigger` keyword configures triggers for pilot packet. This command must be configured in the destination context.

```plaintext
configure
  context context_name
    pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | trigger rat-change
    generate { nat-info-only | user-info-and-nat-info | user-info-only } }
    [ default | no ] pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | trigger rat-change }
  end
```

---

**Release Change Reference, StarOS Release 18**
Performance Indicator Changes

APN Schema
The following bulk statistics are new in the release:
• rat-change-user-info-pilot-packet-sent-per-apn
• rat-change-nat-info-pilot-packet-sent-per-apn

System Schema
The following bulk statistics are new in the release:
• rat-change-user-info-pilot-packet-sent
• rat-change-nat-info-pilot-packet-sent

show apn statistics name
The following new fields are added to the output of this command:
• RAT-Change-User-Info
• RAT-Change-NAT-Info

show pilot-packet statistics all
The following new fields are added to the output of this command:
• RAT-Change-User-Info
• RAT-Change-NAT-Info

show session subsystem facility sessmgr all
The following new fields are added to the output of this command:
• RAT-Change-User-Info
• RAT-Change-NAT-Info

CSCup56736 - SGW Bearer Duration KPIs
Applicable Products: S-GW
Feature Changes

Session Duration Statistics by QCI

This feature modifies a CLI show command and adds system schema bulkstats that indicate the length of time a dedicated bearer is established on the network. The statistics are available for a specified or all standard and non-standard QCI (QoS Class Index) values.

Performance Indicator Changes

System Schema

The following QCI-related statistics have been added to the system schema:

- sess-prerecord-5sec-qcin
- sess-bearingdur-10sec-qcin
- sess-bearingdur-30sec-qcin
- sess-bearingdur-1min-qcin
- sess-bearingdur-2min-qcin
- sess-bearingdur-5min-qcin
- sess-bearingdur-15min-qcin
- sess-bearingdur-30min-qcin
- sess-bearingdur-1hr-qcin
- sess-bearingdur-4hr-qcin
- sess-bearingdur-12hr-qcin
- sess-bearingdur-24hr-qcin
- sess-bearingdur-over24hr-qcin
- sess-bearingdur-2day-qcin
- sess-bearingdur-4day-qcin
- sess-bearingdur-5day-qcin
- sess-bearingdur-5sec-qci-non-std
- sess-bearingdur-10sec-qci-non-std
- sess-bearingdur-30sec-qci-non-std
- sess-bearingdur-1min-qci-non-std
- sess-bearingdur-2min-qci-non-std
- sess-bearingdur-5min-qci-non-std
- sess-bearingdur-15min-qci-non-std
• sess-bearer-dur-30min-qci-non-std
• sess-bearer-dur-1hr-qci-non-std
• sess-bearer-dur-4hr-qci-non-std
• sess-bearer-dur-12hr-qci-non-std
• sess-bearer-dur-24hr-qci-non-std
• sess-bearer-dur-over24hr-qci-non-std
• sess-bearer-dur-2day-qci-non-std
• sess-bearer-dur-4day-qci-non-std
• sess-bearer-dur-5day-qci-non-std

Notes:
• *n* is a standard QCL value expressed as an integer from 1 through 9.

**show session duration**

The following keywords have been added to the `show session duration` command to display bearer session duration for a specified or all standard and non-standard QCI values:

```plaintext
qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | non-std } *
```

Displays the length of time a dedicated bearer is established on the network for a given QCI. More than one QCI value can be specified.

---

**CSCup66766 - MME support on QvPC-DI**

**Applicable Products:** MME, ASR 5x00

**Feature Changes**

**MMEmgr Linear Scalability**

MME (Mobile Management Entity) is a control-plane only node with significant scaling required on two fronts:

• S1AP/SCTP connections with eNodeBs - tens of thousands

• Millions of UEs

In addition a relatively smaller number of SCTP (SGsAP, SLsAP and SBcAP) and Diameter (S6a, SLs and SLg) connections are required

**Previous Behavior:** All S1AP/SGsAP/SLsAP/SBcAP connections are terminated on the demux ASR 5x00 packet processing card using MMEmgr tasks. This limits the signaling capacity which can be provided by MME.

**New Behavior:** The following changes have been made to enhance the scalability of MMEmgr tasks:
• MMEmgr tasks will be distributed across session packet processing cards (ASR 5000 PSCx or ASR 5500 DPC/DPC2)
• MMEdemux task now resides on the demux packet processing card.
• Number of IMSImgr tasks has been increased. (CSCup66362)
• Diameter proxy scaling has been improved. (CSCup75830)

Table 3: MMEmgrs Tasks - ASR 5x00 Packet Processing Cards

<table>
<thead>
<tr>
<th>Platform</th>
<th>Max. Number of Packet Processing Cards</th>
<th>Max. Number of MMEmgrs per Chassis</th>
<th>MMEmgrs per Packet Processing Card (Default)</th>
<th>MMEmgrs per Packet Processing Card (Allowed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 5000 (PSC2/PSC3)</td>
<td>12</td>
<td>12</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>ASR 5500 (DPC/DPC2)</td>
<td>6</td>
<td>24</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

Command Changes

mmemgr-average-cpu-utilization

This is a new MMEmgr-specific congestion control threshold CLI command.

```
configure
  congestion-control threshold mmemgr-average-cpu-utilization { critical | major | minor }
  [ percent_threshold_value ]
end
```

Notes:

• By default this threshold value is not enabled.
• A default value of 80% is assigned to the critical threshold only.

Performance Indicator Changes

congestion-control configuration

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

• Congestion-control Critical threshold parameters
  * mmemgr average cpu utilization

• Congestion-control Major threshold parameters
  * mmemgr average cpu utilization
• Congestion-control Minor threshold parameters
  * mmemgr average cpu utilization

**CSCup68867 - HeNBGW support on ASR5500**

**Applicable Products:** ASR 5500

**Feature Changes**

**Support for HeNB-GW on ASR 5500**

The HeNB-GW (Home evolved Node B Gateway) has been fully qualified to run on the ASR 5500 platform.

**CSCup71713 - PGW RTT Support for Diameter procedures**

**Applicable Products:** P-GW

**Related CDETS ID:** CSCup71684 – PGW RTT Support for GTP procedures

**Feature Changes**

**P-GW Event Reporting Statistics**

New system schema bulkstats and a `show event-record` CLI command have been added to display APN-associated event records for a P-GW node.

**Important**

PGW RTT Support for GTP and Diameter procedures is a customer-specific feature. Contact your Cisco account representative for more information.

**Command Changes**

`show event-record`

This new command displays event record statistics for a P-GW node.

`show event-record statistics pgw`
Performance Indicator Changes

System Schema

The following bulkstats have been added to the system schema:

- sess-pgw-total-number-event-records
- sess-pgw-total-gtpv2-event-records
- sess-pgw-total-csr-event-records
- sess-pgw-total-cbr-event-records
- sess-pgw-total-dsr-event-records
- sess-pgw-total-dbr-event-records
- sess-pgw-total-mbr-event-records
- sess-pgw-total-ubr-event-records
- aaa-pgw-total-diam-event-records
- aaa-pgw-total-s6b-aar-event-records
- aaa-pgw-total-s6b-rar-event-records
- aaa-pgw-total-s6b-asr-event-records
- aaa-pgw-total-s6b-str-event-records
- sess-pgw-total-gx-ccri-event-records
- sess-pgw-total-gx-ccrt-event-records
- sess-pgw-total-gx-ccru-event-records
- sess-pgw-total-gx-rar-event-records
- sess-pgw-total-gy-ccri-event-records
- sess-pgw-total-gy-ccrt-event-records
- sess-pgw-total-gy-ccru-event-records
- sess-pgw-total-gy-rar-event-records

show event-record statistics pgw

This is a new show CLI command that provides events statistics for the P-GW. The following information appears in the output of this command:

- Total Number of Event Records
- GTPv2 Event Records:
  - CSR
  - CBR
• DSR
• DBR
• MBR
• UBR

• Diameter Event Records
• S6b Procedures:
  • AAR
  • RAR
  • ASR
  • STR

• Gx Procedures:
  • CCR-I
  • CCR-U
  • CCR-T
  • RAR

• Gy Procedures:
  • CCR-I
  • CCR-U
  • CCR-T
  • RAR

CSCup75830 - DPC2: Diam proxy scaling

Applicable Products: ASR 5500, DPC2

Feature Changes

Enhance Diameter Proxy Pool to Handle a Higher Number of Transactions

The existing Global Configuration mode require diameter-proxy CLI command has been enhanced to allow multiple diamproxies-per-card and specify the proxy selection algorithm type in the ASR 5500.
Command Changes

**require diameter-proxy**

This command has been enhanced to allow multiple diameter proxies per card with a specified proxy selection algorithm.

```plaintext
configure
require diameter-proxy multiple diamproxy-per-card {1|2|3} [ algorithm { facility | round-robin } ]
end
```

Notes:

- The **facility** keyword selects an algorithm in which all AAA endpoints would be present in CPU 0 and Round-Robin algorithm would be used to allocate CPU for sessmgr endpoints. For example, if the number of proclets running per card is 3, AAA endpoints would always be associated with CPU 0, each sessmgr endpoint would be associated either CPU 1 or CPU 2 based on the order in which it is received.

- The **round-robin** keyword selects an algorithm in which the endpoints would be chosen in the Round-Robin manner. The facility type would not be considered while associating the CPU with the endpoint name. For example, if the number of proclets running per card is 2, the first endpoint configured would be associated with CPU 0 (the proxy running in CPU 0 of the same card) and the next endpoint configured would be associated with CPU 1. The third one with CPU 0 and fourth one with CPU1.

**logging filter active facility proclet-map-frmk**

A new logging facility has been added to track the proclet mapping framework.

```plaintext
logging filter active facility proclet-map-frwk level { critical | error | warning | unusual | info | trace | debug }
```

Performance Indicator Changes

**show diameter proclet-map-memcache**

This new **show** command displays the DIAMPROXY cached memory table for aamgr, diactrl or sessmgr.

```plaintext
show diameter proclet-map-memcache { aamgr integer | diactrl | sessmgr integer }
```

**show diameter proclet-map-table**

This new **show** command displays the DIAMPROXY map table for aamgr, diactrl or sessmgr.

```plaintext
show diameter proclet-map-table { aamgr integer | diactrl | sessmgr integer }
```

CSCup82065 - Abnormal bearer termination info in CDR

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

**Related CDETS ID:** CSCup88929
Feature Changes

New Disconnect Reasons for GTP Path Failures

**Previous Behavior:** For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls previously, for GTPC/GTPU path failure disconnect-reason of path-failure was used.

For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls for GTPU error indication with local-purge configuration local-disconnect was used.

**New Behavior:** For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls new disconnect reasons have been added containing interface information for GTPC/GTPU path failure.

For S-GW/SAEGW(Pure S)/SAEGW(Co-located) calls new disconnect reasons have been added containing interface information for GTPU error indication with local-purge configuration.

New abnormal termination CDR enum values have also been added in an SGW-CDR as part of the network specific diagnostic field in custom34 and custom35 dictionaries. A new field has also been added in SGW-CDR for CDR closure cause abnormal release. Presence of the new field in CDR is controlled by a new CLI in GTPP group.

Performance Indicator Changes

**System Schema**

The following disconnect reasons have been added to the system schema:

- disc-reason-590
- disc-reason-591
- disc-reason-592
- disc-reason-593
- disc-reason-594
- disc-reason-595
- disc-reason-596
- disc-reason-597
- disc-reason-598
- disc-reason-599
- disc-reason-600

**show session disconnect-reasons**

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

- path-failure-s5(590)
- path-failure-s11(591)
CSCup91391 - ICSR requirement in 18.0

Applicable Products: P-GW ICSR

Feature Changes

Planned Outage Time Within 3 Seconds

The ICSR switchover time for a planned outage shall be within three seconds. An unplanned outage where detection-time of outage + the switchover time (ICSR + network convergence) will also be enhanced with the associated improvements for this feature.

The outage events encompassed by this feature include:

- **P-GW VoLTE (8M sessions)**
  - Data traffic for VoLTE calls
  - Control traffic for VoLTE calls
  - New VoLTE calls
  - New PDN activation
  - GTO echo responses

- **P-GW Enterprise (200K sessions)**
  - Data traffic for non-VoLTE calls
  - Control traffic for non-VoLTE calls
  - New PDN activation
  - GTO echo responses

The table below lists the CDETS IDs that were addressed as part of this feature.
Table 4: CSCup91391 Associated CDTS IDs

<table>
<thead>
<tr>
<th>CDTS ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCum46820</td>
<td>diet demux support for SGW-SM</td>
</tr>
<tr>
<td>CSCuo72701</td>
<td>VoLTE-ICSR: Max messages in a buffer for ICSR</td>
</tr>
<tr>
<td>CSCuo72738</td>
<td>VoLTE-ICSR: GTPC Flow preinstallation</td>
</tr>
<tr>
<td>CSCuo72752</td>
<td>VoLTE-ICSR: Flush time reduction by using IDLE timeout</td>
</tr>
<tr>
<td>CSCuo72783</td>
<td>VoLTE-ICSR: Starting the audit in pending active state</td>
</tr>
<tr>
<td>CSCuo94491</td>
<td>NPUMGR audit optimisation for DPC/DPC2</td>
</tr>
<tr>
<td>CSCup30816</td>
<td>ICSR Non VoLTE Outage Improvement</td>
</tr>
<tr>
<td>CSCup77266</td>
<td>ICSR Control Outage: Radius connectivity establishment</td>
</tr>
<tr>
<td>CSCup78123</td>
<td>ICSR: Stats to measure the audit for each subcomponent</td>
</tr>
<tr>
<td>CSCuq46565</td>
<td>Enhancement of npuregr test framework to test audit optimisation.</td>
</tr>
<tr>
<td>CSCur19185</td>
<td>npumgr crash during icsr switchover in audit</td>
</tr>
</tbody>
</table>

CSCuq10869 - ICSR: VoLTE ICSR Bulkstats Support

Applicable Products: All products that support ICSR

Feature Changes

New VoLTE ICSR Statistics

Additional VoLTE-ICSR statistics have been added to the bulkstats ICSR schema and the output of the `show srp call-loss statistics` command.

Performance Indicator Changes

ICSR Schema

The following statistics have been added to the ICSR schema:

- total-num-volte-cap-subs
- total-num-sub-engaged-voice-call

show srp call-loss statistics

The output of this command has been modified to include the following data fields:
• Total number of VoLTE capable subscribers
• Total number of subscribers engaged in voice calls

CSCuq13372 - Reassembly packet distribution to multiple npusims

Applicable Products: ASR 5500

Feature Changes

Distribution of Reassembly Packets to Multiple npusims

Previous Behavior: Currently ASR 5500 NPUs send IP fragments to npusim for reassembly. Exceptions for which NPUs send fragments to npusim for reassembly include:

• Number of fragments are more than three
• Delay between fragments exceeds a predefined threshold

These fragments are sent only to the last instance of npusim. During high loads of fragmented packets, a single instance of npusim cannot scale.

New Behavior: NPU logic has been changed logic to distribute the fragments uniformly across all npusim instances.

CSCuq59705 - Add support for DPC2 HW on ASR-5500 Chassis

Applicable Products: ASR 5500

Feature Changes

Support for New DPC2

The DPC2 is the second generation Data Processing Card (DPC) for the ASR5500. It offers increased performance versus the first generation DPC, while maintaining backwards compatibility with other ASR 5500 cards. The raw input/output has been increased from 80Gbps (DPC/UDPC) to 150Gbps (DPC2).

The DPC2 has three CPU subsystems. Each subsystem consists of two CPUs that are paired with a Platform Controller Hub (PCH). Each CPU is associated with 32 GB of DDR4 memory (total of 192 GB per DPC2) and a latest generation crypto offload engine.

The DPC2 is equipped with the Cisco Anti-Counterfeit Technology 2 (ACT2) chip. The ACT2 services multiple functions including:

• IEEE 802.1AR standard based Immutable Identity
• Extensible set of cryptographic functions
• Secure storage capabilities (cryptographic keys and credential storage).
• Installation of customers’ own identity certificates (802.1AR LDevID)
• Source for true random entropy (NIST SP-800-90 certifiable)

The DPC2 is not equipped with NPUs.

**Important**

The DPC2 must not be intermixed with the DPC in an ASR 5500 chassis.

The table below identifies CDETS IDs associated with the development and release of the DPC2.

### Table 5: DPC2 Associated Features and Functions

<table>
<thead>
<tr>
<th>CDETS ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup06677</td>
<td>Optimization of sessmgr_callline_tC</td>
</tr>
<tr>
<td>CSCul41333</td>
<td>DPC2: Session Audit Removal from demuxmgr</td>
</tr>
<tr>
<td>CSCum42002</td>
<td>Memory optimization for sessmgr</td>
</tr>
<tr>
<td>CSCum46820</td>
<td>Demux support for SGW-SM</td>
</tr>
<tr>
<td>CSCum84097</td>
<td>Enhance messenger vector call internal APIs</td>
</tr>
<tr>
<td>CSCuo41734</td>
<td>ECS Tethering Detection for DPC2 memory (R18)</td>
</tr>
<tr>
<td>CSCuo72738</td>
<td>VoLTE-ICSR.GTPC FLow preinstallation</td>
</tr>
<tr>
<td>CSCuo78758</td>
<td>DPC2 related changes in egtpc stack</td>
</tr>
<tr>
<td>CSCuo93323</td>
<td>DPC2 Scaling: Create Per CPU complex MsgProxy for relaying broadcast msg</td>
</tr>
<tr>
<td>CSCup30923</td>
<td>VoLTE-ICSR: DPC2: ICSR Framework changes due to DPC2</td>
</tr>
<tr>
<td>CSCup44382</td>
<td>DPC2: Session Audit Removal from demuxmgr - PGW_SM</td>
</tr>
<tr>
<td>CSCup44422</td>
<td>DPC2: Session Audit Removal from demuxmgr ePDG</td>
</tr>
<tr>
<td>CSCup47534</td>
<td>DPC2: GTPU manager, memory + session reconciliation optimization</td>
</tr>
<tr>
<td>CSCup53989</td>
<td>ECS modifications/optimizations for DPC2</td>
</tr>
<tr>
<td>CSCup73211</td>
<td>DPC2: Use of messenger proxy in the demux/gtpc stack</td>
</tr>
<tr>
<td>CSCup73230</td>
<td>DPC2: egtpc stack, memory optimization</td>
</tr>
<tr>
<td>CSCup75830</td>
<td>DPC2: Diam proxy scaling</td>
</tr>
<tr>
<td>CSCup86057</td>
<td>SGW DPC2 Related Changes</td>
</tr>
<tr>
<td>CSCup86711</td>
<td>SM changes for Bulkstats design Improvement (pgw, saegw &amp; ggsn schema)</td>
</tr>
<tr>
<td>CSCup86720</td>
<td>ACL related optimisations at SessMgr</td>
</tr>
<tr>
<td>CSCup86730</td>
<td>IP Pool Optimizations specific to both VPNMgr and SessMgr</td>
</tr>
<tr>
<td>CSCup95956</td>
<td>DPC2: AAA Proxy/AAA Mgr scaling</td>
</tr>
<tr>
<td>CSCuq07202</td>
<td>DPC2: CoA/DM from non-admin AAAMgr should send msg to messenger proxy</td>
</tr>
<tr>
<td>CSCuq10888</td>
<td>DPC2: GTPU manager, memory + session reconciliation optimization</td>
</tr>
<tr>
<td>CDETS ID</td>
<td>Headline</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuq16045</td>
<td>Vpnmgr pool optimization changes for dpc2</td>
</tr>
<tr>
<td>CSCuq16050</td>
<td>VPNMGR changes to support Sessmgr side Pool changes</td>
</tr>
<tr>
<td>CSCuq17746</td>
<td>Scale the number of Session/AAA Managers on DPC2</td>
</tr>
<tr>
<td>CSCuq42298</td>
<td>Upgrade the DDF2 FPGA to version 15</td>
</tr>
<tr>
<td>CSCuq38074</td>
<td>NPU sessmgr flowid range scaling for DPC2</td>
</tr>
<tr>
<td>CSCuq59727</td>
<td>Support PGW on DPC2 HW</td>
</tr>
<tr>
<td>CSCuq59733</td>
<td>Support SGW on DPC2 HW</td>
</tr>
<tr>
<td>CSCuq59735</td>
<td>Support SAE-GW on DPC2 HW</td>
</tr>
<tr>
<td>CSCuq59741</td>
<td>Support GGSN on DPC2 HW</td>
</tr>
<tr>
<td>CSCuq59748</td>
<td>Support Consumer-XGW (PGW, GGSN, HA) on DPC2 HW</td>
</tr>
<tr>
<td>CSCuq59760</td>
<td>DPC2: IP address allocation related optimizations</td>
</tr>
<tr>
<td>CSCuq65471</td>
<td>Remove protocol_username and protocol_password</td>
</tr>
<tr>
<td>CSCuq65822</td>
<td>Configure DPC2 Arad PCIe serdes parameters</td>
</tr>
<tr>
<td>CSCuq67662</td>
<td>Incorporate support for TAM/ACT2 chip for diagnostics</td>
</tr>
<tr>
<td>CSCuq96611</td>
<td>Inventory script changes needed to support DPC2</td>
</tr>
<tr>
<td>CSCur16220</td>
<td>Serpentine traffic distribution on DPC2</td>
</tr>
<tr>
<td>CSCur19167</td>
<td>Bulkstats Improvement - using msg proxy for System APIs</td>
</tr>
<tr>
<td>CSCur34177</td>
<td>Update the Register Overrides</td>
</tr>
<tr>
<td>CSCur62858</td>
<td>Fix ingress/egress commands</td>
</tr>
</tbody>
</table>

For additional information on the DPC2, refer to the ASR 5500 Installation Guide.

**CSCuq59763 - Per member link BFD Support for LAG bundles**

**Applicable Products:** ASR 5000 and ASR 5500

**Related CDETS ID:** CSCur53463 - Factor micro-BFD dist exclude status into lag switchover calc and CSCur07640 - Ares: Micro BFD. Add cli commands to configure lag-peers in bfd.

**Feature Changes**

**BFD Support for Link Aggregation Member Links**

Member-link based BFD detects individual link failures faster than LACP and reduces the overall session/traffic down period as a result of single member link failure.
A new CLI command configures BFD interactions with the linkagg task. Once a session is configured, BFD creates per member link BFD sessions and starts sending packets on each of the linkagg member links. If a member link BFD session fails, StarOS notifies failures to the linkagg task.

If you define a linkagg-peer using a slot number, you may configure a linkagg-peer for redundant slot which must also specify a slot. Likewise, if you configure a linkagg-peer without a slot, you must delete it before configuring a peer with a slot specified.

**Important**

Only one IPv4 or IPv6 BFD session-based configuration is allowed per linkagg interface for compliance with RFC 7130.

### Command Changes

**bfd linkagg-peer**

This new BFD Configuration mode command enables member-link BFD and configures the BFD link aggregation (linkagg) session values [RFC 7130].

```bash
configure
  context context_name
    bfd-protocol
      bfd linkagg-peer linkagg_group_id local-endpt-addr local-endpt_ipaddress remote-endpt-addr remote_endpt_ipaddress interval tx_interval min_rx rx_interval multiplier multiplier_value [ slot slot_number ]
      no bfd linkagg-peer linkagg_group_id [ slot slot_number ]
end
```

Notes:

- **linkagg_group_id** specifies the LAG number as an integer from 1 through 255.
- **local-endpt-addr local-endpt_ipaddress** specifies the source address of the multihop BFD session in IPv4 or IPv6 notation.
- **remote-endpt-addr remote-endpt_ipaddress** specifies the remote address of the multihop BFD session in IPv4 or IPv6 notation.
- **interval tx_interval** specifies the transmit interval of control packets in milliseconds as an integer from 50 through 10000.
- **min_rx rx_interval** specifies the receive interval of control packets in milliseconds as an integer from 50 through 10000.
- **multiplier multiplier_value** specifies the value used to compute hold-down time as an integer from 3 through 50.
- **slot slot_number** for redundant active-standby link aggregation, this option specifies the card for which this configuration is intended.

---

**CSCur08278 - SNMP5.7.2 is broken due to CSCur05830: RFC1908 section 3.1.2**

**Applicable Products:** All
Feature Changes

Support for SNMPv1 to SNMPv2 Trap PDU

Previous Behavior: SNMPv2 trap support requires the insertion of an extra zero in the trap PDU (RFC 1908, section 3.1.2). The requirement was not supported because Cisco Prime Network did not support the extra zero.

New Behavior: A new CLI command enables the insertion of the extra zero in the trap PDU.

Command Changes

snmp trap-pdu-v1tov2

This new Global Configuration mode command enables the insertion of an extra zero in the outgoing trap PDU for compliance with SNMPv2. By default, the extra zero is not inserted.

configure
snmp trap-pdu-v1tov2

CSCur19167 - Bulkstats Improvement - using msg proxy for System APIs

Applicable Products: All products

Feature Changes

Bulkstats Performance Improvement

To improve performance, bulkstats now use new message proxy APIs to gather statistics.

CSCur34253 - Reduce time to detect MIO failure subsequent to kernel panic.

Applicable Products: ASR 5500

Feature Changes

Reduce Restart Time for MIO Failure

Previous Behavior: Currently, when an MIO fails due to a kernel panic, the kernel panic function shuts down all other CPU cores and then idles. The other MIO detects failure via a HAT (High Availability Task) heartbeat timeout, resets the failed MIO, and, if the failed card is Active, initiates an MIO switchover.

The HAT heartbeat timeout detection period is 3-4 seconds, which is too long. StarOS must reconverge LAG and reprogram NPU tables in sufficient time for Layer 3 BFD sessions configured at 300ms x 3 detection
intervals to survive. In the MIO switchover case, LAG cannot be reconverged until MIO switchover is initiated and lagmgr transition from secondary to primary is triggered.

**New Behavior:** A restart is immediately initiated if the card type is MIO.

### CSCur53463 - Factor micro-BFD dist exclude status into lag switchover calc

**Applicable Products:** ASR 5000 and ASR 5500  
**Related CDETS ID:** CSCuq59763 - Per member link BFD Support for LAG bundles, and CSCur09301 - [Ares]: Micro BFD core npumgr support

**Feature Changes**

**Exclude BFD Member-Link Port Bandwidth from Aggregator Calculation**

When selecting the active aggregator, lagmgr sums up the bandwidth from each port and switches the LAG to the side with the most available bandwidth. When member-link BFD is enabled the bandwidth calculation discounts ports that are excluded from distribution.

### CSCus04073 - Update support for Russian Timezones

**Applicable Products:** All  
**Related CDETS ID:** CSCuq90891 - Russia timezone update

**Feature Changes**

**Correction for Russian Timezone 1**

When the new Russian timezones were supported in Release 17.1, "RTZ 1" also appeared in the europe-eastern (GMT+2:00) timezone. Russian Timezone 1 does not support Daylight Savings Time, as do the other countries in europe-eastern (GMT+2:00). Therefore, "(RTZ 1)" has been removed from the europe-eastern timezone.
CSCu94073 - Update support for Russian Timezones
VPC-DI Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from VPC-DI in StarOS 18 software releases.

Important

With this release the product name has changed From QvPC-DI to VPC-DI (Virtual Packetized Core-Distributed Instances).

• VPC-DI Feature Changes for 18.2, page 433

VPC-DI Feature Changes for 18.2

This section identifies all of the VPC-DI enhancements included in this release:

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

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

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

Important

For more information regarding features in this section, refer to the VPC-DI System Administration Guide for this release.

CSCue09140 - StarOS Mgmt Interface VLAN

Applicable Products: VPC-DI, VPC-SI
Feature Changes

VLAN Support on Management Interfaces

The VPC management interface now supports VLAN configuration. This support extends to the local context. Bulkstats can be sent out an interface other than the normal management interface. This interface also supports VLANs.

You can also configure other OA&M services on separate VLANs.

You can assign separate source IP addresses for the OA&M services. OA&M services should not be bound to the same VLAN as service VLANs. Other services include SGi, Gi, Pi, eGTP or other packet core specific interfaces and services.

Currently ACL support, the `vlan priority` value and `vlan-map interface if_name context_name` commands are not available for management VLANs.

Command Changes

`vlan`

This feature is implemented by adding support for the `vlan` command to the management port in the local context. See the example command sequence below.

```
configure
  port ethernet 1/1
  vlan 184
  bind interface 19/3-UHA foo
end
```

CSCuo97621 - DI: planned CF switch new standby can't boot from new active - no eth0

Applicable Products: VPC-DI

Feature Changes

Boot from Newly Active CF Upon Switchover

Previous Behavior: Old Active (now Standby) CF booted from local image. If the newly Active CF has a different boot image, the Standby CF will be out of synchronization.

New Behavior: Old Active (now Standby) CF now boots from the newly Active CF.
CSCup36001 - [ePDG] IPSec Support on VPC - DI

Applicable Products: ePDG on QvPC-DI
Related CDETS ID: CSCum64947 - [ePDG] - ePDG service support on SSI

Feature Changes

ePDG Support on VPC-DI

VPC-DI now supports IPSec functionality on an ePDG (evolved Packet Data Gateway).

CSCup36063 - [ePDG] IPSec Scale - Performance Improvement in SSI

Applicable Products: IPSec, VPC-DI

Feature Changes

Increased ESP Packet Processing Performance

OpenSSL will now be used to process ESP (Encapsulating Security Payload) packets instead of SSH crypto routines. OpenSSL crypto routines only support ESP packet authentication and encryption functionalities with the AES-GCM algorithm in the IPSec framework.

Command Changes

encryption

Additional keywords have been added to the encryption command in the IPSec Transform Set Configuration mode. These keywords add support for AEAD (Authenticated-Encryption with Associated-Data) algorithms available through OpenSSL.

```
configure
  context context_name
  ipsec transform-set set_name
    encryption { 3des-cbc | aes-128-gcm-128 | aes-cbc-128 | aes-128-gcm-64 | aes-128-gcm-96 |
               aes-256-gcm-128 | aes-256-gcm-64 | aes-256-gcm-96 | aes-cbc-256 | des-cbc | null }
  end
```

Notes:

- **aes-128-gcm-128** = IKEv2 Child Security Association IPSec ESP Algorithm is AES-GCM-128 with 128-bit ICV (Integrity Check Value). HMAC algorithm with this encryption algorithm should be **none**.
- **aes-128-gcm-64** = IKEv2 Child SA (Security Association) IPSec ESP Algorithm is AES-GCM-128 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be **none**.
• **aes-128-gcm-96** = IKEv2 Child SA IPSec ESP Algorithm to be AES-GCM-128 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be **none**.

• **aes-256-gcm-128** = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 128-bit ICV. HMAC algorithm with this encryption algorithm should be **none**.

• **aes-256-gcm-64** = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be **none**.

• **aes-256-gcm-96** = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be **none**.

**hmac**

The **none** keyword has been added to the **hmac** command in the IPSec Transform Set Configuration mode. This keyword must be used in conjunction with the AEAD algorithms described above.

```bash
configure
  context context_name
    ipsec transform-set set_name
      hmac { aes-xcbc-96 | md5-96 | none | null | sha1-96 }
  end
```

**Notes:**

• The **none** option is only used only with combined mode encryption algorithms such as AES-GCM.

CSCup66766 - MME support on VPC-DI

**Applicable Products:** MME

**Feature Changes**

**MMEmgr Linear Scalability**

MME (Mobile Management Entity) is a control-plane only node with significant scaling required on two fronts:

- **S1AP/SCTP connections with eNodeBs** - tens of thousands
- **Millions of UEs**

In addition a relatively smaller number of SCTP (SGsAP, SLsAP and SBcAP) and Diameter (S6a, SLs and SLg) connections are required

**Previous Behavior:** All S1AP/SGsAP/SLsAP/SBcAP connections are terminated on the demux SF-VM using MMEmgr tasks. This limits the signaling capacity which can be provided by MME.

**New Behavior:** The following changes have been made to enhance the scalability of MMEmgr tasks:

- **MMEmgr tasks will be distributed across session SF-VMs**
- **MMEdemux task now resides on the demux SF-VM.**
- **Number of IMSImgr tasks has been increased.** (CSCup66362) [see table below]
• Diameter proxy scaling has been improved.

### Table 6: MMEmgrs Tasks - VPC-DI

<table>
<thead>
<tr>
<th>Max. Number of SF-VMs</th>
<th>Max. Number of MMEmgrs per VPC-DI Instance</th>
<th>MMEmgrs per SF-VM (Default)</th>
<th>MMEmgrs per SF-VM (Allowed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>24</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

### Command Changes

**mmemgr-average-cpu-utilization**

This is a new MMEmgr-specific congestion control threshold CLI command.

```plaintext
custom
configure
  congestion-control threshold mmemgr-average-cpu-utilization { critical | major | minor }
percent_threshold_value
end
```

Notes:

- By default this threshold value is **not** enabled.
- A default value of 80% is assigned to the critical threshold only.

### Performance Indicator Changes

**congestion-control configuration**

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

- Congestion-control Critical threshold parameters
  - mmemgr average cpu utilization

- Congestion-control Major threshold parameters
  - mmemgr average cpu utilization

- Congestion-control Minor threshold parameters
  - mmemgr average cpu utilization

---

**CSCup68855 - HeNBGW support on Virtual Platform (VPC-DI)**

**Applicable Products:** VPC-DI
Feature Changes

HeNB-GW Support on VPC-DI
HeNB-GW (Home evolved Node B Gateway) has been qualified as being supported on VPC-DI.

CSCup75830 - DPC2: Diam proxy scaling
Applicable Products: VPC-DI

Feature Changes

Enhance Diameter Proxy Pool to Handle a Higher Number of Transactions
The existing Global Configuration mode require diameter-proxy CLI command has been enhanced to allow multiple diamproxies-per-card and specify the proxy selection algorithm type in the ASR 5500 and VPC-DI. For additional information on command changes associated with this feature, refer to the description of CSCup75830 in the System Changes in Release 18 chapter of this Release Change Reference.

CSCup86883 - VPC-DI Serving GPRS Support Node
Applicable Products: SGSN
Related CDETS ID: CSCuq24364 - SGSN SCCP Support for VPC-DI

Feature Changes

SGSN Support on VPC-DI
SGSN (Serving GPRS Support Node) has been qualified as being supported on VPC-DI.

CSCuq12270 - Add support for multiple IP interfaces in the same IP subnet
Applicable Products: VPC-DI

Feature Changes

Multiple IP Interfaces in the Same IP Subnet
Previous Behavior: IP interfaces must belong to different subnets.
New Behavior: IP interfaces can now belong to the same subnet.
OSPF is not supported for multiple interfaces on the same subnet.

**CSCuq12399 - Implement flow-redirect mechanism.**

Applicable Products: VPC-DI

**Feature Changes**

**Packet Flow Redirection**

A flow-direct capability now redirects packets to another SF-VM for flow lookup while npumgr is recovering the local flow database. This occurs during npumgr restart and SF-VM initialization.

**CSCuq13710 - openstack cfgdisk metadata for DI Slot number**

Applicable Products: VPC-DI

**Feature Changes**

**OpenStack Configuration Metadata**

OpenStack cfgdisk metadata now includes a param.cfg file to include anything that is in the param.cfg on the vHDD. This would include slot number, card type (if needed), etc.

**CSCuq60328 - LESS: Qualify with VPC**

Applicable Products: VPC-DI and VPC-SI

**Feature Changes**

**L-ESS Now Supported on VPC-DI**

L-ESS (Local External Storage System) has been qualified as being supported on VPC-DI.

**CSCuq97176 - VPC-DI Network mapping and A-B bonding support**

Applicable Products: VPC-DI
Feature Changes

Network Mapping of NICs for non-UCS Hardware

VPC-DI now supports a way to specify network topology in a param.cfg file that specifies NIC operating parameters including:

- Designation of DI-Network or service ports
- VLAN for DI-Network
- Configuration applies to single NIC or a pair of NICs in A-B redundancy mode

A-B network redundancy (bonding driver) is supported for non-UCS hardware. This feature allows for setup of redundant connections to the physical L2 switch.

The following are sample bonding configurations:
```
qvpc-di:card3-cpu0# cat /cdrom1/staros_param.cfg
CARDSLOT=3
ETH0_MAC=00:05:47:00:02:01
ETH1_MAC=00:50:56:87:d7:1d
ETH2_MAC=00:50:56:87:a2:52
BOND0_MAP=ETH0
BOND0_PRIMARY=ETH0
BOND0_REVERSION_POLICY=0
BOND0_LINK_DETECT=0
BOND0_MII_POLL=100
BOND1_MAP=ETH1,ETH2
BOND1_PRIMARY=ETH1
BOND1_REVERSION_POLICY=0
BOND1_LINK_DETECT=0
BOND1_MII_POLL=100
```

CSCut22121 - [SaMOG] - Qualification of SaMOG on VPC-DI platform

Applicable Products: SaMOG

Feature Changes

SaMOG Running on VPC-DI Platform

S2a Mobility Over GTP (SaMOG) has been fully qualified to run on VPC-DI.

CSCut30530 - 32 BGP ECMP Support for vPC-DI

Applicable Products: VPC-DI
Feature Changes

Increase Maximum Number of ECMP Paths

**Previous Behavior:** Prior to this release, a maximum of ten BGP ECMP routing paths were supported per context.

**New Behavior:** With this release, a maximum of thirty-two BGP ECMP paths are supported.

Command Changes

maximum-paths

The maximum number of paths has been increased to 32.

```bash
configure
context context_name
router bgp AS_num
    maximum-paths { ebgp | ibgp } max_num
end
```

Notes:

- `max_num` is an integer from 1 through 32.

CSCuu51841 - [ePDG]DI: Unable to scale when OCSP is not reachable

**Applicable Products:** VPC-DI, ePDG

Feature Changes

Configurable OCSP Responder for Crypto Template

**Previous Behavior:** If the Online Certificate Status Protocol (OCSP) responder is unreachable, a non-blocking system call to the connect process takes time to return an error (due to TCP retransmission exponential backoff mechanism). This delay in returning the error also delays session establishment.

Regardless of the time taken by the connect process to return an error, if there is no response from the kernel within the configured timeout, the TCP socket will be closed and the session proceeds with an alternate fallback mechanism for certificate validation.

**New Behavior:** A new Crypto Template CLI has been added to configure a certificate server timeout interval.
Command Changes

timeout cert-server

A new Crypto Template Configuration mode `timeout cert-server` command sets the Certificate Server timeout in seconds. This is the interval within which the response from an external OCSP server should be received.

```bash
configure
crypto context context_name
crypto template template_name ikev2-dynamic
timeout cert-server seconds
end
```

Notes:

- `seconds` is an integer from 1 through 60 (Default = 20).
VPC-SI Changes in Release 18

This chapter identifies features and functionality added to, modified for, or deprecated from VPC-SI StarOS 18 software releases.

- VPC-SI Feature Changes for 18.2, page 443

VPC-SI Feature Changes for 18.2

This section identifies all of the VPC-SI enhancements included in this release:

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

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

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

Important

For more information regarding features in this section, refer to the *VPC-SI System Administration Guide* for this release.

CSCue09140 - StarOS Mgmt Interface VLAN

**Applicable Products:** VPC-DI, VPC-SI

**Feature Changes**

**VLAN Support on Management Interfaces**

The VPC management interface now supports VLAN configuration. This support extends to the local context.
Bulkstats can be sent out an interface other than the normal management interface. This interface also supports VLANs.

You can also configure other OA&M services on separate VLANs.

You can assign separate source IP addresses for the OA&M services. OA&M services should not be bound to the same VLAN as service VLANs. Other services include SGi, Gi, Pi, eGTP or other packet core specific interfaces and services.

Currently ACL support, the `vlan priority value` and `vlan-map interface if_name context_name` commands are not available for management VLANs.

### Command Changes

**vlan**

This feature is implemented by adding support for the `vlan` command to the management port in the local context. See the example command sequence below.

```
configure
  port ethernet 24/1
  vlan 184
    bind interface 19/3-UHA foo
  end
```

### CSCum64947 - [ePDG] - ePDG service support on SSI

**Applicable Products:** VPC-SI

### Feature Changes

**ePDG and HNB-GW Support on VPC-SI**

ePDG (evolved Packet Data Gateway) and HNB-GW (Home NodeB Gateway) have been qualified as being supported on VPC-SI.

### CSCup35998 - [ePDG] IPSec scale and performance improvement on SSI

**Applicable Products:** VPC-SI
Feature Changes

Higher Number of IPSec Sessions for ePDG

**Previous Behavior:** The number of allowed IPSec sessions supported for ePDG (evolved Packet Data Gateway) was constant.

**New Behavior:** The number of allowed IPSec sessions supported for ePDG is now dynamic based on available memory CPU cores.

CSCup36063 - [ePDG] IPSec Scale - Performance Improvement in SSI

**Applicable Products:** IPSec, VPC-SI

Feature Changes

Increased ESP Packet Processing Performance

OpenSSL will now be used to process ESP (Encapsulating Security Payload) packets instead of SSH crypto routines. OpenSSL crypto routines only support ESP packet authentication and encryption functionalities with the AES-GCM algorithm in the IPSec framework.

Command Changes

encryption

Keywords have been added to the encryption command in the IPSec Transform Set Configuration mode. These keywords add support for AEAD (Authenticated-Encryption with Associated-Data) algorithms available through OpenSSL.

```
configure
  context context_name
    ipsec transform-set set_name
      encryption { 3des-cbc | aes-128-gcm-128 | aes-cbc-128 | aes-128-gcm-64 | aes-128-gcm-96 |
        aes-256-gcm-128 | aes-256-gcm-64 | aes-256-gcm-96 | aes-cbc-256 | des-cbc | null }
  end
```

**Notes:**

- **aes-128-gcm-128** = IKEv2 Child Security Association IPSec ESP Algorithm is AES-GCM-128 with 128-bit ICV (Integrity Check Value). HMAC algorithm with this encryption algorithm should be none.
- **aes-128-gcm-64** = IKEv2 Child SA (Security Association) IPSec ESP Algorithm is AES-GCM-128 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be none.
- **aes-128-gcm-96** = IKEv2 Child SA IPSec ESP Algorithm to be AES-GCM-128 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be none.
- **aes-256-gcm-128** = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 128-bit ICV. HMAC algorithm with this encryption algorithm should be none.
aes-256-gcm-64 = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be none.

aes-256-gcm-96 = IKEv2 Child SA IPSec ESP Algorithm is AES-GCM-256 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be none.

hmac

The none keyword has been added to the hmac command in the IPSec Transform Set Configuration mode. This keyword must be used in conjunction with the AEAD algorithms described above.

configure
context context_name
    ipsec transform-set set_name
        hmac { aes-xcbc-96 | md5-96 | none | null | sha1-96 }
end

Notes:
• The none option is only used only with combined mode encryption algorithms such as AES-GCM.

CSCup66766 - MME support on VPC-DI

Applicable Products: MME

Feature Changes

MMEmgr Linear Scalability

MME (Mobile Management Entity) is a control-plane only node with significant scaling required on two fronts:

• S1AP/SCTP connections with eNodeBs - tens of thousands
• Millions of UEs

In addition a relatively smaller number of SCTP (SGsAP, SLsAP and SBcAP) and Diameter (S6a, SLs and SLg) connections are required

Previous Behavior: All S1AP/SGsAP/SLsAP/SBcAP connections are terminated on the VPC-SI using a single MMEmgr task. This limits the signaling capacity which can be provided by MME.

New Behavior: Default number of MMEmgr tasks have been increased for the Medium and Large VPC-SI models.

Table 7: MMEmgrs Tasks - VPC-SI

<table>
<thead>
<tr>
<th>VPC-SI Model</th>
<th>Max. Number of MMEmgrs per Chassis</th>
<th>MMEmgrs per Chassis (Default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VPC-SI Model</td>
<td>Max. Number of MMEmgrs per Chassis</td>
<td>MMEmgrs per Chassis (Default)</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Large</td>
<td>42</td>
<td>42</td>
</tr>
</tbody>
</table>

**Command Changes**

`mmemgr-average-cpu-utilization`

This is a new MMEmgr-specific congestion control threshold CLI command.

```
configure
congestion-control threshold mmemgr-average-cpu-utilization { critical | major | minor }
percent_threshold_value
end
```

Notes:
- By default this threshold value is **not** enabled.
- A default value of 80% is assigned to the critical threshold only.

**Performance Indicator Changes**

`congestion-control configuration`

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

- Congestion-control Critical threshold parameters
  - mmemgr average cpu utilization

- Congestion-control Major threshold parameters
  - mmemgr average cpu utilization

- Congestion-control Minor threshold parameters
  - mmemgr average cpu utilization

**CSCuq59203 - HeNBGW support on Virtual Platform (VPC-SI)**

Applicable Products: VPC-SI
Feature Changes

HeNB-GW Support on VPC-SI

HeNB-GW (Home evolved Node B Gateway) has been qualified as being supported on VPC-SI.

CSCuq60328 - LESS: Qualify with VPC too (in addition to ASR5000 and ASR5500)

Applicable Products: VPC-DI and VPC-SI

Feature Changes

L-ESS Now Supported on VPC

L-ESS (Local External Storage System) has been qualified as being supported on VPC-DI and VPC-SI.